

RISK MANAGEMENT

2023

ERM
SPECIAL EDITION

- Using Technology to Drive Sustainable ERM Initiatives
- Applying ERM Processes to ESG Risks
- The Evolution of the Risk Manager





RISK MANAGEMENT

COLUMNS

2 Using Technology to Drive Sustainable ERM Initiatives
As organizations progress through various stages of their ERM initiatives, certain key considerations can help them get the best results from risk management technology.

6 6 Steps to Maximize the Value of RMIS Tools
Make the most out of risk management information systems with these key strategies.

8 Applying ERM Processes to ESG Risks
Incorporating ESG factors into your ERM program can strengthen your organization's understanding of its risks and enhance overall business performance.

10 Q&A: Melissa Reynard
Melissa Reynard, former director of ERM at the Internal Revenue Service and winner of the RIMS 2021 ERM Global Award of Distinction, discusses anticipating emerging risks, creating a more risk-aware culture, and developing a structure to enhance risk-sharing and strategic decision-making.

13 Q&A: Denise Cosentino
Denise Cosentino, director of ERM at Eversource Energy and a U.S. Honoree recipient of the 2021 ERM Global Award of Distinction, discusses what it took to get a seat at the table of New England's largest energy delivery company.

FEATURES

15 The Evolution of the Risk Manager
Technology such as artificial intelligence promises to alter the practice of risk management. Will these advances simply change how risk professionals work or create new, more strategic roles?

20 Managing Data Security Risks of AI Technology
AI holds tremendous potential to change how we work, but it also introduces massive risks, including to data security. Risk managers must act now to build smart, safe guidelines for AI use within their organizations.

26 Eye of the Beholder: Understanding the Psychology of Risk Perception to Improve Risk Management
To best design and implement an effective risk management program, it is critical for risk professionals to understand the psychological aspects of risk perception.

30 How to Measure Risk Capacity for Strategic Initiatives
By applying holistic risk management techniques, organizations can estimate and expand their risk capacity to make room for strategic initiatives.

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



Chief Executive Officer

Gary LaBranche, glabranche@RIMS.org



AN AWARD-WINNING PUBLICATION



CONTACT US

All submissions and letters should be sent to:

Morgan O'Rourke

Editor in Chief

Risk Management

228 Park Ave S, PMB 23312

New York, NY 10003-1502

morourke@RIMS.org

T: (212) 655-5922

www.RMmagazine.com



INSIDE

Getting the Most from RMIS.....	06	Q&A: Risk Culture at the IRS	10
Applying ERM to ESG	08	Q&A: An Energetic ERM Program.....	13



Using Technology to Drive Sustainable ERM Initiatives

by Joshua Newsum

Many promising enterprise risk management (ERM) programs are launched as a disciplined process for an organization to understand and address critical exposures. However, they often become difficult to maintain beyond the initial phases as key team members need to focus attention on their primary job responsibilities.

The right technology can help sustain ERM initiatives by automating much of the data-gathering and reporting aspects that are critical for ongoing decision-making. Nonetheless, technology-based solutions can only be as effective as an organization's internal culture and established ERM processes.

The following are some key considerations to help organizations at various stages of their ERM initiatives to get the best results from risk management technology:

RISK MANAGEMENT FRAMEWORK

Organizations typically have different expectations for ERM initiatives based on factors like their level of risk maturity, industry sector, internal and external resources, business model, and organizational complexity. For instance, those in the early stages of ERM implementation may be looking initially to capture and analyze data on their most significant exposures to establish baselines, set priorities for treat-

ing risks, and monitor progress.

Meanwhile, organizations with more advanced risk maturity may want to leverage ERM to support strategic decision-making and meet specific internal and external reporting requirements.

Less-mature risk functions may simply need the basic capabilities of risk systems or may be able to accomplish many data gathering, reporting and analytical tasks manually. However, advanced programs typically call for more sophisticated applications for data capture/sharing, workflow management, analytics and multi-level reporting.

Although most current risk information technology systems perform well in facilitating risk assessments and allowing users to input and retrieve data to address specific



RIMS-CRMP

RIMS-Certified Risk Management Professional

Get Certified

Start Your Application Today

Validate your performance ability, technical knowledge, and commitment to excellence—earn the RIMS-Certified Risk Management Professional (RIMS-CRMP) certification.

Add the only competency-based risk management credential to your professional profile to:

- Stand out in the job market
- Increase your earning potential
- Elevate your status
- Show your commitment to ethics
- Raise the standards of your profession

Learn more and apply www.RIMS.org/Certification



ANSI Accredited Program
PERSONNEL CERTIFICATION
#1223





requirements, they differ in the versatility they offer to configure workflows based on the needs of individual business units or to facilitate reporting to accommodate both low- and high-maturity clients. As a result, organizations need to evaluate systems and technology vendors carefully to determine whether a provider's functions and capabilities are aligned with their enterprise-wide risk management needs.

ERM STRATEGY

Those launching new ERM initiatives often start with specific goals and document an overall vision for ERM that aligns with the expectations and priorities of the board and senior leadership. The vision describes what they ultimately expect to achieve and how they plan to get there, including milestones and what it will take in terms of leadership commitment and internal and external resources.

This involves determining what will be needed with respect to engagement and participation by individuals in various business units, departments, and functions within the organization. Establishing guiding principles for the ERM initiative and mapping out a plan will put risk managers in the best position to evaluate how technology can help drive success in both the initial phase and subsequent expansion.

For instance, as an ERM initiative develops over time, it will expand to encompass more business functions and units, diverse risks and an increasing number of participants throughout the organization. In turn, technology will have to be scalable to accommodate increasing volumes of data and offer the versatility to accomplish more complex analytical and reporting requirements.

In evaluating technology systems and vendors, consider not only how you see your ERM program today, but also how you see it evolving in the future. If you change some elements of your risk management methodology, can your technology solution readily support that transition?

Organizations typically use two different

approaches for implementing risk management technology. Some select a risk technology system and vendor and build their ERM process around those capabilities, while others choose their technology after they have established a process.

In the former case, when selecting technology is the starting point, if risk management wants to make adjustments in its data capture, workflows, analytics and reporting processes at some point in the future, it can find itself boxed in by its technology and it may be difficult and costly to make the necessary changes. These situations typically surface later in the ERM lifecycle and often result in inefficiencies and significant costs to make adjustments to the system to accommodate the changes.

So, in selecting a technology vendor, it is often prudent to start with your process and try to project how it might evolve over time. Then, you can ask: "Is this a technology solution that works for us today, and will it also work for us three to five years from now? And how does the technology vendor demonstrate that?"

ERM ROLL-OUT PROCESS

Risk managers launching or revitalizing an ERM process may begin by assessing their resources and then developing a process that will generate desired results, both in the initial phase and in later stages. For example, an incremental approach might be to conduct a limited initial roll-out to specific business units and then expand to encompass other functions or operations across the organization on a scheduled basis over time.

On the other hand, risk management departments with greater resources or established internal networks of managers with risk-related responsibilities may be in position to launch or reintroduce their ERM initiative on an organization-wide basis. It is worth pointing out, however, that even organizations with extensive resources may face obstacles with a full-scale approach, which still must be conducted in a scheduled, prescribed manner with proof of concepts

and a series of quick wins.

Whether the ERM process is rolled out incrementally or full-scale, risk managers will have to collaborate with individual business units, functions and operations to identify individual contacts and delineate their responsibilities for gathering or reporting information from their respective areas.

Consider what efficiencies might be achieved by leveraging information already being captured and used for discrete purposes by individual units, as well as what workflows might be streamlined through automation. In some cases, there may be a need to import data from spreadsheets or discrete systems used by individual business operations into the enterprise system. Ultimately, any manual information gathering, reporting and analytical activities might be automated to streamline workflows and free up individuals throughout the organization to focus more on their primary roles.

The roll-out activities should include a focus on preparing individuals throughout the organization for change. Often overlooked and underestimated is helping people understand their roles in risk assessment and risk management and their value to their department or business unit and to the entire organization. The deployment of centralized risk technology can help facilitate this by enabling individual business units to compare their risk analytics, progress and results to peer operations as well as to the overall organization.

In this context, the transparency of your data is key, along with the ability to slice and dice assessment results to provide ready access to critical data across various business units. This should also be able to accommodate dynamic reporting requirements that may change over time. Effective ERM and GRC programs typically require the ability to examine data from multiple angles, choose discrete data to analyze and report, and determine the frequency, recipients and format of reporting. Thus, from the outset, it is important to identify vendors and systems that

enable you to access data in multiple ways for use by management at various levels within the organizations. Otherwise, any efficiencies achieved in the data collection process may be lost to reporting issues.

RISK PROFILE

Leadership must define an aggregated level of risk or volatility acceptable across the organization. This is a cornerstone of an effective and sustainable ERM initiative because it establishes a critical benchmark for assessing how effectively the organization's current risk management program is helping to meet that objective and to determine where specific improvements in risk assessment and remediation activities may be needed.

This is typically a dynamic process. Organizational risk appetites may evolve over time, depending on performance; changes in corporate structure, such as through a merger, acquisition, divestiture or reorganization; operating environment; economic and regulatory conditions, among other variables. Accordingly, risk management needs to maintain an ongoing dialogue with senior leadership and board members to recalibrate the organization's risk appetite and tolerance over time, as well as to make corresponding adjustments to its ERM initiative.

At the same time, risk management activities of individual business units or operations need to be brought into alignment with organizational priorities, even as they may have relatively higher or lower risk tolerance levels, depending on their business activity, exposures, and potential impact on the organization's overall risk profile.

Risk managers at dynamic organizations whose priorities might need to be adjusted will need to make sure that any risk technology they choose to support their ERM initiatives give them the flexibility to make periodic or more frequent adjustments to address evolving needs and priorities.

In effect, the technology must be able to support dynamic assessments of an organization's risk profile, including reconcil-

ing risk assessment data with the organization's risk appetite. This allows leadership to compare their current risk profile against their objectives and determine whether they are over- or under-investing in their risk controls and mitigation plans relative to their risk appetite. They then can pivot quickly (or on period-over-period basis) to adjust their investment in controls or reevaluate mitigation options.

RISK LANGUAGE

Various disciplines and functions within any organization often have different ways of defining and describing risk. Effective and sustainable ERM initiatives call for developing and implementing common language, terminology and measurements that will be readily understood by participants across all functions and disciplines throughout the organization.

