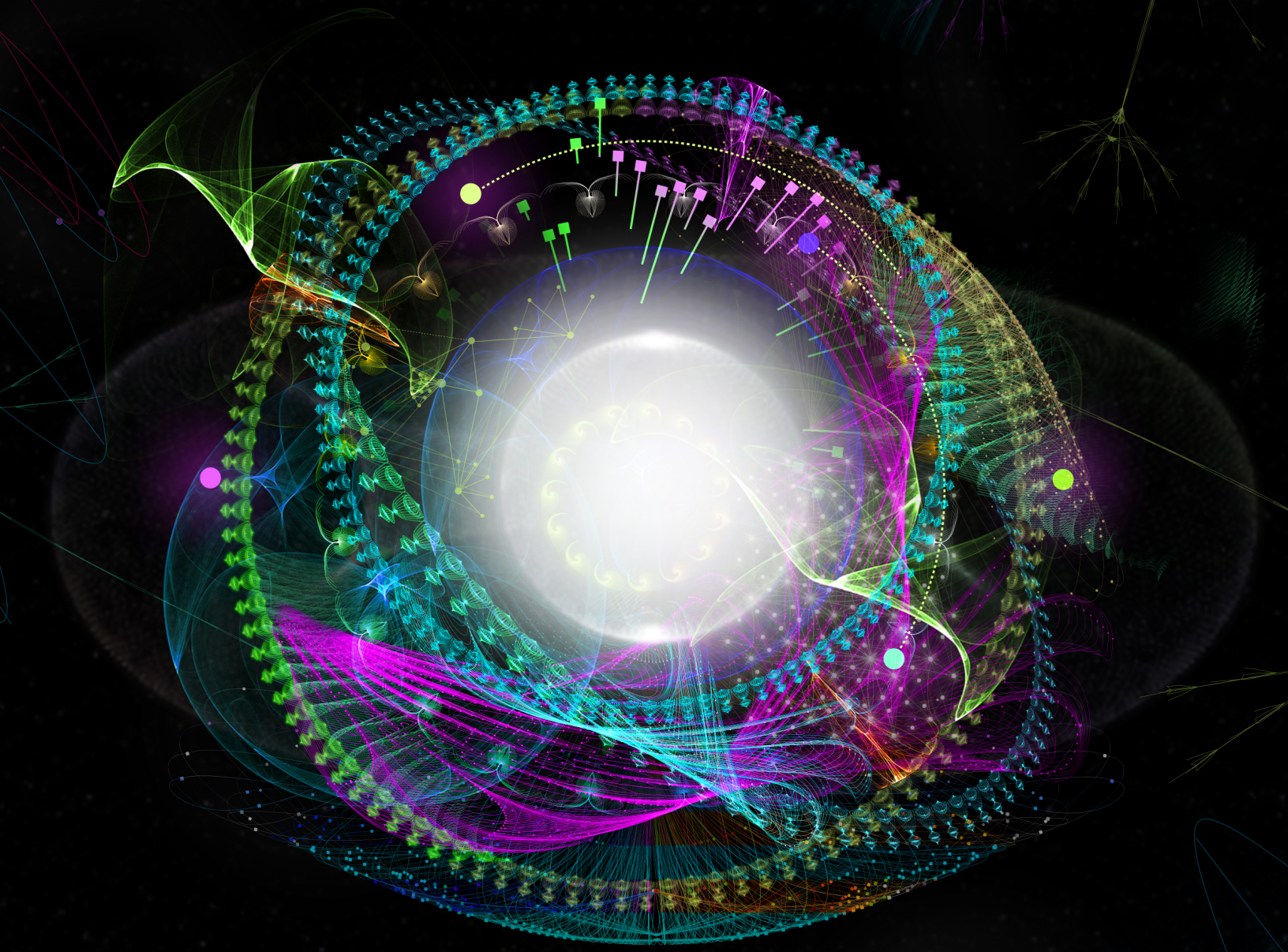
Deloitte.
Insights



Rebooting risk management

Making risk relevant in a world remade by COVID-19

Deloitte Risk & Financial Advisory

We don't believe that risk is simply managed—it is confronted. In Advisory, we do not take a defensive crouch. We move forward, defining the unknowns and framing the issues before you encounter them. Whether your challenge is cyber, transactional, regulatory, or internal controls, we can help prepare you to preempt the threat, define what's vital, and aggressively secure it. So that you can keep pace, get back to the business at hand—and move on what matters. To learn more, visit Deloitte.com.

Contents

Elevating business agility with risk management	2
The end of performative risk management	3
A failure of imagination	4
What is a risk reboot, anyway?	5
Elements of a risk reboot	6
Shape—or be shaped by—events	16
Endnotes	20

Elevating business agility with risk management

BLANKET STATEMENTS ABOUT the impact of the coronavirus pandemic and its economic fallout may be viewed skeptically. But this much we can say: Risk management failures abounded. Indeed, regardless of how your organization has been affected, there is much to be learned about risk management from this still-unfolding crisis.

Even after the past 20 years of continual disruption, risk management is too often either misunderstood or mistakenly thought of as a compliance function. Too many executives make it only about loss prevention. Too many see the chief risk officer, chief compliance officer, chief information security officer, or other risk leader as a dotter of I's and crosser of T's—or as someone who is just going to tell them why they shouldn't do something. Organizations have invested untold sums in response to major risk events, yet have left themselves exposed to the next one.

Most compliance regimes may work well for known risks with clear implications and proven mitigations in a fairly static environment. But as COVID-19 has demonstrated, the environment is anything but static. Risk is not a well-behaved house guest and the impact of COVID-19 was impossible to predict. Yet stakeholders, notably customers, investors, and regulators, will continue to hold management accountable for performance and results even when a risk event is unpredictable and unprecedented.

The chance to upgrade and reposition risk management is one of the true opportunities this crisis presents to risk leaders, executive teams, and organizations.

Risk is not a well-behaved house guest and the impact of COVID-19 was impossible to predict. Yet stakeholders, notably customers, investors, and regulators, will continue to hold management accountable for performance and results even when a risk event is unpredictable and unprecedented.

The end of performative risk management

PERMISSION TO SPEAK frankly? This crisis has revealed that much of the risk management that organizations engage in could be termed performative—that is, undertaken as an exercise rather than a strategic practice, as a means of providing comfort rather than challenge.