This work should include implementing a standard risk taxonomy and scoring methodology so that data can be captured, analyzed, shared and acted upon as appropriate by participants in all areas of the organization. Getting this right—and having the technology in place to enable users in various functions to input and access the information and analytics they need on a timely basis—will enable the ERM program to interact seamlessly with other risk assurance functions and help drive value throughout the organization.

In practice, different governance functions within an organization view risk differently for different purposes. Thus, technology needs to be able to standardize the view for each of the governance purposes, but also must be flexible enough to allow for different methodologies across those governance functions.

For instance, an ERM group, internal audit and compliance group might each rely on the risk register built to conduct risk assessments for their own centralized purposes. But they may view and rate those risks differently based on their individual requirements. If the technology does not allow for differ-

ent governance groups to evaluate risk and report related data in different ways based on their needs, then the technology is not supporting them and it will not be used.

CONTINUOUS IMPROVEMENT

A sustainable ERM initiative will have continuous improvement built into its vision and DNA. Over time, effective ERM initiatives facilitate steady improvements in overall risk management practices and results. There also should be anticipated process improvements in the ERM initiative that come from finding better and faster ways to gather the right data, perform analytics and prepare and disseminate reports with findings tailored to specific audiences at all levels in the organization. Of course, those transitioning from spreadsheets and shared drives to various software tools will invariably see dramatic improvements in workflow and efficiency.

With ready access to vast amounts of data and analytics facilitated by their deployment of technology, risk managers will be better positioned to make critical decisions to scale or expand their ERM program to correspond with any adjustments to their organization's risk appetite. At the same time, they can gauge how well their ERM program is aligned with their organization's strategic objectives and make any necessary adjustments to keep these in sync.

Over time, risk leaders will need the versatility to adapt their ERM initiatives to the dynamic requirements of their organizations as well as to evolving frameworks, such as ISO and COSO. By having a sound vision for ERM backed by leadership, embraced by engaged participants throughout the organization and supported with technology-based systems that help drive results, risk managers will be able to deliver the value organizations need to navigate critical exposures and achieve their strategic objectives. **R**

Joshua Newsum is senior ERM practice lead at Origami Risk LLC.



6 Steps to Maximize the Value of RMIS Tools

by Patrick O’Neill

Risk professionals increasingly rely on technology to manage business risk, yet many also feel they are underutilizing their current risk management information system (RMIS). In fact, more than half of the over 1,000 risk executives surveyed in Redhand Advisors’ *2023 RMIS Report* characterize their use of analytics as “only moderately effective or worse.” Nearly as many still do not utilize their RMIS to full capacity due to cost, lack of resources and lack of training or knowledge of the system.

To close the gap, risk managers need to focus on improving their data quality and governance; engage skilled data analysts; and explore adopting big data analytics, artificial intelligence and machine learning.

Below are six strategies for achieving better results when applying advanced analytics to your risk management process, whether you are just starting to use risk technology or have been implementing a system for several years:

1. Define goals and objectives for your data analytics project. Understanding your goals and objectives will allow you to align your efforts with outcomes that deliver value. Work backward and start the process by considering how applying advanced analytics will help achieve your goals. You might even outline the use cases and then apply the specific tools or functionality that generate the best outcomes for your needs. For example, if your team finds dashboards especially helpful, some tools will offer more robust visualization than others.

2. Review what is in your current technology toolbox. Do the systems you have in place support your goals, or do you need to



look for additional third-party tools to meet them? It is not a simple process to activate the various tools your vendor might offer and have them automatically meet your specific needs—software is only as effective as the planning behind it.

3. Make sure the data is accurate and clean. The quality of data is an industry-wide challenge. On the surface, your data might appear up to date and accurate. However, upon closer scrutiny, you might find your code tables are not suitable to your risks, or your injury and accident cause codes are outdated or too generic for your level of activity. For example, if you use the standard lists from your insurance carrier or third-party administrator, 90% of your claims may be coded as single claim types because

there is no list specific to your industry. To capture the right data, it is critical to have codes specific to your industry or even your individual organization. Similarly, if you are analyzing your locations relative to local flood zones and potential for hurricanes but lack the specific geocodes corresponding to those locations, your property data will not be accurate and your output will not be useful.

4. Mine valuable data in the commentary of a claim instead of the codes. If a worker injures multiple parts of their body and the only options in your RMIS are “shoulder injury” or “multiple injuries,” that will not give your claims team what they need. Instead, you might “mine” the important commentary under each claim.

For instance, shoulder and back injuries are the most costly for organizations, so the proper treatment and response can have a positive impact on your claims trends. Another benefit to analyzing narrative data is that details that are not coded may be central to a claim's resolution. For example, co-morbidities of the worker are typically not captured as part of the claim, but may be found in the narrative or commentary.

5. Integrate data analytics into your business processes. Even when they get past the hurdle of obtaining quality RMIS data, many risk management teams still use this information in silos instead of leveraging it to make decisions across the business and its operations. For instance, do you flag claims early on that have a potential for

years ago. The ability to embed AI, such as ChatGPT, into data analytics processes only became available within the past eight months, for example. Integrating advanced analytics into your risk processes requires a certain level of expertise, so it is critical to have teammates who can support such activity. The move to a software-as-a-service (SaaS) model in recent years has enabled enterprises to push their IT department out of the software implementation process as RMIS vendors are typically responsible for everything in the cloud. However, many companies are now bringing IT back to the table to support SaaS applications across business operations. If your risk management team has not been able to make this happen, you may find a valuable partner in your IT department.

Even when they get past the hurdle of obtaining quality RMIS data, many risk management teams still use this information in silos.

high cost or severity? If your RMIS could instantly get such a claim to the adjuster, then a team member could quickly reach out to the injured employee.

Similarly, if your RMIS could automatically flag potentially fraudulent claims and deliver them to the right adjuster, your team could act quickly rather than waiting for a report that might get circulated a week later. It is possible to embed RMIS analytics and outcomes into your workflows and processes, and to make that data actionable within a compressed timeframe.

6. Take steps to adopt big data analytics, artificial intelligence and machine learning into your RMIS. Technology-based risk tools and functionality have come a long way from where they were even just two

As RMIS capabilities continue to evolve, risk professionals have been actively involved in testing, evaluating and refining their enterprise's analytics processes. This requires engaging with departments and operations across your organization to break down silos and maximize the technology solutions you have in place. You also need to collaborate with your vendors to keep abreast of new tools and resources they may be adding to their platforms. By integrating your technology applications into your continuous improvement process, you will be able to achieve a strong and sustainable return on investment from your RMIS tools. [R](#)

Patrick O'Neill is founder and president of Redhand Advisors.



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

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



RISK
MANAGEMENT



Applying ERM Processes to ESG Risks

by Karl Viertel

ESG risks are now playing a much larger role in the overall risk exposure of organizations. For instance, some jurisdictions have developed corporate regulations targeting climate sustainability, while some financial regulators have adopted specific requirements regarding ESG disclosure rules. Consumers are also making buying decisions based on a company's ESG standings.

Incorporating these factors into your enterprise risk management (ERM) program can strengthen your organization's understanding of its full portfolio of risks and enhance overall business performance. The good news is that ERM and ESG risks have a significant intersection. If you already have solid ERM processes in place, you can leverage these to address ESG risks while also applying new metrics for evaluating these risks and any related data.

To increase the chances of success when setting up an ESG governance capability, key elements to consider include:

- **Establish clear ownership:** Determine who is responsible for ESG risk assessment processes. As this is a new focus for many organizations, the role may still be in the process of being defined. This responsibility is likely to fall under operational or non-financial risk teams, or even to a new dedicated role. Defining this role and allocation of resources is vital for overall success as it will provide decision-makers with reliable information to inform strategies.
- **Develop mitigation strategies:** The same risk identification process can be applied to ESG risks, such as categorizing assets and defining a maturity



rating based on a performed ESG risk assessment. With these insights, you need to strategize on how the organization can best utilize information gathered from identified ESG risk analyses to drive decision-making. Of course, due to the varying nature of ESG risk, some mitigations may not be possible due to the magnitude of the risks addressed. However, it will be beneficial for ESG reporting and invoke greater investor confidence if you have a thoroughly thought-out strategy and roadmap to address threats before they happen, and if you can demonstrate a proactive approach.

- **Prioritize risk data:** Evaluating ESG risk exposure might require gathering information from multiple data sources. It is essential to spend the time

identifying and narrowing down the relevant data sources to be included and prioritized in your analysis.

- **Determine a reporting structure:** When deciding on your reporting structure, always ask: Who will consume the risk information and use it to make decisions? Identify a reporting structure that will allow your company to align with regulatory reporting requirements, and take into account key decision-makers, such as operational risk teams, ESG sustainable finance teams, shareholders and regulators. As accountability increases among the board and senior leadership, they must also assume responsibility here. The emphasis they place on ESG risk management topics will greatly contribute to overall success

of the framework. With many jurisdictions beginning to implement requirements for ESG-related disclosures, it is imperative to speak in the language of socially conscious investors and lenders on ESG factors.

- **Integrate with existing methodology:** Do not try to reinvent the wheel. If you have sound and comprehensive ERM processes in place, leverage the same mechanisms to identify, assess and address ESG risks as well. This reduces friction in business lines and among people consuming the reports, including auditors.
- **Develop a comprehensive view of ESG:** ESG is a broad concept so extend your scope beyond the environmental factors of climate change and resource protection. Taking too narrow a view will lead to rework, audit findings and lost effort. Diverse social

risks, such as protests or unethical treatment of employees, are a direct risk to a company's success and reputation. Governmental risks, like inefficient internal controls systems or compliance failures, can all have a significant impact on ESG reporting. In the case of ESG financing, this may also lead to misinformed investment decisions. Additionally, keep in mind that ESG materiality is dynamic and it is critical to consider risks even if they seem "dormant."

- **Account for risks and opportunities:** Make sure to account for both the opportunities and risks within a certain "megatrend," such as climate change, politics, digital privacy and resource scarcity. For example, if your organization produces battery technology that utilizes substances such as lithium or cobalt,

then resource scarcity might be a primary risk. However, the increased demand for electric vehicles might be an opportunity.