To some extent, we may be overstating to make a point. Actual risks are certainly being recognized and managed, and useful defenses are being deployed. Yet these steps rarely address the threats that could most surely devastate the organization. Even companies with relatively mature risk programs have essentially calibrated those programs to address well-known financial, operational, cyber, compliance, and legal risks. Those programs were not built to assist management in navigating low-probability, high-impact risk events.

Your risk function may be termed performative to the extent that it focuses on an audience rather than a result. Many risk functions perform for regulators. But regulators are concerned with known and measurable risks and tend to regulate to the previous crisis. Risk functions often perform for management and the board, assuring them that all risks have been identified and addressed. The risk function also may perform for itself, writing policies, setting up procedures, and designing controls—all necessary activities. In such cases, risk management fails to align with the business and management or to convert insights into actions that could mitigate risk and keep the strategy on course.

Actual risks are certainly being recognized and managed, and useful defenses are being deployed. Yet these steps rarely address the threats that could most surely devastate the organization.

This is, emphatically, not to say that risk leaders have not been doing their jobs and delivering on management expectations. It is to say that their jobs have typically been defined too narrowly and that management has set expectations too low.

Too narrowly and too low compared to what?

Compared to the risks posed by a global pandemic and its economic fallout, and by any future event of similar magnitude or impact.

A failure of imagination

WE HAVE CLEARLY entered a period of not only heightened risk, but of prolonged uncertainty. Every senior executive, board member, or risk leader whose organization has prospered in spite of, or even because of, this crisis should clearly understand: Next time will be different. As has been noted elsewhere, the volatile, uncertain, complex, ambiguous (VUCA)[1] environment virtually guarantees that the next crisis will not be any more predictable than any others have been during the past 20 years.

What if the next crisis is a technology one that wreaks havoc on digital assets and communication systems? Imagine the impact to accounting processes, trading platforms, telecom networks, electric grids, and defense systems.

A risk event need not be global to destroy a company, either. Imagine if your organization were targeted—with or without substantive reason—by a cadre of activists using sharp social media tools to shred the trust you have developed with your customers, employees, and investors. Do you understand all of the risks that possibility poses to your organization? Do you have an effective response that you can activate immediately?

Such events are worth imagining not just because it is appropriately humbling to do so, but because the shortcomings of risk management at the level we aim to discuss in this paper often begin with failures of imagination. This was recognized in 2004's *9/11 commission report*, which identified failure of imagination as a limiting factor in US national security policy and noted that "Imagination is not a gift usually associated with bureaucracies."[2] Anyone leading a large, complex organization knows that bureaucracies are hardly limited to government.

While it is impossible to predict crises of the order of 9/11 or COVID-19, management cannot simply throw its hands up. Stakeholders, including customers and investors, understand that new risks will emerge and expect management to have plans in place to address them. This is where risk management can add value, by sensing changes in the risk environment and providing an early warning system, thus buying time to plan a response. Risk also has a role to play in converting insight into action and activating change, even under—or especially under—conditions characterized by imperfect information.

Playbooks can connect risk management with the business by defining risk events that trigger contingency plans. Simulations can rehearse the team to help them be coordinated and ready. Although trying to identify all conceivable risks and risk events is futile, connecting an evolving risk profile with implications and actions can enable a transition from performative to results-oriented risk management. In fact, many senior leadership teams found themselves turning to the risk function for risk data, scenario planning, and risk-based decision support during this crisis simply because risk possessed those capabilities.

Meanwhile, risk management failures in the face of major events are rooted not in any specific element of risk management, a failure to pick up this signal or to secure that area. Rather, they arise from a lack of appreciation, at the top of the organization, of the role of risk management in today's disruptive environment. That lack of appreciation—and imagination—has led many organizations to apply 20th-century risk management to 21st-century risks.

What is a risk reboot, anyway?

WHAT DO WE mean by a risk reboot? Not a reboot in the reset-your-device or restart-the-system sense from the tech world. We mean it in the reboot-the-franchise sense from the moviemaking world. We mean reimagining, refreshing, and re-energizing risk management and all of its elements—compliance, cyber, enterprise, legal, strategic, internal audit, and more—to help address a highly uncertain future. The concrete outcome of this reboot is a risk leader's agenda and mandate—and a risk management function—geared to the critical risks the organization faces as it pursues its purpose, mission, strategy, and goals.

Here's why a risk reboot may be necessary for so many organizations at this time:

- Risk leaders—the CRO, CLO, CAE, and CCO, among others—too often lack the organizational clout, executive support, and access to intelligence needed to do their jobs effectively.

- Organizations must comply with a glut of externally and internally mandated policies and procedures that, over time, generate a complex and expensive maze of rules to comply with and report on. This creates organizations that are too bureaucratic to anticipate and respond to the threats that matter most.

- This, in turn, generates a system in which much of risk management is structured for irrelevance at best and failure at worst. This is particularly so during periods of uncertainty, but it can even occur with respect to well-known risks: for example, when the CISO cannot articulate the likely business impact of a potential cyber breach for the executive team.

- Equally important, extremely few organizations have calculated either the cost of risk management and compliance or the value that those activities deliver. This invariably reduces risk management to the status of cost center when it actually—when properly positioned and resourced—is a function that should partner with management on ways to understand the business environment, weigh strategic options, and deliver value to stakeholders.

- A risk reboot can—based on an organization's industry, needs, and capabilities—position the risk leader and risk management function to provide essential assistance and decision support to the executive team, board, and business managers under conditions of ongoing uncertainty. It can also help eliminate useless, redundant, and low-value risk management activities. At its best, it should promulgate risk management across the enterprise and drive it into the organization's culture. A reboot accomplishes this by appropriately updating the risk leader's mandate and the organization's capabilities in ways that serve internal and external stakeholders in our extremely uncertain environment.

In short, a well-conceived and properly implemented risk reboot positions the organization to thrive going forward, as this crisis continues and after it is ultimately resolved. Blurring the lines between business-as-usual risk management, crisis management, and resilience can enable the organization to continuously hone strategic, financial, and operational agility, as well as actual risk management. By the same token, failure to seize this moment may undermine an organization's ability to thrive as the current crisis continues and future crises emerge.

Elements of a risk reboot

THE SPECIFICS OF a risk reboot are too numerous to address in this publication, as they will vary with an organization's industry, needs, risks, and capabilities. However, three guiding principles can ignite a risk reboot and help guide it in productive directions. Those principles are to:

- Build trust among stakeholders
- Elevate the role of risk management
- Generate and disseminate risk intelligence

Building trust among stakeholders

Cultivating stakeholders' trust requires risk leaders to think more broadly and deeply about the organization's ecosystem of stakeholders. Every group of stakeholders is, in its own way, critical to an organization's success. Further, they are now far more connected and aware of one another by means such as the internet and social media, and they are much more interrelated than in the past. In such an environment, what affects one stakeholder has the potential to affect many more.

Relevant risk programs are designed around the needs and expectations of *all* stakeholders—customers, employees, the board, vendors, partners, investors, the media, the community, and society at large. Relevant programs also focus most on risks that could undermine the organization's ability to meet those needs and fulfill those expectations, or undermine stakeholders' confidence in that ability.

Viewing stakeholders more broadly and deeply positions a risk leader to:

- Identify all groups in the organization's ecosystem of stakeholders and their relationships; not only with the organization, but among one another
- Articulate what each stakeholder group specifically needs and expects from the organization
- Understand the full range of risks that could undermine the organization's ability to fulfill each group's needs and meet their expectations
- Grasp the interrelatedness of stakeholder expectations and the ways that stakeholder groups affect one another, and understand the interrelatedness of the associated risks
- Challenge management on potential flaws in a strategy, errors in execution, and areas where the organization might break, while pointing out potential opportunities, solutions, and fixes—with that second part key to avoid being viewed as a naysayer
- Make sure their program proactively monitors, mitigates, and manages risks that could affect the organization's ability to deliver on stakeholder expectations as well as trust and confidence among key stakeholder groups

The resulting risk program should possess innate relevance because it focuses on preserving the trust that exists between the organization and its stakeholders. The program thus enables management to consider decisions and initiatives,

as well as risks, more holistically. It also enables the risk function, management, and the board to locate opportunities to increase trust, which itself has tremendous value (see sidebar, "Why stakeholders' trust matters").

The program thus enables management to consider decisions and initiatives, as well as risks, more holistically.

One example of an organization that has engaged stakeholders around risk is the specialty chemical company Clariant AG. In 2019, Clariant received a World Procurement Award 2019 for "Supplier Risk Management" as well as an EcoVadis Sustainable Procurement Leadership award for "Best Internal Stakeholder Engagement" program. In both cases, the awarding organizations highlighted Clariant's efforts to involve multiple internal and external stakeholders to deliver a more integrated supply chain process.[3] As part of this effort, Clariant began using artificial intelligence tools in 2017 to monitor supply chain disruptions, including fires and explosions, and to ensure that suppliers were financially stable and in compliance with regulations. The organization applies these tools across the full cycle of supply chain risk management, to identify risk, to understand the potential impact of each risk, and to work proactively with supply chain partners to mitigate it.[4] The organization emphasizes that risk management is not designed to stop people from taking risks but to help them to optimize the level of risk taken and to encourage entrepreneurial behavior.[5]

Identifying all stakeholders and their needs and expectations—and the risks to the organization's ability to meet them, now and going forward—presents an elegant yet comprehensive approach to initiating a risk reboot.

Useful questions to pose in considering stakeholders might include:

- Which internal and external groups inhabit our ecosystem of stakeholders? What are the needs and expectations of each group?
- What strategic, financial, operational, cyber, regulatory, and other risks could compromise our ability to deliver on each of those needs and expectations?
- Which stakeholder groups did we continue to serve well during the current crisis? Which ones did we serve less well, or to some extent fail?
- Which of our organization's capabilities have enabled us to continue to deliver value to each group during this crisis? Which ones proved inadequate?
- How can we best balance and address the needs and expectations of each stakeholder group in the context of our risk program? What analytical, predictive, risk-sensing, and data-visualization capabilities do we need to invest in to accomplish this?

WHY STAKEHOLDERS' TRUST MATTERS

Many reasons exist for senior executives to prioritize building trust among stakeholders and to use stakeholders' needs and expectations as a starting point in rebooting risk:

- **Trust generates value.** Higher trust is associated with increased customer loyalty, employee engagement, and product quality, and theoretically with decreased fraud, waste, and abuse. In these ways, trust enhances financial performance, market valuation, and resilience. Trust also is closely tied to reputation, an asset that—once lost—is difficult to recover.[6]
- **Distrust increases costs.** By the same token, lack of trust invites increased regulatory scrutiny as well as reliance on complex contracts and expensive monitoring and enforcement mechanisms, particularly among suppliers and employees. It can also lead to litigation, employee turnover, lost customers, and reputational crises.
- **Trust has frayed.** In recent years, trust in institutions among stakeholder groups and the general public has plummeted to new lows. A widely respected 2020 study (conducted in late 2019) found that "despite a strong global economy and near full employment, none of the four societal institutions that the study measures—government, business, NGOs and media—is trusted."[7]
- **Trust has risen in importance.** In times of upheaval and uncertainty, stakeholders gravitate toward organizations they trust and move away from those they do not. A study related to the one quoted above found that 70% of respondents said that trusting a brand is more important today than in the past, and 81% cited personal vulnerability (around health, financial stability, and privacy) as a reason that brand trust has become more important.

When an organization and its stakeholders truly trust one another, they become partners in risk management, alerting one another to emerging risks, collaborating on mitigation, and creating greater value for each party. This has been demonstrated through mechanisms such as customer councils and preferred supplier programs, and among extended enterprise partners, in which key stakeholders are "brought into the organization" to enhance relationships and build trust.

LESSONS LEARNED: A CONVERSATION WITH A RISK LEADER IN FINANCIAL SERVICES

How would you say your organization's risk management practices have worked during this crisis?

Our preparation paid off. We had our business continuity plans in place before the pandemic, and recertified annually, so our operational processes remained effective. We had been increasing our data center's capacity to support our virtual private network (VPN) and ran tests with 30 or 40% of employees connecting from home. We reviewed those tests and added capacity as needed. Also, our third-party risk management program had been focused mainly on security, but over the last year we've extended it to financial, reputational, and other risk domains.

How did your business continuity plans work out?