- **Keep it simple:** While ESG risk management might be new to the organization, the same core principles of ERM can help identify, mitigate and manage these risks. Understanding core risks and gaining an overall perspective on ESG exposure should be your first priority. Then, it can be improved by shifting focus to more complex methodology and data structures. With pressure mounting and stakeholders demanding transparency around an organization's approach to ESG topics, it is important to get a head start. Start simple and then refine. **R**

Karl Viertel is managing director of the GRC unit at legal and risk software firm Mitratech.

Here, There & Everywhere

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

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



**RISK
MANAGEMENT**



Q&A

Creating a Culture of Risk Management in the IRS

Interview by Russ Banham

IN NOVEMBER 2021, RIMS presented the Internal Revenue Service with the society's 2021 ERM Global Award of Distinction. The IRS was honored for its progress in anticipating emerging risks, the steps it took to create a more risk-aware culture, and ultimately developing an ERM structure to enhance risk sharing and strategic decision-making.

The honor was well deserved, as so much needed to be accomplished and implemented against the backdrop of an extended government shutdown, sweeping tax reforms and significant operational disruptions within the IRS itself caused by the COVID-19 pandemic. The government agency's ERM program assisted its resilience amidst mounting uncertainties and vulnerabilities. To learn more about the ERM program, we met with **MELISSA REYNARD**, director of ERM at the IRS, who was on site to receive the award at the RIMS ERM Conference 2021. Reynard has served in the position since January 2020, and previously was a senior risk advisor in 2014.



RIMS: First of all, congratulations on earning the ERM Global Award of Distinction, a well-deserved honor, given how few organizations were prepared for the extraordinary economic duress caused by the COVID pandemic.

Reynard: Thank you. Like many ERM programs, ours is a work in progress. Interestingly, we established the program in 2013 in response to another crisis—a change in our leadership. The acting IRS commissioner made the decision to create the ERM program and brought in our first Chief Risk Officer. We have a relatively small core office, which comprises the CRO, an ERM director and four senior risk advisors. But we have a significant network of risk liaisons representing each of the two-dozen or so IRS business units, such as the wage and investment division, criminal investigation, and information technology office. At the outset (of the program), we worked with them to operationalize risk management across the IRS. Since then, the program has evolved.

RIMS: Tell us how the program has evolved, into your current ERM culture and processes.

Reynard: One of the key components of the initial construct of the program was the decision to develop a half-dozen risk management standards, so each business unit had to put specific processes in place to identify, assess, respond, report, monitor/elevate and communicate risks. Once the standards were in place, over time, each business unit was entrusted to develop their own processes to address the standards, enabling them to do what worked best for them and their culture.

RIMS: That sounds like several cultures as opposed to one. Is that advisable?

Reynard: Great question. Let me provide some historical context. I've been with the IRS for about 38 years (after starting as a Customer Service Representative in 1984). The culture then was, if you identified a problem or a risk, you focused on fixing it or solving it. You weren't necessarily going to



bother your boss with it; you just got it done. Now, while each business unit still has its own unique culture, they follow the ERM standards we put in place and use their own established processes to actively identify and raise risks, as needed. We encourage them to build upon what already exists and self-assess against the standards to identify areas for improvement. What brings it all together is transparency. You still fix the problem in your unit, but the associated risks have a greater level of awareness, resulting in cross-cultural, cross-business unit discussions. Each business unit's risk liaison meets with their peers monthly in group sessions, talking about what they're doing in their respective units.

RIMS: So, the culture is one of sharing risks and risk management best practices.

Reynard: Yes, and that is a departure from the past. In the pre-ERM program days, you knew the risks in your business unit, but you generally kept them to yourself and worked to resolve them. Nevertheless, people still have difficulty with change. You can't simply direct them to raise risks and share information. The risk liaisons, and the leadership teams, need to feel comfortable talking about risks and what they are doing to address them.

RIMS: That's not easy, I would imagine, particularly in a highly bureaucratic government agency where people are often very concerned with processes and procedures. How have you overcome these impediments?

Reynard: One thing we did early in the program is introduce the Risk Acceptance Form and Tool, or "RAFT." When a business unit is deciding to accept a certain risk associated with a significant decision, the tool puts forth the necessary due diligence in a consistent framework for them to fill out before making the final decision. The RAFT will ask, for example, if you've considered other alternatives, what risks

are associated with those alternatives and if the risk decision will have a potential impact on other business units. In effect, it compels the leadership to collaborate with other business units, if needed, and document the rationale for accepting the risk.

RIMS: You mentioned that the acceptance of a risk in one unit may have an impact on another unit. Can you elaborate on that?

Reynard: If you're in the communications division and tasked with contacting taxpayers via letters about newly-enacted legislation, the risk is that the letter will generate phone calls that come into the wage and organization. This group may need additional staffing, particularly if the letter goes out during the tax season, when everyone is filing their tax forms and the staff is overwhelmed. By having everyone apprised and discussing the situation, others can weigh in and add their insights, perhaps thinking up a new strategy. We've completed more than 300 RAFTS since the inception of the form. It's been a great tool and fits our culture here; employees and leadership are very comfortable with forms.

RIMS: You mentioned "overwhelmed staff" and the IRS has experienced huge staff cuts over the past decade or so. Has that affected the goals and effectiveness of the ERM program?

Reynard: You're right that we've had some budget cuts, [resulting in] a reduction in overall staff, with the preponderance of those job losses occurring in the customer service, audit, and collection parts of the IRS. We're constantly prioritizing and re-prioritizing the workloads. In fact, the number one risk for 2022 in our Enterprise Risk Profile

is the adverse impact of reduced enforcement on voluntary compliance (the dependence on taxpayers to voluntarily assess the correct amount of tax and file their returns in a timely manner). We're concerned about the tax gap—the difference between what people should be paying and are paying.

RIMS: Are you referring to average income taxpayers or wealthy taxpayers?

Reynard: Primarily complex high dollar audits. There's no single fix, but by using data and analytics technologies we can prioritize the workload and other resources to examine those cases we need to be more fully exploring.

RIMS: What is the current state of technology at the IRS? Given the budget cuts, has the service been able to invest in the kind of digital transformation that many large corporations have pursued?

Reynard: We have a long way to go. With the budget cuts, we still have a number of antiquated technology systems; one of the technology tools we use to process tax returns dates from the 1960s. That's a big problem at a time when we receive a significant number of Freedom of Information Act requests and litigation discovery requests, via our work with the Department of Justice. It's a substantial challenge for us to respond to these requests, according to the legally implemented deadlines. There are software and other technology tools that can make that work more efficient.

RIMS: Are you investing in these tools?

Reynard: The risk liaisons for these business units raised the need (for the investments) through the Risk Working Group,



which subsequently brought it to the attention of the Executive Risk Committee. The committee was able to secure some funding for some of these technology needs. We're now bringing these tools to bear.

RIMS: That's a great example of how an ERM structure can affect important strategic decisions. By toppling the silos precluding the identification and sharing of risks and instilling a culture of openness and transparency, big changes can be achieved—even with reduced staffing and capital. What else is being done to better prepare for emerging risks?

Keynard: We instituted an Annual Risk

Awareness Week, now in its fourth year. It involves training employees at all levels to learn about risk management activities and advance their knowledge of the subject. All new IRS managers now must take mandatory ERM training. We've also put together an ERM welcome video for new hires. All of these measures are designed to increase risk awareness and make sure all employees know what role they play in identifying and raising risks.

RIMS: How do you ensure the culture of risk-sharing you've created remains resilient?

Keynard: We've developed a Risk Culture and Awareness Index to measure those

concepts that had previously been difficult to gauge. It's our largest survey and is distributed to all employees, with the findings informing continuous improvements, which we've been able to attain on an annual basis. In all cases, by developing an ERM structure that enables the business units to build a program their way, based on their culture, you foster a risk culture of openness and transparency, increasing opportunities to get ahead of risks that produce positive outcomes and minimize negative operational surprises. **R**

Russ Banham is a veteran financial journalist who frequently covers risk management topics.

TAKE OWNERSHIP OF YOUR RISK DATA

Attend our three-part, virtual workshop series to improve your knowledge and enrich your risk management program with the best practices in data management, analytics and artificial intelligence.

You will earn your certificate once you purchase and complete this three-part workshop series. Part one of this workshop series begins December 7.



Instructor: **Pat Saporito**
Founder & Principal Consultant
Saporito & Associates, LLC

GO.RIMS.ORG/DATASERIES2023





Q&A

Generating an Energetic ERM Program

Interview by Russ Banham

EVERSOURCE ENERGY is New England's largest energy delivery company, providing electric, gas and water service to 4.3 million customers in Massachusetts, Connecticut and New Hampshire. The Fortune 500 company traces its roots to the middle of the 19th century, when watchwords like “climate change” and “energy sustainability” certainly had yet to enter the lexicon. Having divested most of its fossil fuel generation capabilities more than 20 years ago, Eversource is now focused on clean energy sources like solar and offshore wind, and was the company was the first utility in the United States to commit to a carbon-neutral status by 2030. Eversource is also committed to a strong enterprise risk management program, launched in 2005 when the utility was about to make a significant investment on a energy transmission buildout. To learn more about the company and its ERM program, a 2021 RIMS Award of Distinction honoree, RIMS sat down with Eversource Energy ERM Director **DENISE COSENTINO**.



RIMS: Many ERM leaders have a tough time getting a seat at the table as a strategic leader. How did you earn yours?

Cosentino: Over time, we demonstrated the value we added to our capital investments. This translated into inclusion into other strategic initiatives, such as offshore wind and acquisitions.

RIMS: Looking over the history of Eversource Energy, the company wasn't branded as such until 2015, right around the time you became ERM director (Eversource was previously known as Northeast Utilities and composed of six main subsidiaries serving different regions, such as NSTAR Electric, Western Massachusetts Electric Company and Connecticut Light and Power Company). As you took charge, did the consolidation and rebranding make managing ERM more efficient?

Cosentino: It did. In many large organizations, departments sometimes operate in silos. I consider our program to be successful based on how we've structured things to embed risk management into the culture. The Eversource Risk Committee, for instance, comprises executives from across the company and is chaired by the CFO. Members include the CIO, the controller and chief accounting officer, and the heads of Internal Audit, Government Affairs & Community Relations and Energy Strategy and Policy Development. The presidents of three of our operating companies also are on the committee, as well as other high-level executives. We meet quarterly to discuss the status of our top enterprise risks, doing deep dives in at least one of them to possibly uncover a previously unidentified risk driver. Then, on at least an annual basis, I meet with our executive leadership team, which includes the CEO, COO, corporate secretary, general counsel, and other leaders. Separately, I meet with our Board of Trustees annually. The executive team and Board of Trustees asks risk-related questions about our top enterprise risks, as well as

our emerging risks. These are highly interactive discussions.