Our business continuity plans had identified which people, processes, and technology would enable us to recover under different scenarios. For example, we needed to identify the people essential to a process and decide whether they have to be onsite. We didn't have that data before, but were able to develop it quickly. We had asked all plan owners to identify essential and nonessential processes and employees so we could get essential processes going before lower priority ones.

What kind of challenges did you face around access to data and communications?

Not so much around data, but around enabling our partners to produce their deliverables when they were not working from our offshore development center, which is our dedicated facility for third parties. Much of their staff comes into that center and connects through a dedicated VPN to our network, but some do not or could not in the first days. We addressed that challenge quickly so projects and deliverables were not impacted.

In what ways do you use scenarios in risk management?

We do scenario-based tabletop exercises for a number of our businesses. I am sure we will be including a pandemic in those exercises going forward. We've also been looking at scenarios that would influence our US locations. Every state has different stay-at-home orders and reopening plans, and the pace is variable and may affect our workforce. We currently have 97% of our employees working from home, and productivity hasn't been an issue, so we may not have to rush to bring people back into our offices.

How do you know that productivity hasn't been an issue?

We've done surveys of managers and we're seeing that projects and deliverables are on schedule. However, no decision has been made on continuing working from home. Senior leaders' main concern is employee health and safety. Some teams would miss the collaboration of working in the office, and management will do what works best for different teams.

Has this crisis revealed any areas that might benefit from improvement?

Our third parties mostly work out of a dedicated, secure development center. But some of those in Asia were among the first to send people home, so our teams scrambled to provide devices so that those parties could be certified to connect to our network. We also had to quickly make decisions about providing access to various data. This has taught us to be prepared and to ensure that our third parties have solid business continuity plans.

How have you been planning to thrive going forward, given the levels of ongoing uncertainty?

We want to be sure that work from home does not lead to loss events. So, we're watching operational trends and monitoring for increasing loss events. For example, we've seen very high call-center volume because of market volatility, with customers moving money between funds. That kind of volume could lead to loss events, and we monitor for that.

Has the relationship between the senior leadership and risk management changed during this crisis?

I see it as ever-evolving. Business continuity and third-party risk management are front and center. Everyone wants to be sure that the businesses have mitigation plans and that staff can perform at the same level. That's where management involvement has increased, with the monitoring and reviews of operational risk, and around seeing that our third parties can continue to function at the same level.

Going forward, what changes would you like to see in how your organization manages risk?

A lot has to do with third parties. We want to know all we can from different risk perspectives, and a lot of that has to be gathered through questionnaires, assessments, and legwork. We also need to be able to say for a service that we want to outsource, these are—quantitatively—the risks, and this is how we can mitigate them.

How do you think a risk function can elevate its visibility and influence in an organization?

I believe lack of visibility and influence happens when risk is done mainly as compliance and fails to give management an integrated view of risks. Also, we've found that it's good to place a dollar value on risks—here is the exposure and here's what we'd have to spend to mitigate it, for this much benefit. For us, that's superior to high, medium, and low risk rankings; because if you have multiple risks classified as, say, medium, they're harder to compare. If you quantify them in monetary terms, you can say, we really need to look into this versus that.

Any final thoughts?

I would say that risk management has to be as important as compliance. Compliance operates from the government agency regulatory perspective, but risk management operates from the perspective of your organization and your business.

Elevating the role of risk management

Many organizations do not know what risk management costs or what value it provides, or could provide. A risk reboot can help address this situation by:

- Taking a fresh look at the organization's approach to risk, then rationalizing and rightsizing risk activities—particularly compliance activities, which can often be automated—and reinvesting in higher-value/higher-return activities
- Integrating risk management by cutting across organizational silos and activities
- Streamlining risk management by focusing people, processes, technologies, and investments on the risks that matter most—the risks that could undermine the ability to fulfill stakeholder expectations
- Quantifying the cost and value of risk management outputs
- Gearing risk management to an environment of ongoing uncertainty by providing enhanced risk data and risk-based decision support

A reboot elevates the role of risk by identifying new opportunities to deliver value as well as by addressing actual and potential threats. This increases C-suite confidence in the risk function by delivering more relevant information, including predictive information, and solving the compliance conundrum created by the need to continually create controls, processes, and reports in response to new mandates.

How can this be accomplished at the action level? First, assess the current state of risk management by cataloging all risk-related activities, and then analyze the cost, necessity, impact, visibility, and potential for consolidation or automation, or both. Next, optimize risk activities by simplifying or eliminating those that can be, integrating stand-alone risk-related activities into existing processes, and automating activities by means of intelligent technology. Finally, migrate to higher-value risk management by building out capabilities that focus on the most important risks and streamlining workstreams, investing in proactive risk management solutions, and communicating costs savings and performance improvements to drive risk transformation.

A successful reboot also calls for C-suite and board-level support and for having the right risk leaders in place. Regarding leadership, most risk professionals have sound technical expertise. They can define and calculate inherent and residual risk, and possess deep expertise in compliance, cyber, health and safety, legal, and other risk domains. Yet they tend to speak the language of risk rather than of business. This leaves them communicating in ways that fail to illuminate actual risks for senior executives, which may undercut their credibility.

Forward-thinking organizations are seeking risk leaders who understand not only risk but also business strategies and how they are implemented. These leaders, equipped with eclectic backgrounds and broad business experience, can translate the often-abstract concept of risk into concrete impacts on strategies, initiatives, and decisions. They can also assist the executive team and the business in risk identification, monitoring, mitigation, management, and response.

The best of these leaders promulgate the notion that risk management is inseparable from business management, talent management, data management, supplier management, and so on. This makes risk everyone's responsibility, which it must be for truly effective risk management. It also combats the (mistaken) idea that someone else, as

in “someone in risk management,” is responsible for risk. Managing risk is, as appropriate to the position and its responsibilities, part of every job in the organization.

Lockheed Martin, for example, has closely linked enterprise risk management with sustainability and resilience to ensure that risk-management data informs decisions throughout the corporation. This approach also promotes collaboration and shapes annual imperatives at the highest levels of management. The organization’s sustainability governance structure comprises the board of directors, executive leadership team, and functional leaders responsible for sustainability. The lead sustainability executive is the senior vice president, Ethics and Enterprise Assurance who oversees ethics; enterprise risk; environment, safety, and health; internal audit; and sustainability.

Aligning sustainability and enterprise risk management under one department reporting to a senior executive has brought about greater integration between sustainability and risk management for Lockheed Martin. This has enabled management to tap risk assessments and sustainability performance data, gauge talent and manufacturing risks more accurately, and oversee corporate policies. As a best practice, the organization shares its sustainability reports to prospective business partners when discussing long-term contract agreements.[8]

Some useful questions to ask as you consider ways to elevate risk management’s role include:

- How does management and the organization currently view the risk function? As primarily compliance-driven? As a key strategic function? Or somewhere in between?
- Which of our risk management activities deliver the most value to the organization and its stakeholders? Which deliver the least?
- How can we efficiently minimize, eliminate, or automate the lower-value activities we engage in? What could we accomplish with the liberated resources?
- Do I, as a risk leader, have a practical, panoramic view of the risks to our organization and its stakeholders?
- Do I speak the language of business, as well as risk? How can I broaden and deepen my view of risk and my ability to communicate that view?
- What are the two to four most impactful steps I could take in the next 6 to 12 months to increase risk management’s value to my organization?

LESSONS LEARNED: A CONVERSATION WITH ANDREW WHEATLEY

Vice president, Audit, Risk & Compliance, ServiceNow

How have your organization's risk management practices worked, given the coronavirus outbreak?

Overall, quite well. We had invested a lot in digitizing our processes, so 50 to 60% of our risk team were already working remotely. About three years ago, we moved from a check-the-box to an action-oriented approach to risk, with regular updates on progress against plans. More recently we created digital workflows to support risk-related activities, including those beyond risk assessment. Those shifts kept us going after the coronavirus.

What things might still need improvement?

A big takeaway for me is getting a handle not only on known unknowns, things we're thinking about on a macro level, but also on unknown unknowns, things we're not thinking about but should be. Before, we didn't think much about pandemics but we do now, along with things like escalating trade wars or geopolitical environments that could impact both our own business models and those of our customers. Macro forces, even slow-moving ones, can be disruptive if you're not prepared.

How did you transition from compliance-oriented risk management to true risk management?

Our previous CEO expected his leadership team to engage on enterprise risk management. That set the tone, and he was a mentor on how this should operate. We set the objective of being action oriented, and had accountability of individual enterprise risks at the c-level. Being an enterprise risk owner, also means you have an annual date with the board to go deeper on your risk.

This drives a whole other level of accountability to show progress and establish objective measures against critical risks. This support and mentoring have continued with our new leadership team at both the CFO and CEO level.

What's your system of characterizing risks?

Often in an organization people use various risk assessments that don't share a common taxonomy, standards, or framework. We've defined a methodology, taxonomy, and rating system to give us a common definition of how to talk about risks regardless of the domain. It is really helpful when the CFO, CIO, CISO, and General Counsel are all speaking the same language and prioritizing risk in the same way. We also developed an issue rating system for security, financial, and other risks, and a common reporting structure. That move to address issues as well as risks let us show real progress quickly.

How do you go about considering your internal and external stakeholders?

Internally, we help risk owners to drive their risk management activities, including issue remediation and closure. Our digital workflows and common policies enable them to do their jobs more effectively. When they update the board or audit committee and we help them do that, it wins support.

Externally, I have an organization that focuses on customers from a compliance, certification, and audit standpoint. So, any customer gap or issue, whether regulatory certification or identified by a customer, goes through the same intake, evaluation, remediation, and tracking process. We focus both on customer regulatory issues and on risks they've identified, so it's all integrated.

This ultimately gets us back to our single system of record, and our common language. Risk assessment is not a point in time exercise for us, but a lifecycle from risk identification, risk assessment, control environment evaluation, assessment of known gaps and issues, and evaluation of residual risk. We need all of this information working together to make better decisions and prioritize our activities.

Do you use scenarios when assessing risks, formulating plans, and supporting decisions?

Our GRC product enables an organization to dive into a scenario, perform a prospective risk assessment, and assess the preparation. That takes us into an operational risk mindset, the next step for us.

How has your organization been able to access data and communicate during the crisis?

Given our proactive approach, not much has changed. We had excellent analytics and access to data, and were already using online collaboration tools. Also, I serve on several cross-functional committees to address data governance/ethics, enterprise transformation, and compliance strategies. All of that helped us to be prepared.

How is your organization positioning itself to thrive going forward?

We're focusing on talent. Working from home taxes your workforce, emotionally and mentally. A new blend of family life and work life raises issues of managing a remote workforce, staying connected, overcommunicating, and being transparent. We're insisting on boundaries and people taking vacations, even if they're staycations. There are major talent risks and I don't think it's going to go back to how it was. So how you attract, retain, and manage great talent, and maintain a culture, are critical.

What would you say to a risk leader who wants to elevate the risk function but may not yet have leadership support?

Make the effort data-driven and measurable, to make it real for leaders. If I debrief an executive for an hour and never give back anything useful, that's not worth their time. But if I can provide an action plan that creates accountability, and perform data-driven risk assessments, track analytics such as, patching or vulnerability analytics, and audit progress, all of that helps risk owners.

How do you go about disseminating risk information to the business and functions?

We focus on several key domains, like cybersecurity, privacy, legal and regulatory, financial, controls, and a few others, and report to risk owners on how we evaluated risks, key risk drivers, actions taken, and status of actions. We also focus on issue management—and on policy, requirement, or control gaps—and tie it to a risk in their area. We identify how many high-risk issues we've addressed, and work to get highly rated issues to trend downward. We also avoid detailed reports on 50 or 80 risks.If you focus on eight to 10 critical risks, you can capture leaders' attention and develop meaningfulKPIs and KRIs. More detailed risks can be under those, but focusing on those that can really impact the organization works best.

Has your organization's risk appetite changed?

We already had a low appetite for high-risk areas, but new risks can arise where we may have had more of an appetite, for example, among third parties. So, there are risks where we may reset the bar.

Any final thoughts?

A risk management program benefits from clear goals, a common taxonomy, and engaged stakeholders. Make it data-driven and actionable and demonstrate that you are moving the needle on the most critical risks and issues for your organization, and you will see progress.

Generating and disseminating risk intelligence

When a crisis strikes and amid ongoing uncertainty, management needs a clear picture of current and potential developments. While effective controls and compliance are still needed, risk management should shift toward providing intelligence about the organization's risks and anticipating the path forward. This enables management to position the organization to respond, recover, and thrive.