RIMS: What would you consider to be the backbone of the ERM program?

Cosentino: I'd say our annual risk identification and assessment process. We engage all levels of employees across the enterprise to assess each risk, based on likelihood and potential impact. We then work with our business risk liaisons to dig into apparent trends to identify the top enterprise risks. We cannot do everything ourselves, of course, and leverage other assurance functions for assistance, like insurance, internal audit and compliance. For example, we recognize insurance as a form of risk transfer and include insurance team members in our risk mitigation conversations to see if there are available insurance products we can leverage. We also leverage internal audit to validate our mitigation plans.

RIMS: Let's turn to the subject of sustainability, as it is a key pillar of Eversource Energy and an integral component of ESG (environment, social and governance). As in the past three years, ESG factors are expected to be front and center at public company annual meetings, given their growing importance to institutional investors, shareholders, customers, and other stakeholders. Is ESG part of the ERM program or the culture at Eversource?

Cosentino: ESG is a big deal for us, given (the politics in) our geographic market footprint. The states of New Hampshire, Massachusetts and Connecticut are all focused on clean energy. In Massachusetts, we have a utility-owned solar power facility that the state recently allowed us to expand from the current 70 megawatts to 200 megawatts statewide.

RIMS: How is the ERM program directly involved in the sustainability agenda?

Cosentino: My group provides input into the sustainability reports the company files

each year. We have a risk section, where we talk about the risks associated with climate change and sustainability. From an operational standpoint, we consider the uptick in the frequency and severity of storms occurring in a particular service territory. While we don't normally experience full hurricanes across the three states, we do get some bad windstorm events that cause significant damage and flooding events.

RIMS: Are there any risk mitigation efforts put forward in these regards?

Cosentino: Yes. A great example is in Boston where we built a new substation on a platform, recognizing the possibility that the water levels will likely rise in 20 years. We purposely designed it to be above the flood plain. In other words, if the flood maps tell us one thing, we then add to [that height] to account for the potential of rising sea levels.

RIMS: Are there any other ways you have integrated ERM into aspects of Eversource's strategy and operations?

Cosentino: You mentioned the proxy season coming up, and we have a section on ERM in the proxy statement. We also have an ESG committee on the board. Many public companies have different board committees looking at the E or the S or the G, but we're one of the few that has a full standing committee focused on ESG. Another area we get involved in is our 10K annual report. My group studies the previous 10Ks of comparative utilities to see what they've disclosed as emerging risks. We then analyze our risks to ensure they track the emerging trend. We also do a study of what we're currently reporting to make sure it addresses what we should be reporting in the future.

RIMS: From everything you've said, ERM appears to be woven into every fiber of the company. Is it farfetched to conclude that every employee is effectively a risk manager?

Cosentino: That's not farfetched at all; it's the reality. We encourage all employees,



more than 9,000 in all, to understand what ERM is and the strategic role we perform. We recently developed an e-learning module, where employees will learn about our ERM structure and processes and their role in risk management.

RIMS: In your speech accepting the RIMS Award of Distinction, you thanked your fellow ERM professionals, mentioning that you belonged to several risk management benchmarking groups. How has this been helpful to you?

Cosentino: I can't say enough about the importance of risk-sharing opportunities. I belong to a few informal and formal benchmarking groups, including one whose members include the ERM leaders at Pepsi, IBM and several utilities. We share what we're doing, where we're having problems and how we overcame them, learning from each other's examples.

RIMS: Is there a particular lesson you learned that you could share?

Cosentino: One member of a benchmarking group talked about the correlations between top enterprise risks, insofar as how one risk might influence another risk. For example, a risk like a cyberattack—something every utility confronts—can adversely influence customer satisfaction, the laws and regulations governing utilities, our financial picture and stock value. We now have a top risk correlation exercise we do to make sure we identify and assess these possible influencing factors. It's just another example of how an ERM program is never static; it constantly evolves. **R**

Russ Banham is a veteran business journalist who frequently covers risk management topics.

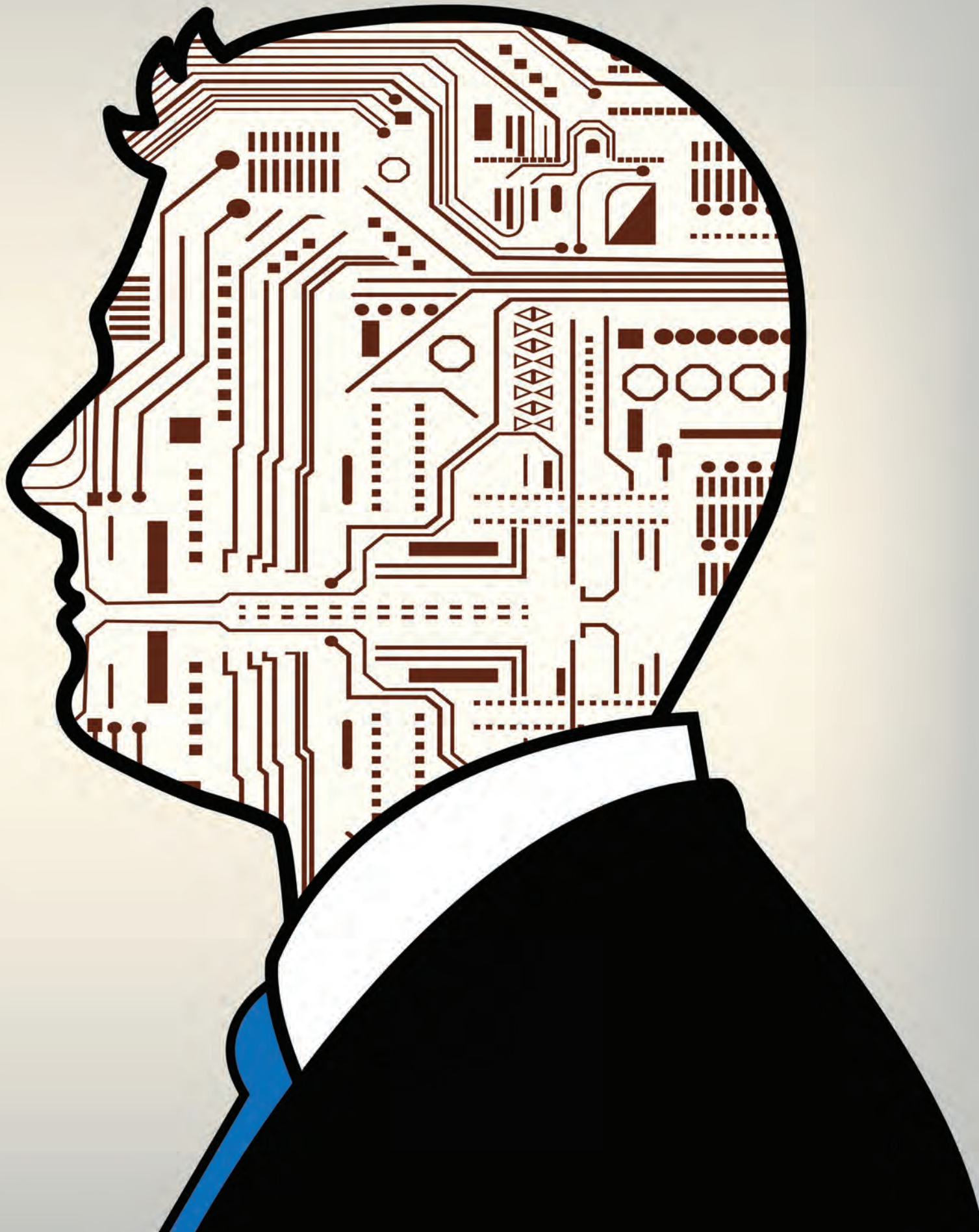
THE Evolution OF THE Risk Manager

Technology promises to alter the practice of risk management. Will these advances simply change how risk professionals work or create new, more strategic roles?

by Neil Hodge

AS ORGANIZATIONS RELY MORE HEAVILY ON advances in areas like artificial intelligence, data analytics and machine learning, the nature and focus of many professions will begin to shift. Risk management is no exception. As technology takes on more of the basic, process-driven work that makes up a large part of a risk professional's current workload, practitioners may be free to concentrate on more "value-adding" work and explore new or underdeveloped areas of risk management that have—until now—been relatively untapped. In this way, rather than posing a threat, artificial intelligence and machine learning may actually enable more sophisticated risk management, if used well.

According to Tom Bigham, risk advisory partner at Deloitte, the risk professional's role has already been undeniably impacted by new technologies, and it will continue to be molded as emerging technologies mature further. In fact, there is little other choice—evidence suggests that risk managers need to embrace artificial intelligence, machine learning and other technologies as a matter of course. In Deloitte's recent *Digital Risk Survey*, 60% of senior executives across over 160 global organizations rated the effec-



tiveness of current risk management tools as five (or less) out of 10—hardly a ringing endorsement of current capabilities.

Bigham said that the risk management departments “leading the way” are moving towards using technology to perform more basic, repetitive tasks. At the same time, they are also looking to improve these processes—for example, by ensuring that tasks are being completed with a greater level of accuracy, while also challenging existing processes to remove duplications and unnecessary layers of governance. In the near future, he believes, tasks such as manual controls testing (used to gain assurance on an annual basis) will become automated, and risk managers will use live dashboards to monitor to ensure tests are configured correctly.

However, over the longer-term, Bigham said, new technologies will help the role of the risk manager evolve into two camps: “engineers” and “thinkers.” As one would expect, the “engineers” are tech savvy. “Understanding the technologies allows these risk managers to ensure they are providing the right service to the organization and are aligned to their risk appetite,” he said. “Integrating the risk managers earlier in the development process (otherwise known as ‘shift to the left’) will ensure controls are considered at the right point in time, avoiding unnecessary delays later in the process.”

Meanwhile, “thinkers” will analyze their organization’s data by identifying patterns and rules, creating insights from which senior management can make decisions based on external events happening to their organization. “This allows risk managers to inform senior management of the potential impact of these events, and to introduce safeguards to prevent negative impact,” he said. “In addition, the risk manager’s expertise is required to ensure information and data collected from newly introduced tools is mapped to a common framework and combined to provide an overarching view to senior management.”

Many believe that new technology will not only change the future of risk management—it will also drive it. According to Arvind Govindarajan, partner at McKinsey & Company, a number of “structural trends” will impact the future of the risk function, including big data, analytics and digitization, and the growth of a number of emerging risk types, like cybersecurity. However, other factors will also play a defining role. For example, expectations from external customers and internal stakeholders for real-time, more granular and customized insights will affect the focus and work of risk managers, as will a continuous expansion in the breadth and depth of regulations. This is amplified by increased pressure on costs and competitive intensity, often from non-traditional players such as technology companies.

Govindarajan believes that the risk departments of the future will be “a high-intellect, highly automated nerve center.” In the future, advanced models and artificial intelligence will help assess emerging risks, early-warning signals and potential responses. “There will also be increased integration of risk management with other disciplines,” like business strategy, portfolio management and operations, he said. However, this movement will also create new risks

that risk managers must address—namely, the risk from increased use of models and digitization, and ensuring that risk professionals fully understand how these models work and what their capabilities (and limitations) are. Additionally, the increased reliance on data will require more focus on managing data risk, including data privacy, access and quality.

In the immediate term, “risk managers are going to have to check that the technologies they are relying on to enhance risk and management information actually work and deliver the assurance that they are supposed to,” said Fergus Allan, head of regulation and compliance at management consultancy TORI Global. Risk professionals will need to meet these new expectations, which means investing now in upskilling, training and recruitment.

In the long run, as technology takes on more of the analytical and processing tasks, risk professionals will be able to take a longer-term view of risks to the business, with the opportunity to focus more heavily on “horizon-scanning” for emerging risks that may impact the business in two or three years. “This will allow risk managers to think more strategically,” he said.

Allan believes that risk management will become more about “managing resilience”—ensuring that the business can cope with immediate shocks, such as natural catastrophes, power outages and supply chain failures, as well as more long-term disruptive risks, like those caused by new and more nimble challengers entering the market, new technologies, more stringent regulation and changing consumer sentiment.

“As technology takes on more of a risk manager’s current workload, risk managers will need to focus on more value-adding activities, and that includes the issues underpinning business strategy and the organization’s resilience,” Allan said. “The business environment is changing much more rapidly now, and companies can only rely on brand loyalty if their products and services are better than their rivals and affordably priced—not necessarily because they are the most established or dominant in the market. Risk managers need to concentrate on how the organiza-


FEATURE

tion can sustain itself in an environment that is more competitive, more highly regulated, and where ‘shocks’ can take place more frequently than before. As a result, it is obvious that risk managers need to be more engaged in reviewing risks around strategy and organizational resilience.”

Rob Clyde, immediate past chair of ISACA and director at data protection software firm Titus, agreed that there is a real need for risk managers to be more strategic. Indeed, he believes increased automation of the risk function will allow risk professionals more time and resources to engage in other activities where they could make a positive impact, and provide an opportunity for the profession to develop further.

“Risk functions need to move on from simply alerting management to risks, and they need to steer the organization toward getting the rewards from effective governance rather than just focusing on managing risks,” Clyde said. “They need to show that they understand the business, show how these risks will impact the bottom line, and show how opportunities can be leveraged from better risk management. Risk managers need to think about how they can make the strategy work even more effectively and drive more profitability. They need to think about how they can help the organization ‘win.’”

Clyde believes that risk managers will move away from some traditional priorities, such as crunching data, and will instead focus on new and emerging risk areas where artificial intelligence and other new technologies have not yet made the same degree of impact as data analytics. These include reviewing cyberrisk, data protection and data privacy risks, macroeconomic risks, and even the impact that misinformation on social media might have on the company’s reputation and bottom line.

ther experts, however, are less convinced that adoption of new technologies will change the underlying focus or approach of risk management. While they accept that the growth and accessibility of new technologies will have a positive impact on risk management, they say it does not necessarily follow that the profession’s priorities or usual tasks will change much. Instead, they believe that new technologies merely represent new risk tools that enable different ways of working on the same traditional areas, rather than revolutionizing what the function does.

Increased automation largely means that risk functions can concentrate more effectively on what is typically their primary focus—operational risks. “We’re seeing from our member organizations that operational risk is increasingly becoming a concern for boards,” said Dr. Luke Carrivick, head of analytics and research at ORX, an operational risk association for banks, insurers and asset managers. “Whereas 10 years ago credit and market risk dominated institutional risk profiles, boards today are far more focused on their operational risk exposure—for example, their highly valuable digital assets and how resilient they really are to events such as cyberattacks.”

According to Carrivick, “Boards don’t want to see endless reports showing what has happened previously. Instead, they want to know how their operational risk profile is changing as their strategy advances. Good data analytics is central to providing this forward-looking view.”

Michael Harris, director of financial crime compliance and regulation risk at LexisNexis Risk Solutions, is skeptical about technology’s role in shaping the future of the profession, particularly the idea that risk managers will somehow become more involved in corporate strategy. While technology may take a lot of the basic tasks away from risk management, it does not mean that risk professionals will take a more strategic role and become “risk leaders.” “Executives will still be ultimately responsible for strategy and risk—not risk managers,” he said.

The extent to which risk managers take on a more strategic role may depend on the industry vertical. “In heavily regulated industries such as financial services and pharmaceuticals, for example, there is still going to be a strong focus on compliance, despite what new technology can—and can’t—do,” Harris said. “As a result, boards in those industries will primarily want reassurance from risk management that operational risks are still being managed appropriately.”

As decision-making becomes more automated, Harris believes firms will face a greater need for assurance that the technology underpinning decision-making is working in the best interests of the company and its customers, and that it is compliant. “It will fall to risk managers to check that the processes that determine decision-making and produce management information are working properly,” he said. “This will mean that risk managers will need to understand the technology and its associated risks, and that will probably require retraining and upskilling. Over the past few years, risk, compliance and internal audit departments in financial services firms especially have grown due to increased regulatory demands and scrutiny. While these functions will likely cut staff as technology adoption becomes more prev-



As technology takes on more of the analytical and processing tasks, risk professionals will be able to take a longer-term view of risks to the business.

alent, it is probably fair to say that their roles will stay largely the same.”

Mike Hampson, CEO at Bishopsgate Financial Consulting, believes that “machines should do the ordinary so that the risk management function can do the extraordinary.” But the reality may be that “technology will simply free up risk managers to look at new areas of risk rather than change their role or the way the function works,” he said.

This may be because regulators shape risk management’s role more than technology or executives do. “Risk managers may want to play a more strategic and consultative role in their organizations, but more often than not, it is regulators that largely define what their areas of focus are going to be,” he said. “For example, in recent years, regulators—particularly in areas like financial services—have asked organizations to move away from just looking at financial risk and market risk to examine areas like operational resilience, systemic risk, macroeconomic risk, climate risk and data protection. Consequently, risk management functions have had to follow that lead, providing assurance on other, new

risk areas rather than trying to turn themselves into some kind of management consultancy.”

Despite the influence of new technology and compliance requirements, risk managers generally will need to become more commercially-minded and business savvy, Hampson said. This means being much more conscious about cost, competition and the wider macroeconomic environment—in effect, looking at external, market-driven risks to the business.

“At some level, risk managers need to think about rewards and not just risks,” he said. “Despite the cliché that there is no reward without risk, it is still true that most risk managers look at the risks inherent in business strategies, rather than look at the predicted rewards associated with them. This needs to change. Risk managers need to be more prepared to question whether the strategy is the best option and, if so, whether it can be tweaked or improved to deliver even better returns.”

There is little doubt that technology will impact the future role and work of risk professionals, but how this technology is ultimately implemented will still depend on what the board—and regulators—deem to be priority areas. Even if developments like artificial intelligence prove merely to be tools to enable risk managers to do their current work more effectively, rather than empowering them to explore new areas to add value, expectations about what the risk function can and should deliver are also changing. Regardless of technology’s potential uses, risk professionals will need to be more sensitive to how the business operates and where the organization can take advantage of commercial opportunities. **R**

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

Managing **DATA SECURITY RISKS** of AI Technology

by Neil Hodge

In recent months, artificial intelligence has generated widespread interest and conversation as tools like ChatGPT demonstrate a wide range of personal and professional applications. Perhaps equally important to this discussion, however, is an understanding of the risks posed by AI technology, including the significant data security threats that are already having unintended consequences for companies.



With current AI technology, users can input more data than ever before and use that information to learn patterns of behavior; uncover and predict future trends; and create and emulate works, sounds and images quickly and efficiently. While this can have many beneficial applications for organizations, experts warn that data exposure, loss of intellectual property and other data security risks will all increase exponentially.

These threats have already been materializing. In March, Samsung found out the hard way how easily employees acting in good faith can inadvertently breach company confidentiality and compromise its intellectual property by using third-party AI tools. In three separate incidents in the space of a month, employees unwittingly leaked sensitive company information when they tried to use ChatGPT to solve work-related problems. One employee asked ChatGPT to optimize test sequences for identifying faults in chips, which is a confidential process. Looking for help to write a presentation, another employee entered meeting notes into ChatGPT, putting confidential information for internal use into the public domain. Employees also pasted sensitive, bug-ridden source code from the company's semiconductor database into ChatGPT in an attempt to improve it.

The problem with asking ChatGPT or other public AI-based platforms to assist with fixing such issues is that the information that is put in becomes training data for the platform's large language model (LLM). And since ChatGPT retains data users input to further train itself, Samsung's trade secrets and intellectual property were effectively put into the hands of the platform's parent company, OpenAI.

Although OpenAI later acknowledged that it was possible for an organization to retrieve such information, the key takeaway from this self-inflicted breach is that proprietary information should never be pasted into ChatGPT or any other LLM-based services. Further, companies should ask any third-party AI provider what happens to the data inputs and outputs from any queries or prompts its employees enter.

DEVELOPING POLICIES FOR AI USE

Such mistakes have forced companies to reconsider who in the organization should have access to AI tools and for what purpose. Samsung's response has been to restrict employee usage of the tool to such low-volume data inputs that it is unlikely another security blunder of a similar magnitude could occur. Several other large companies including Amazon, Apple and Verizon have banned employees from using ChatGPT, while Wall Street giants JPMorgan Chase, Bank of America and Citigroup have also curtailed its use.