Yet the risk leader and the risk function often lack the access to data, the analytical firepower, and the ability to communicate with management and the organization in real time or near-real time. All of these capabilities are needed to fulfill the role of advisor to the executive team and the business. They are also needed to enable management to use risk-informed decision-making to become more agile, resilient, and competitive.

A successful risk reboot empowers the risk leader with ready access to risk and performance data, analytical tools, and reporting mechanisms such as data visualization. Equally important, the risk leader and his or her team should be prepared to, provide early warnings of emerging risks to further support decision-making—perhaps with an assist from risk-sensing technologies, predictive analytics, and scenario planning—along with actionable insights and recommendations.

Scenario planning in particular can enable risk leaders to clearly portray the impact of potential risk events on specific stakeholders. It enables management to more clearly understand the full range of available options as well as the if-then ramifications of each decision. Scenario planning also enables leaders to define potential signals that, if they were to emerge, might indicate the nature and impact of potential risks as well as the direction of future events. However, that said, scenarios should be used not only to game out situations, but also to incorporate actual risks into the organization's decision-making processes. Note, too, that the richer the data the organization feeds into scenario planning, risk monitoring, risk sensing, and predictive analytics, the more valuable those tools can be.

Royal Dutch Shell Plc created a scenario planning team in the 1960s to anticipate disruptions in the energy industry. Although the post-WWII years seemed to guarantee stable oil prices, the team aimed to identify factors that could cause volatility in the energy market. So, they considered events in the Middle East and, while they did not predict OPEC, they did forecast that continuing oil price stability was relatively unlikely. As a result, Shell was prepared for the energy crisis of 1973 and incorporated scenario planning permanently into decision-making. Various media have attributed anticipation of Russia as an emerging power, liberalization of global markets, and China's status

as the world's largest energy consumer to this methodology.

Shell explains that the inability to predict events is what makes scenario planning necessary. It liberates analysts from futures based only on the past and enables decision-makers not to assume that the current course of action will remain in place.Understanding the technological, social, and political forces that shape the future stimulates analysis of problems from multiple perspectives and identifies trends that could impact the organization and its stakeholders.[9]

Some useful questions to ask as you strive to deliver risk intelligence include:

- What risk data does management need, and how can we access and analyze that data and effectively distribute and communicate the results?
- How can we apply predictive analytics, risk sensing, and other smart technologies to improve our risk management and decision support capabilities?
- How can we use scenarios to better understand developments in this and future crises?
- How can we better assist management in crafting potential responses to risk events? What signals and triggers might enable us to determine which responses should be implemented and when?
- How can we communicate better about risk across our organization? How can we more clearly portray the potential business impact of risk events on our organization and stakeholders?
- What actions do we recommend to mitigate risks and leverage opportunities that have been identified? How can we frame our recommendations in ways that compel management to act on them?

This pandemic has shown organizations that they can make decisions rapidly under conditions of extreme uncertainty. The challenge is to make even better decisions under the conditions that lie ahead. This calls for combating the inertia that may cause the organization to lose that ability and return to business as usual, and drive risk management to return to former modes of operating.

Risk functions have a rare but real opportunity in this moment. Rather than slowing down decisions, raising only objections, or entering the process too late, risk must be an enabler, not a barrier. That means supporting fast decisions, presenting solutions, and being engaged at the outset.

This calls for combating the inertia that may cause the organization to lose that ability and return to business as usual, and drive risk management to return to former modes of operating.

Put another way, management can do something other than simply trying to de-risk strategies or initiatives by failing to take action, doing the same things repeatedly, or adopting late adopter or laggard modes of operating. Instead, with assistance from the risk function, management can employ strategies and initiatives that accommodate feedback, modifications, iterations, and course corrections. In an environment of ongoing uncertainty, no decision is final, strategies must be flexible, and initiatives will need fine-tuning. That calls for a very different approach to risk and for a very different risk function.

LESSONS LEARNED: A CONVERSATION WITH A RISK LEADER IN TECHNOLOGY

What has been the greatest challenge posed to your organization by COVID-19?

We work with many third-party partners/suppliers to serve customers, so supply chain resiliency was a big focus area in this virtual world. Another big area of focus was enterprise data and reporting. We saw a major spike in sales as everyone went remote, but we had to work on the reporting dashboards to see if we had enough supply/inventory in stock or at our partners warehouse to meet customer demand.

Has any of this changed the way you'll manage risk in the future?

One of the big takeaways from how we responded to this crisis, has been developing rapid action plans to potential worst-case scenarios. So, whether it's a supply chain or cyber or financial event, we want to utilize scenario planning to make our ERM program even more action oriented. The scenarios helped us create response plans and do dry runs with cross functional teams, that eventually helped us be prepared to respond to the crisis. People may say, "Well, the worst-case scenario will never happen." I would say to that, "If you plan for the worst case then you can respond to something short of that."

It's about planning for things you can't predict.

Exactly! Now that [COVID-19] has happened, we realize there are four or five potential things that could hugely impact our business, things you didn't think could happen. So, we're building scenarios and some context around them and identifying metrics and data that will indicate whether or not something is really happening. We want to work on that over the next year. Not just scenario planning, but also, what are we monitoring behind these scenarios, so if things change, we are ready to respond.

As a risk manager, how do you think about the broader ecosystem of stakeholders?

It starts from the board, then goes to the customers, then to other internal and external stakeholders and in our case our partners, who are very important to us. We focus on high risks and on the owners of the risk, for example the CISO and CIO for cyber, and the impact on our customers and partners. I see real value in looking at the potential impact on various stakeholders and making sure we think about them for each risk or scenario we're working on.

How about your ecosystem of supply chain partners and your resilience?

Over the last few months, we've worked closely with our partners to learn more about their capabilities. For example, how many warehouses do they have? Which ones serve our customers? What if this warehouse goes down? How will we be affected? Or if we go down, how can we shift more work to them? We're learning more about our third parties' business continuity plans for operations that support us. We've done a lot of scenario planning with them, and we'll revisit this annually or more frequently.

How has this crisis impacted risk leaders' relationship with senior executives?

It's given risk leaders more visibility to the executive team. I don't think all the executives knew what I do, things like decision trees, process flows, response plans and cross-functional scenario planning. They now have a better understanding of how they can incorporate risk considerations into initiatives and manage risk in a more structured way. I don't think they had seen the value of organizing specific risks, like supply chain risks, into a framework and identifying alternative decisions and outcomes that can help them make better decisions.