But banning or restricting the use of such prevalent and easy-to-use solutions can lead to other problems. "The issue with this response is that some employees are going to use LLMs in the workplace regardless of a company policy that bans them," said Greg Hatcher, co-founder of cybersecurity consultancy White Knight Labs. "LLMs make employees exponentially more productive, and productivity is directly correlated to compensation in the workplace. Companies have been battling shadow IT for 20 years—we do not want a 'rinse and repeat' situation with LLMs becoming shadow AI."

The best way forward is for companies to explicitly tell employees what constitutes acceptable and unacceptable AI use in the workplace. "Although we are relatively early in AI/LLM adoption, eventually there will be compliance and regulatory requirements around AI usage in sensitive environments where privacy is critical," he said. "We are just not there yet."

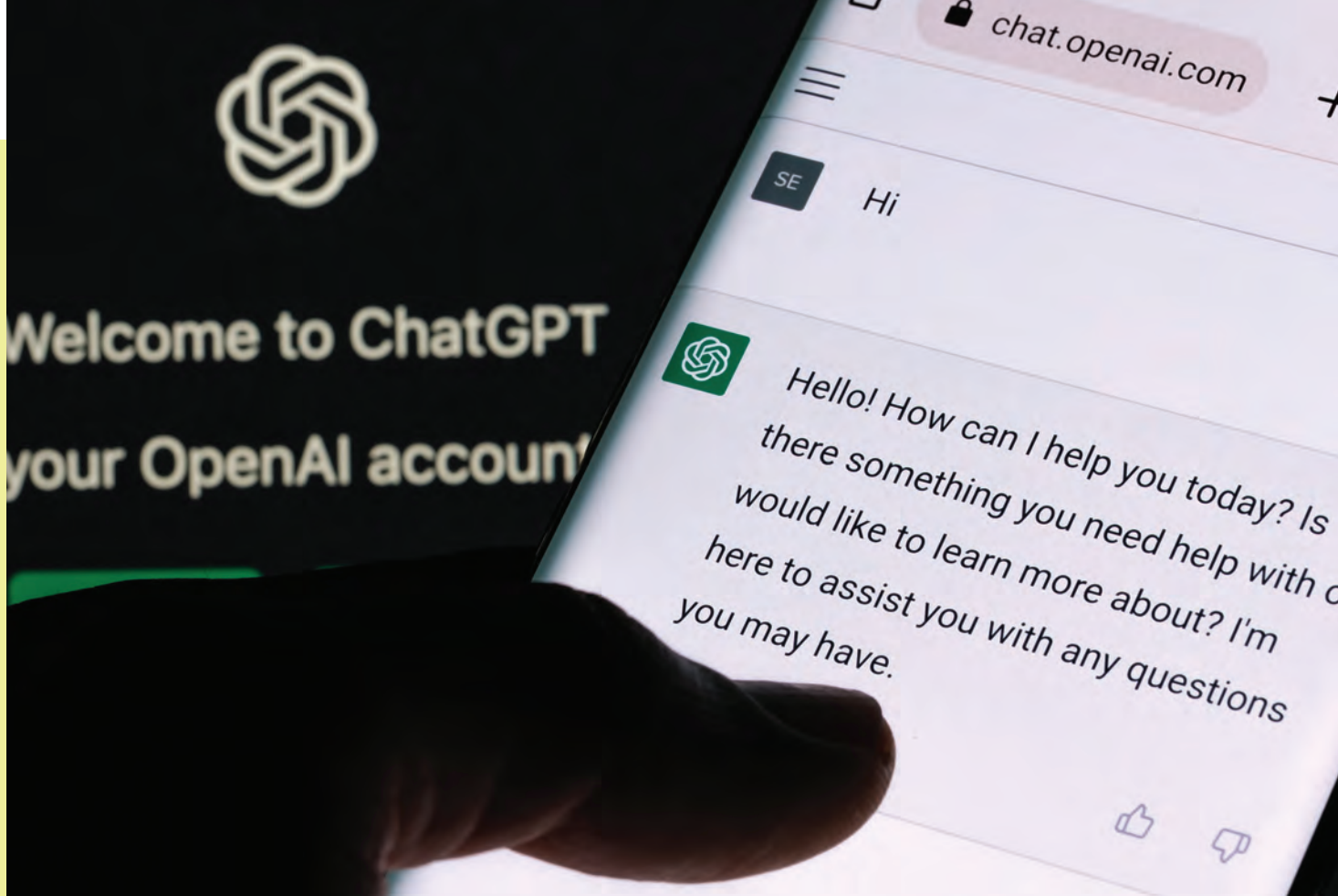
Moving forward, experts believe it is essential to raise employee risk awareness through training. According to Kevin Curran, professor of cybersecurity at Ulster University, senior management needs to prioritize security training for each level of employee. "All training should provide real-world examples and case studies that employees can relate to, showcasing the impact of security practices on their work," he said. "It is important to encourage employees' continuous education and for organizations to provide regular opportunities for staff to stay updated on emerging security threats and countermeasures. There should also be far more active participation in security initiatives, such as reporting suspicious activities and contributing to discussions or even offering suggestions for improving security measures."

It is also vital that companies develop and circulate an enterprise-wide policy on the use of AI technologies that prevents people from using such tools until they have been fully trained and made aware of the associated risks, said Dr. Clare Walsh, director of education at the Institute of Analytics.

She recommended companies establish clear rules on what can and cannot be entered into the tool, such as no personal data, nothing with commercial value to the company, and no systems code. All staff should also be required to state when any material has been produced by AI.

Another sensible precaution would be to sanction only "low-stakes" data requests, and to "advocate the use of these technologies only where the human requesting the output has the training and knowledge to supervise and check that the machine has produced something accurate," Walsh said. To that end, employees should be trained to look for simple anomalies in presentations, marketing material and other documents, such as outputs that do not make sense, are irrelevant or are factually inaccurate.

Both employers and employees have a duty to question how they use AI and whether they are using it securely, agreed Ed Williams, EMEA regional vice president of pentesting at cyber-



Many companies probably already have the governance and control infrastructure in place to address several key emerging AI risks—they just may not be aware of it.

security firm Trustwave. They should consider key issues such as: whether the AI model (including its infrastructure) is secure by design; what vulnerabilities it might have that could lead to possible data exposure or harmful outputs; and what measures can be put in place to ensure correct authentication and authorization, as well as appropriate logging and monitoring.

“Once both the business and employee have adequately answered these questions, it then becomes a question of risk acceptance or mitigation where possible, and consistent evaluation of employees’ skills, internal cybersecurity capabilities and threat detection going forward,” he said.

THE ROLE OF RISK MANAGEMENT

Risk managers have a key role to play in protecting companies from increasing cybersecurity and data risks introduced by AI. First, companies must conduct thorough risk assess-

ments. “Begin by evaluating the potential risks associated with AI technologies within the organization,” said Rom Hendler, CEO and co-founder of cybersecurity firm Trustifi. “Identify the AI systems in use, the data they process, and the potential threat vectors. Assess the existing security measures and identify gaps that need to be addressed.”

Another important step is to implement robust data governance by developing comprehensive policies and procedures to ensure the secure collection, storage and processing of data. Companies should encrypt sensitive data, implement access controls and regularly audit data handling practices. They should also promote a culture of security awareness, emphasizing best practices for data handling, recognizing social engineering techniques and reporting potential vulnerabilities. Data minimization strategies are also critical to reduce the potential impact of breaches. The more data a company has, the more data that can be stolen, potentially resulting in bigger ransomware demands and fines from data regulators around the world.

Establishing an AI data governance framework may not be

as difficult as it sounds. Many companies probably already have the governance and control infrastructure in place to address several key emerging AI risks—they just may not be aware of it. “Some key AI risks look very similar to already known cybersecurity risks and companies can calibrate their technical and organizational measures to account for variations on the theme,” said Brock Dahl, partner and head of U.S. fintech at law firm Freshfields.

He advised companies to build on current cybersecurity risk governance frameworks while continuing to ensure they remain flexible and adaptable. Organizations should question whether the use of new technology is integral to their assets

and activities and if there are any features of this technology that present familiar governance challenges, or introduce new ones.

“In the age of rapid innovation, the key is not simply to keep pace with each new development, but to take a step back and ensure the organization’s risk management architecture is geared toward absorbing constant flux,” he said. “There will be surprises, but the goal of the risk management enterprise is to create a robust mitigation capability for when those surprises emerge, while also limiting surprise to the greatest degree possible.”

However, risk managers need to be aware of other risks that

In the age of rapid innovation, the key is not simply to keep pace with each new development, but to take a step back and ensure the organization’s risk management architecture is geared toward absorbing constant flux.



may be more unique to AI. For example, in inversion attacks, hackers try to determine personal information about a data subject by poring through the outputs of a machine learning model. In data poisoning cases, malicious actors input incorrect information to skew results. Even if the necessary controls look similar to existing governance measures, these risks will require specialized mitigation approaches.

It is also critical to monitor the development of AI, data and cybersecurity regulation. Since the use of chatbots in business is still relatively new, current rules can be vague.

“We are seeing steps toward AI-specific legislation in various jurisdictions around the world,” said Sarah Pearce, partner at law firm Hunton Andrews Kurth. “By far the most advanced of these is the European Union’s AI Act, which is going through its final phases before coming into force. Certain aspects of the proposed legislation will undoubtedly require clarification in due course. The definition of AI itself, for example, will likely pose issues as to interpretation and, ultimately, in identifying which technologies are subject to the act’s requirements.”

Risk managers should make a dedicated effort to foster collaboration across the organization, engaging cybersecurity experts, AI specialists, and legal and compliance teams so there is a shared understanding of AI-related risks and appropriate safeguards. According to David L. Schwed, cybersecurity professor and practitioner-in-residence at Yeshiva University’s Katz School of Science and Health, risk managers should align themselves with cybersecurity professionals who understand these unique attack vectors to establish strong controls. “Controls that were good enough last week may not be good enough this week,” he said. “Given the advancement of AI-related and broader cyber risks, the ‘rinse-and-repeat’ mindset will not work in this new world.”

FOCUSING ON BETTER DATA SECURITY

Some experts believe the increased cyberrisk is not the fault of AI—it is because of poor risk management. According to Richard Bird, chief security officer at AI security firm Traceable, the increased exposure is due “in no small part” to the fact that companies have been mishandling data and IT security for years. Trying to embrace AI technologies at an enterprise-wide scale has just exposed the weaknesses further.

“It is not time to integrate AI into every aspect of any enterprise’s workflow for one very simple—yet very obviously overlooked—reason: No one has taken the time to figure out the operational, functional and corporate changes necessary to consume, leverage and optimize their uses of AI,” he said.

“Our operational workflows have been conditioned to



direct human interaction for centuries,” Bird explained. “A simple ‘rip and replace’ approach to implementing AI is going to lead to a massive outbreak of unintentional consequences. Large and medium-sized enterprises are rigid, inflexible institutions when it comes to change, compounded by the problems of corporate politics, budget restrictions and shareholder liabilities. Simply dropping AI into the mix is going to result in a lot of avoidable pain and failure.”

Bird added, “When it comes to security, it is clear that most companies are in much worse condition to mitigate the risks of their corporate and customer data being stolen or leaked than they were just six months ago.” This is because most companies were already struggling to keep their data safe before the rise of generative AI. The ease with which employees can take advantage of the technology and the lack of adequate security controls around it have further increased the risk to companies.

AI technology is evolving quickly. Organizations and risk professionals need to act fast to understand AI risks and ensure that they not only have the appropriate controls in place, but that their risk governance frameworks are flexible enough to adapt as new threats emerge. Anything less may put valuable company data at risk. **R**

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

O K H D V

O Z N K H V O

DON'T

PANIC

EEEE

EEEE

EEEE

EEEE

EEEE

EEEE

EEEE

EEEE

Eye of the Beholder

Understanding
the Psychology
of Risk Perception
to Improve
Risk Management

by John J. Brown
Illustration by
John W. Tomac

INDIVIDUALS PERCEIVE RISKS IN MARKEDLY different ways. One person may consider a risk to be critical, while another could consider it inconsequential. Often rooted in psychology, these differences in risk perception can create challenges for risk management professionals, especially when designing and implementing an effective risk management program. After all, if the program is focused on the wrong risks from the outset, the consequences to the organization could be dire. It is therefore critical for risk professionals to understand the psychological aspects of risk perception and develop techniques to address the resulting challenges.

The Effect of Heuristics and Biases

Our reaction to risks can be traced to early humans who were either the hunter or the hunted, and responded to danger by fighting or fleeing. Our ancestors' survival depended on responding quickly and correctly. A part of the brain—the amygdala—helped humanity's survival by bypassing cognitive processes and initiating immediate responses. Today, however, we generally have the time to obtain information, analyze risks and develop a reasoned response. Yet we still seem to let our innate reactive-mode override our cognitive thinking.

Many factors impair our ability to develop an accurate assessment of risks. Chief among these are heuristics and biases, which

can overtake reasoned analyses and decisions. Heuristics are practical problem-solving methods that serve as shortcuts in our cognitive thinking, influenced by our life experiences. Heuristics are important to consider because they may cause us to arrive at erroneous conclusions. Instead of stepping from A to B to C to D, heuristics allow us to jump directly from A to D. If the current situation is aligned to the foundation of our heuristic, this is good because the heuristic saves us time. However, if information in steps B or C indicate a different path, jumping from A to D can result in a completely different and wrong conclusion.

Biases impact heuristic thought processes and have a major impact on how we identify, analyze and evaluate risks. Important biases in risk perception include:

Anchoring bias. Our thinking is influenced by the first relevant data point we encounter when considering any situation. For example, if we are purchasing a used vehicle, the first person to offer a price establishes a range of reasonable prices in everyone's minds, anchored around the first stated value.

Availability bias. People tend to make judgments and decisions based on new, recent or dramatic information. Our memories fade quickly and the significance of what happened two years ago pales in contrast with what we read in daily—or hourly—news feeds. In our always-on social media lives, the dual effect of availability and anchoring poses a dangerous combination. Early reports of events can be fraught with inaccuracies, which are generally corrected later. The anchoring effect of the early news, however, can overpower the later, accurate—and perhaps less dramatic—information.

Confirmation bias. People also tend to believe information that supports our position or preconceptions and discount other data, regardless of how accurate or relevant it is. In his book *The Black Swan*, Nassim Nicholas Taleb noted, “We will tend to more easily remember those facts from our past that fit a narrative, while we tend to neglect others that do not appear to play a causal role.”

Conservatism bias. Unlike the availability bias, we may also tend to discount new data or evidence in favor of knowledge we have obtained over time. Consumer companies, for example, are often slow to recognize and adapt to changing consumer preferences.

Information bias. Many individuals and organizations seek more and more information about a situation even though the additional information will not affect decisions on how to act or react.

Other Factors Influencing Risk Perception

In addition to biases, a number of other factors also affect the way we perceive and deal with risks. One of the most important is experience and familiarity. If we do not have first-hand knowledge of a risk, we tend to discount both the likelihood that it will materi-

If a risk survey or other risk identification process is conducted at roughly the same time every year, results will skew risks to those that are most front-of-mind at that time.

alize and its possible consequences. This factor is two-sided: On one hand, having direct experience with a risk makes it seem more likely; on the other hand, constant exposure to a risk makes it so familiar that we often discount the consequences, perhaps because we have adapted to living with it.

Another factor is time relevancy. We tend to magnify the importance of risks that have occurred recently, compared to risks that have not occurred for some time. For example, after the September 11 terrorist attacks, aviation safety and security was paramount, and significant measures were implemented to secure air travel that remain in place to this day. Terrorists are just as likely, if not more so, to attack other modes of transportation or public gathering locations such as shopping malls and sports venues, however.

Control also impacts risk perception. People tend to discount risks if they feel in control of the situations exposing them to those risks. As David Ropeik points out in his book *How Risky Is It, Really?*, we believe that it is safer to drive



than fly to a distant location, yet statistics show it is much more likely for a traveler to die in a traffic accident. A similar situation exists for the risk of being distracted using a mobile phone while driving: Hands-free technology is considered a viable risk reduction technique because the driver does not hold a physical handset while driving, yet research indicates that the real risk is the mental distraction of talking with someone and processing information not relevant to operating a vehicle.

Putting a face to a risk and its consequence also has an outsized effect on perception of a risk. Notice how the American Society for the Prevention of Cruelty to Animals (ASPCA) and humanitarian aid organizations use this to influence our contributions. Heart-wrenching images of neglected animals and malnourished children stir our emotions and drive us to donate.

Weighing downside risks versus benefits is another important consideration. When looking at the pros and cons of a deci-

sion and considering the risks, people often discount downside risk consequences in inverse proportion to the perceived upsides or benefits. The greater the upside, the more they discount the likelihood that the downside risk will occur. This phenomenon is evidenced in many failed acquisitions where the expected benefits never materialize.

Risks like automobile accidents and workplace safety incidents have rich historical data sets that lend themselves to mathematical modeling and projections of future occurrences. Advanced software can perform sophisticated calculations to estimate the “level of risk” based on likelihood and consequence curves. However, for many business-level risks, scant data exists to determine curves that realistically model likelihood and consequence. Yet many executives rely on calculated “value-at-risk” figures to make strategic and tactical business decisions. Running thousands of calculations using Monte Carlo techniques implies accuracy and validity, yet the inputs used for likelihood and consequence can be unrealistic.

Techniques to Compensate

Despite the seemingly insurmountable challenges to determine an accurate accounting of risks and risk levels, there are some relatively simple techniques that can be used to provide a counterbalance. Remember that risk management is a journey, and programs should improve over time. Incorporating one or more of the following techniques will help move toward more accurate risk identification, analysis and evaluation.

Use calibration exercises. In his book *The Failure of Risk Management*, Douglas Hubbard discusses using calibration exercises prior to a risk identification session to guide individuals’ estimates of risk likelihood and consequence. People are generally overconfident in their abilities, and calibration exercises provide a dose of reality. Subsequent risk identification and analyses are usually more realistic and accurate following calibration sessions.

Adjust likelihood and consequence scales. Many risk management programs determine risk levels by combining estimates of likelihood of occurrence and magnitude of consequence. Simple techniques like adding or multiplying the ratings together are often used, and then a scheme is derived to decide thresholds for risk significance. An observed shortcoming of this approach is that low-likelihood but high-consequence risks are overlooked. Yet it is precisely these risks that significantly harm organizations. A useful counterbalance is to place more weight on the consequence scale compared to the likelihood scale to maintain the visibility of lower-likelihood but higher-consequence risks.

Ask the same question multiple ways. As discussed earlier, heuristics and biases impact the way we perceive risks and risk levels. Our thought processes are affected by the wording and presentation of a question or scenario. Employing a technique that solicits information about potential risks using differing language or contexts can help detect variances in risk perception and guide follow-up work to determine more accurate information. Well-constructed risk surveys often employ this technique to great advantage.

Ask the same question of multiple people. Similar to asking

the same question multiple ways, presenting questions to multiple people highlights disparities in risk perception. Risk surveys can be sent to multiple people from different parts of an organization and the results analyzed to detect wide variances in risk perception. For example, higher up the leadership chain, views of risks tend to focus on longer-term strategic risks, while those in the lower- to mid-levels focus on more operational and tactical risks. Similarly, individuals in different functional areas will frequently view risks and risk levels differently based on their individual heuristics and biases. This does not mean one is right and the other wrong. Rather, it highlights the necessity and usefulness of considering multiple factors in identifying significant risks.

Ask the same question at different times. Current events and work issues affect thought processes. If a risk survey or other risk identification process is conducted at roughly the same time every year, results will skew risks to those that are most front-of-mind at that time. For example, if risk assessments are conducted around strategic planning time, longer-term strategic risks will appear more important. If assessments are conducted during heavy manufacturing periods, such as an inventory build-up for holiday sales, manufacturing capacity and supply chain risks will seem more important. To counter these tendencies, conduct risk assessments at varying times during the year.

Ensure the risk management process is continuous. Risks are dynamic and a risk management program should be as well. Building on the technique above, multiple risk identification processes and frequencies should be used and should be time-independent. Emerging risks do not wait for regularly scheduled risk assessment workshops. Use multiple risk sensing platforms to identify new risks and detect the onset of a known risk. Well-defined risk indicators accompanied by robust data acquisition and analytics are useful for this purpose. Every organization has a unique operating structure and rhythm, and risk management processes benefit by aligning to these. Maintaining a real-time or near-time focus on risks and risk treatment helps limit the potential that a critical risk is missed or not addressed.