What can a risk leader do to elevate the risk function in the organization?

I think that the risk function should have its own point of view. Often, you evaluate scenarios or provide insights, and the company strategy is what it is, and management is going to pursue it. But we don't want to pursue it or be tied to it if it's the wrong strategy. So risk needs to have its independent point of view on potential events, which may or may not happen, but we need to be prepared to analyze and respond if any of them do happen. It's not so much about challenging senior executives on what they know or don't know. It's about stretching their thinking on "What if this happened, how would we respond?"

Any final thoughts?

I think this crisis is forcing the conversation in new directions because the worst-case scenario actually happened. Now organizations realize that they need a solid plan for responding to something like this.

Shape—or be shaped by—events

AS NOTED IN disclosures in publicly held companies' annual reports, senior executives and the board are responsible for managing and governing risk. Indeed, heightened expectations from the investment community, particularly in the form of activist and impact investors, have intensified the overall focus on this area. At the same time, this responsibility has become more complex and challenging in a world that is far more globalized, interconnected, digitized, diverse, and rapidly evolving than that of the last century.

Yet legacy methods of managing risk persist, particularly in large organizations. The speed of change and the nature of threats can actually prompt management to perceive things in familiar ways, reach for familiar tools, and do familiar things precisely because they are familiar.

As deadly and damaging as COVID-19 and its economic and social impacts have been, they have provided valuable lessons regarding what a truly unanticipated major risk event can do. Those lessons have in turn revealed new ways of perceiving risks and new ways of creating value, even in the face of future events of similar proportions. They also drive home the point that risk management is not about predicting events but about fostering institutional agility and resilience to modify strategies as the business environment evolves.

External complexities combined with complex internal processes—and the staggering range of stakeholders in a large, global organization—present the need to efficiently identify and address the highest priorities for a risk reboot. While those priorities will vary from organization to organization, they will most often include one or more of the following:

- Calculating and controlling the costs associated with compliance and risk management
- Delivering risk management that provides measurable value to the organization and its stakeholders
- Positioning the organization to recover from and thrive after the next unprecedented risk event

A successful reboot also hinges on using demonstrated methods of change management and continual improvement. Many organizations find that they benefit from a process for addressing such needs—a process that can germinate in a facilitated lab experience.

This may seem like an inopportune time to reboot risk, but it is actually the ideal time to do so. The current climate of uncertainty is, again, revealing what is most important to the organization and its stakeholders. This moment is not simply providing a new perspective. It is prompting a deeper examination of the value that the risk function has delivered, not delivered, and can deliver in a perennially uncertain environment.

Endnotes

1. Foo See Lang, Lex Lee, and Cheng Nam Sang, *Risk management in a VUCA environment: Some key considerations, Journal of the Institute of Singapore Chartered Accountants*, April 22, 2016.
2. National Commission on Terrorist Attacks Upon the United States, *9/11 commission report: Chapter 11: Foresight—and hindsight*, 2004.
3. Thijs Bouwens, "Clariant recognized for risk management and sustainability achievements in procurement," Clariant, May 27, 2019.
4. Riskmethods, "Chemical industry is most at risk to supply chain disruption from fires and explosions," July 31, 2019.
5. Clariant, "Risk management," accessed August 7, 2020.
6. Jennifer T. Lee et al., *Embedding trust into COVID-19 recovery: Four dimensions of stakeholder trust*, Deloitte Insights, 2020.
7. Edelman Trust, "Edelman Trust barometer 2020," January 19, 2020.
8. Lockheed Martin Corporation, *2018 sustainability report: The science of citizenship*, 2019.
9. Ricardo Solano, "Good practices in risk management: Shell scenario planning," Riesgos Políticos, April 15, 2019.

About the authors

John Peirson | usrfajohnpeirson@deloitte.com

John Peirson is the chief executive officer (CEO) of Deloitte Risk & Financial Advisory and has held multiple leadership roles across the firm. As Deloitte Risk & Financial Advisory's current CEO, Peirson leads more than 15,000 professionals who help organizations navigate a variety of risks, embrace complexity, and accelerate performance. He also is a member of the US Executive Committee and US Management Committee. John has more than 30 years of experience advising global clients on strategy and transformation across a broad spectrum of financial and regulatory matters. Throughout his career, he has helped clients in areas including external and internal audit, controls optimization, operational risk transformation, accounting and reporting, and governance-related services, all with an eye toward guiding organizations to become high-performing businesses.

Ed Hardy | ehardy@deloitte.com

Ed Hardy is the market segments leader who is responsible for advancing the portfolio of our services across Deloitte Risk & Financial Advisory to meet our clients' risk needs. He is a Deloitte & Touche LLP partner and has more than 20 years of experience serving clients in the financial services industry, focusing on derivatives, hedging, asset securitization, and structured finance transactions. Hardy has advised several investment banks and securities institutions in understanding the accounting implications and unique regulatory accounting considerations of alternative structures relating to financial instruments. He has also provided divestiture and IPO-related services to some of our largest financial services clients, including assisting companies with the establishment of the necessary process and procedures to support a successful transaction.

Don Fancher | dfancher@deloitte.com

Don Fancher is a Deloitte Risk & Financial Advisory principal in Deloitte Financial Advisory Services LLP, and serves as the US national and global leader for Deloitte Forensic. He has more than 25 years of experience assisting clients on matters including forensic investigations, dispute consulting, intellectual property services, and reorganization services. Fancher has also testified as an expert witness on numerous occasions in federal, state, and bankruptcy courts.

Deborah Golden | debgolden@deloitte.com

Deborah Golden, a principal at Deloitte & Touche LLP, is the US Cyber & Strategy Risk leader for Deloitte Risk & Financial Advisory. In the prior six years, Golden served as the Government & Public Services (GPS) Cyber Risk Services leader, as well as the GPS Advisory Market Offering leader, GPS Empowered Well-Being leader, and the lead principal for a major federal government health care provider.