Use technology to help. Technology solutions are valuable in managing risk information, acquiring and analyzing risk data, and automating information flows and decisions. A key benefit is the ability to remove psychological and emotional influences in processing risk data. Advances in artificial intelligence and data analytics can provide cost effective and valuable insight into risk environments and emerging risks. And risk management software platforms can aggregate risks, automate risk assessments, and track risk treatment actions.

Developing, implementing and evolving a risk management program is challenging at best. Psychological influences on risk perception can negatively impact the validity and focus of risk mitigation measures included in a program. Understanding these influences and integrating methods to compensate for them can substantially improve the effectiveness and value of any risk management initiative. ■

John J. Brown is managing consultant of enterprise risk management solutions at Guidehouse.



How to Measure Risk Capacity for Strategic Initiatives

By Johan Nystedt

Enterprise risk management is evolving into holistic risk portfolio management. This means eliminating unwanted risks to create room for smart risk-taking on high-return strategic business initiatives. Managing risk on a holistic level poses challenging questions, including:

- What is our organization's risk capacity?
- How do we assess how much aggregate risk-taking is prudent?
- What if our risk tolerance requires a cash buffer for unexpected cash flow surprises?

The answers to these questions depend on understanding your organization's risk capacity and risk tolerance.

A TOP-DOWN APPROACH TO ESTIMATING RISK CAPACITY

Estimating your company's risk capacity does not have to be a daunting exercise. The principles are fairly straight-forward. It is often better to keep the analysis relatively quick and simple, versus engaging in overly complex approaches that take a long time to develop and may thus be irrelevant by the time an initiative is launched. Also, understanding the relative value of competing initiatives may often be more relevant to decision-making than focusing on the precise valuation of each initiative by itself.

STEP 1: Identify critical financial metrics thresholds

An organization's risk capacity is typically constrained by specific thresholds, such as commitments to minimum corporate credit ratings or compliance with financial debt covenants. The objective is to identify and determine such critical thresholds, typically over the medium-term horizon (e.g., maximum financial leverage for each of the next eight quarters).

For example, credit rating agencies provide issuer-specific reports that illustrate what financial metrics would put upward or downward pressure on assigned credit ratings. For a company that is determined to stay within specific credit ratings or categories, such as investment grade (defined as Baa3/BBB- or better), the minimum threshold would be defined as the financial metrics that correspond to such minimum ratings. Two common financial metrics in this context are leverage ratios and coverage ratios, which are based on debt, EBITDA and interest rate expense.

STEP 2: Determine historical financial metrics fluctuations

Once critical financial metrics have been determined, the next step is to estimate future uncertainties in projections for these metrics (referred to as "fluctuations"). One common approach to estimate future expected fluctuations is to measure the variability in historical financial statement data.

For example, let's say that debt and EBITDA represent the most applicable financial metrics to stay within an identified critical leverage threshold. To assess the likelihood that we comfortably reside within such a leverage threshold, we need to determine reasonable fluctuations of debt and EBITDA over the forecasting horizon. Historic fluctuations in debt and EBITDA would be a starting point to estimate future variability in such financial metrics. When performing this historical analysis of past variability, companies often chose to "adjust" historic data to eliminate the effect of impacts that are unlikely to have any bearing on future results. This includes one-time items or outlier events that are stripped out of reported financials to improve the relevance for forecasting future fluctuations.

STEP 3: Build the base case scenario and evaluate strategic initiatives

Having identified critical financial metrics and related thresholds and having estimated future reasonable fluctuations around projections of these metrics, we can now build the base case stochastic model of our business results. This stochastic model leverages our estimated variability of future financial metrics, thus providing reasonable distributions of future results around the conventional "point estimations" of projections. This base case represents the business as is (i.e., without accounting for contemplated strategic initiatives).

We can construct our base case stochastic model by applying estimated fluctuations to financial projections. This is done to assess the likelihood of complying with the previously identified thresholds. Building on this base case, we can evaluate various, perhaps competing, strategic initiatives, such as M&A or business transformations, by overlaying scenarios on top of the previously discussed base case.

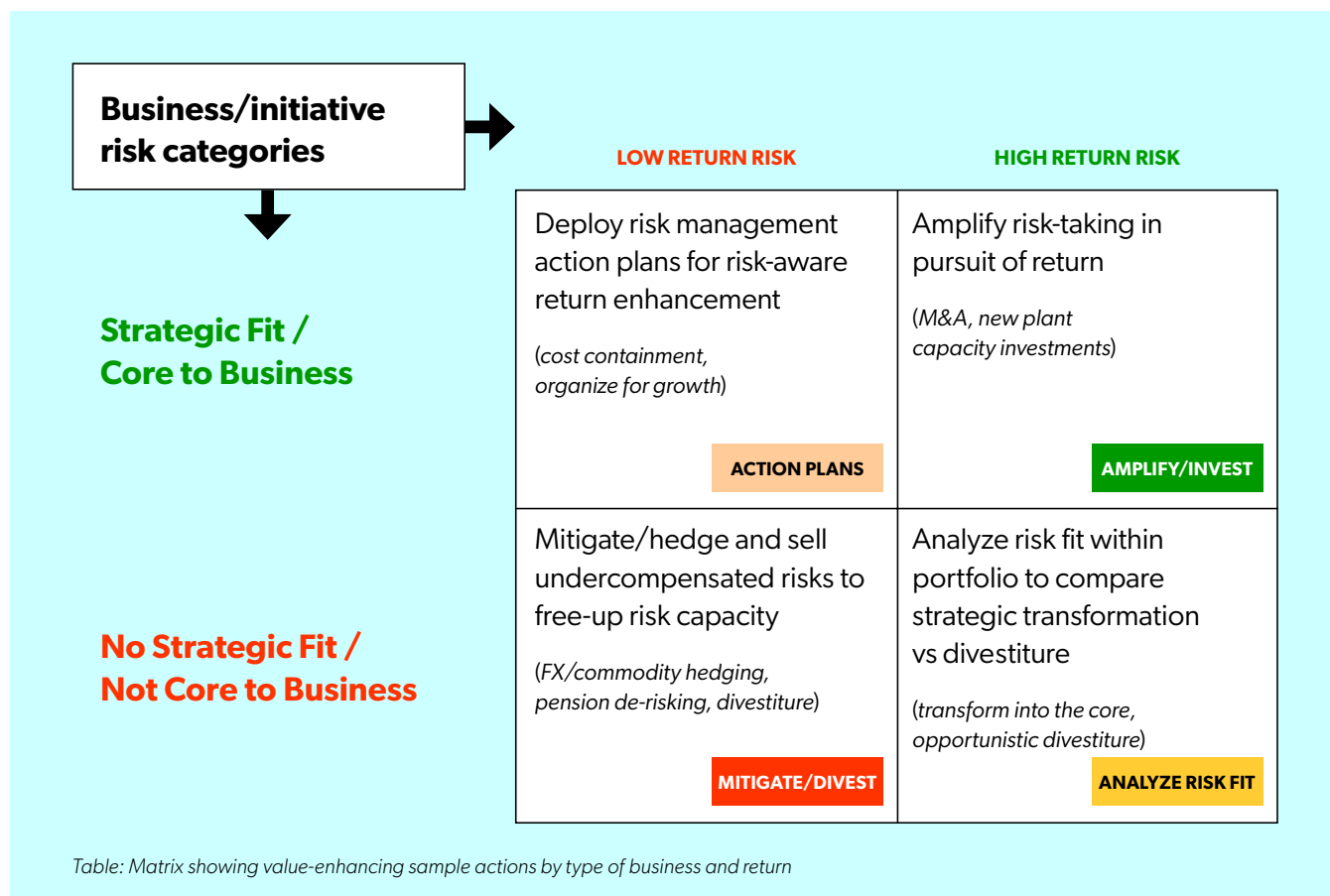
This is a valuable tool for CEOs and CFOs seeking to better deal with M&A auctions, where potential acquirers often must act extremely quickly to provide new bids for in-play companies. Thus, the likelihood of the so-called "winner's curse" can be reduced. Instead, informed decision-making in time-sensitive situations relieves stress on decision-makers.

CREATING RISK CAPACITY FOR STRATEGIC INITIATIVES

When there is time to plan for strategic initiatives, multiple contingency scenarios can be built on top of the base case scenario to offer insights into what mitigating actions provide sufficient risk capacity room for strategic initiatives. Thus, if we do not like the odds, we can proactively free up room by eliminating existing risks. This is the essence of holistic risk management—looking at risk holistically across the organization and looking at the portfolio of risk as a whole.

The key here is to identify undercompensated risks that are not part of our core business to be eliminated. Foreign exchange and commodity exposure are frequent examples of risks that are non-core to most non-financial companies. Whereas such risks may be non-core to you, they may well be core to financial market players, and can thus be mitigated at low frictional costs.

After identifying risks to be eliminated, you can reassess the likely threshold compliance proforma for the subtraction of the unwanted risk. To account for unknown or unmodeled risks, or when risk tolerance concerns demand a more conservative approach to estimating risks, it is common to add a dollar risk buffer into the modeling. For instance, a company may want all scenario likelihood calculations to allow for an extra \$100 million surprise cash flow shortfall to compensate for unknown risk factors. This can be built into the model as an overlay scenario.



The table above shows a framework that can be used to conceptualize what type of actions to be considered for each risk type in an organization's risk portfolio. For example, for a risk that is both a strategic fit (top row) and provides a high return (right column), the focus is to amplify good risk taking in pursuit of return. If the opposite is true, we would seek to reduce risk taking in this category to free up risk capacity to make room for better endeavors.

In summary, by measuring an organization's base case risk capacity, and adding scenarios for strategic initiatives, we can

take smart risks while staying within our risk tolerance limits. When risk capacity space is not available, we can add room by eliminating or mitigating risks. The resulting adjusted risk portfolio may be conducive for prudent strategic risk taking in pursuit of risk-adjusted returns. [R](#)

Johan Nystedt is president and founder of Nystedt Enterprise Solutions LLC, and has managed risk for many companies including Conagra Brands (as the chief risk officer), Levi Strauss, RR Donnelley and Kraft Foods.



WE WANT YOU

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

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



**RISK
MANAGEMENT**