Mike Kearney | mkearney@deloitte.com

Mike Kearney is a Deloitte Risk & Financial Advisory partner and chief marketing officer in Deloitte & Touche LLP. As chief marketing officer, he leads the effort to fulfill and amplify our brand promise—to help organizations navigate business risks and opportunities to gain competitive advantage. He is also the host of Deloitte's award-winning Resilient podcast series. Kearney has served clients for more than 25 years, focusing on elevating risk as a key C-suite topic. Prior to his current role, he led our next-generation Brand and Reputation solutions Ventures Fund and our curated client experiences, which bring our innovative solutions to life.

Dan Kinsella | dkinsella@deloitte.com

Dan Kinsella is the managing partner of the Omaha office and serves as the US Extended Enterprise Marketplace leader in Deloitte & Touche LLP. He combines business and technology experience to help clients create and optimize their extended enterprise through cost and revenue recovery services. He specializes in creating efficient exchange of risk information synergies in the marketplace. Kinsella leads Advisory Service Delivery Transformation, helping clients' efforts in shared services and outsourcing environment improvements.

Matt Marsh | mamarsh@deloitte.com

Matt Marsh is the managing partner for Deloitte LLP's Minneapolis office, guiding more than 950 professionals providing audit, consulting, financial advisory, risk management, tax, and related services to clients in Minnesota, South Dakota, and North Dakota. He leads the strategy, operations, business development and talent for the practice. Matt is the Global and US Risk & Financial Advisory leader for the Retail, Wholesale & Distribution practice of Deloitte & Touche LLP.

Chris Ruggeri | cruggeri@deloitte.com

Chris Ruggeri is Deloitte Risk & Financial Advisory's Crisis & Resilience leader in Deloitte Transactions and Business Analytics LLP, as well as the Global Strategic Risk leader. With more than 25 years of experience, she is focused on helping our clients manage strategic risk to drive sustainable shareholder value, financial flexibility, and agility, and improve stakeholder confidence. Ruggeri has also served as the Strategy and Innovation leader and the M&A leader where she advised companies, boards of directors, and committees on negotiated and unsolicited transactions to understand the value of business enterprises and associated risk factors. Ruggeri has been quoted by top-tier media on M&A trends, corporate development, and shareholder activism.

Damian Walch | dwalch@deloitte.com

Damian Walch is a Deloitte Risk & Financial Advisory managing director in the Crisis & Resilience practice of Deloitte & Touche LLP. As a resilience leader for more than 25 years, he has assisted companies in reducing the financial and reputational impacts associated with business disruptions and disasters. He was named a "Top 25 Consultant" by *Consulting Magazine* in 2003 and has spoken at leading resilience conferences, as well as authored more than 50 articles on risk- and resilience-related topics.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

John Peirson
CEO | Deloitte Risk & Financial Advisory
+1 612 397 4714 | usrfajohnpeirson@deloitte.com

John Peirson is the chief executive officer (CEO) of Deloitte Risk & Financial Advisory and has held multiple leadership roles across the firm. As Deloitte Risk & Financial Advisory's current CEO, Peirson leads more than 15,000 professionals who help organizations navigate a variety of risks, embrace complexity, and accelerate performance.

Ed Hardy
Market Segments leader | Partner | Deloitte & Touche LLP
+1 212 436 2832 | ehardy@deloitte.com

Ed Hardy is the Market Segments leader, who is responsible for advancing the portfolio of our services across Deloitte Risk & Financial Advisory to meet our clients' risk needs. He is a Deloitte & Touche LLP partner and has more than 20 years' experience serving clients in the financial services industry, focusing on derivatives, hedging, asset securitization, and structured finance transactions.

Don Fancher
US and global leader, Deloitte Forensic | Principal | Deloitte Financial Advisory Services LLP
+1 770 265 9290 | dfancher@deloitte.com

As the US and global leader of Deloitte Forensic, Don Fancher has more than 25 years of experience assisting clients on matters including forensic investigations, dispute consulting, intellectual property services, and reorganization services.

Deborah Golden
US leader, Cyber & Strategy Risk| Principal | Deloitte & Touche LLP
+1 703 623 8306 | debgolden@deloitte.com

Deborah Golden, a principal at Deloitte & Touche LLP, is the US Cyber & Strategy Risk leader for Deloitte Risk & Financial Advisory. Over the past 25 years, she has worked with commercial organizations and government agencies to navigate multifaceted cyber issues and successfully transform business and mission objectives.

Mike Kearney
Chief marketing officer, Risk & Financial Advisory | Partner | Deloitte & Touche LLP
+1 415 846 7948 | mkearney@deloitte.com

As the Deloitte Risk & Financial Advisory chief marketing officer, Mike Kearney leads the effort to fulfill and amplify our brand promise—to help organizations navigate business risks and opportunities to gain competitive advantage.

Dan Kinsella
US Extended Enterprise Marketplace leader| Partner | Deloitte & Touche LLP
+1 402 203 5341 | dkinsella@deloitte.com

Dan Kinsella is the managing partner of the Omaha office and serves as the US Extended Enterprise Marketplace leader in Deloitte & Touche LLP. He combines business and technology experience to help clients create and optimize their extended enterprise through cost and revenue recovery services.

Matt Marsh
Partner | Deloitte & Touche LLP
+1 612 397 4575 | mamarsh@deloitte.com

Matt Marsh is the managing partner for Deloitte LLP's Minneapolis office and serves as the Global and US Risk & Financial Advisory leader for the Retail, Wholesale & Distribution practice of Deloitte & Touche LLP. Marsh has more than 25 years of experience across risk domains in the retail sector.

Chris Ruggeri
National managing principal | Partner | Deloitte Transactions and Business Analytics LLP
+1 212 436 4626 | cruggeri@deloitte.com

Chris Ruggeri is the leader of Crisis & Resilience in Deloitte Risk & Financial Advisory as well as the Global Strategic Risk leader, helping our clients manage strategic risk to drive sustainable shareholder value, financial flexibility, and agility, and improve stakeholder confidence.

Damian Walch
Managing director | Deloitte & Touche LLP
+1 630 215 6519 | dwalch@deloitte.com

Damian Walch is a Deloitte Risk & Financial Advisory managing director in the Crisis & Resilience practice of Deloitte & Touche LLP, assisting companies in reducing the financial and reputational impacts associated with business disruptions and disasters.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Junko Kaji, Sayanika Bordoloi, and Rupesh Bhat
Creative: Sylvia Chang, Molly Woodworth, and Jaime Austin
Promotion: Alexandra Kawecki
Cover artwork: Tatiana Plakhova

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte