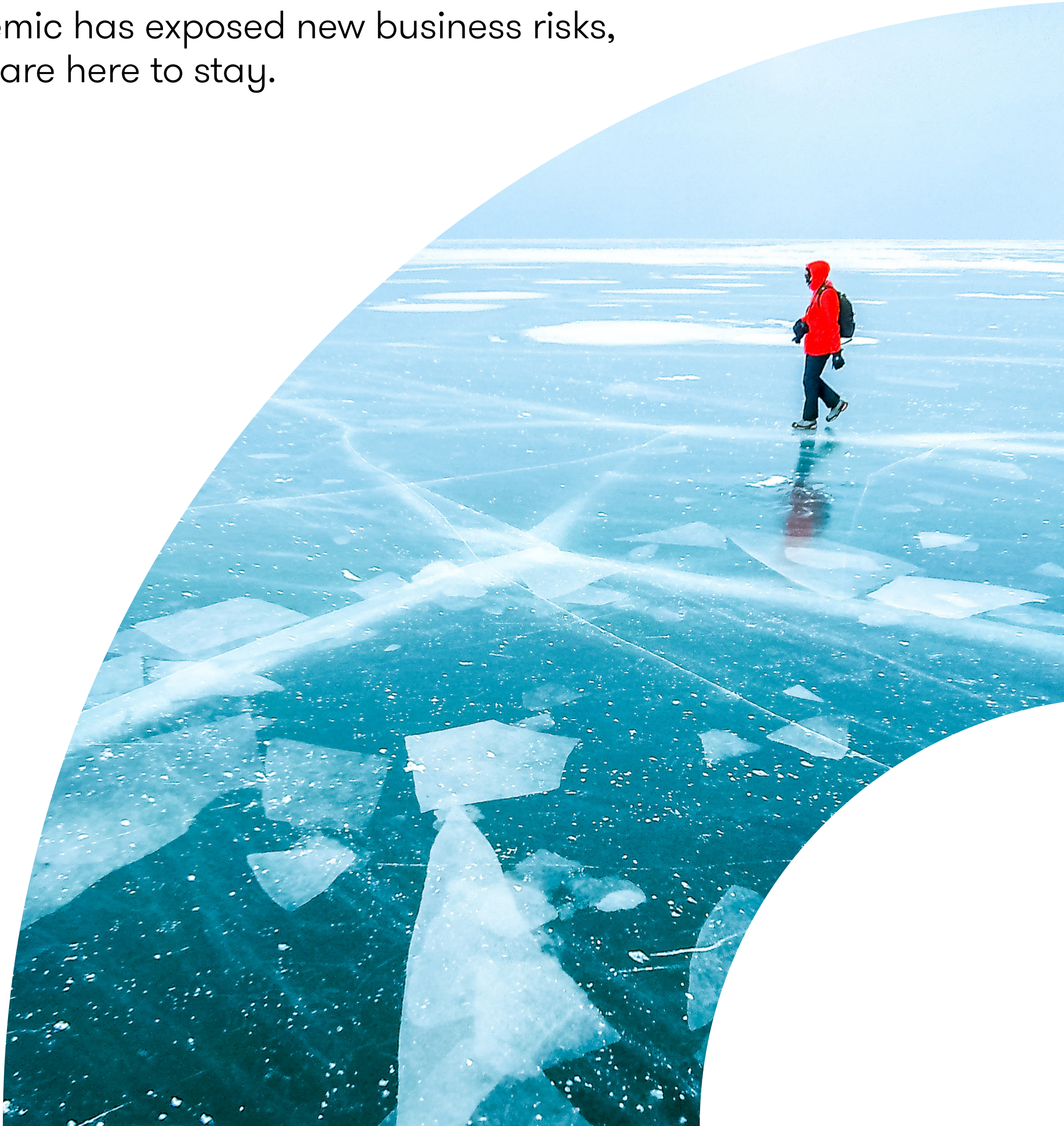
Grant Thornton

Update your enterprise risk management

The pandemic has exposed new business risks, and some are here to stay.



Your ERM needs to cover new gaps and drive new value.

In the past two years, the emergence of new or unseen risks has spurred both boards and operators to focus more time and attention on improving risk management. “Many leaders found that they had some gaps,” said Grant Thornton Strategic Risk and Operations Principal Yvette Connor. “They didn’t understand how a multi-dimensional event could impact their organizations in so many direct and indirect ways. Now, they’re seeking ways to better identify, assess and manage risks.”

Now, enterprise risk management (ERM) has a mandate to consider risk impacts more holistically — and solve more creatively — across all risk types. ERM needs to look for new and better approaches, such as creating a “single pane of glass” to provide holistic insight into material risk dimensions. ERM needs to consider risk intelligence tools that deliver and incorporate Artificial Intelligence (AI) to accelerate risk management across all domains. Many organizations are using new tools and techniques to integrate and inform resilience topics like supply chain; inflation; workforce; credit; and Environmental, Social, and Governance (ESG). These integrated insights can help leaders understand “where the puck is going,” so they can avoid unwanted surprises and potential impairments to working capital, customer engagement or the brand. Better risk insights can guide risk and control alignment and efficiencies, inform product line and business strategy, and ultimately improve resilience and competitive advantage.

That is how ERM can drive the most business value.

To make sure ERM keeps driving business value, organizations need more than a one-time adaptation. They need accurate risk definitions, consistent processes, effective controls and secure technology. Most of all, they need updated risk management that quickly adapts to changes in the risk landscape.

The COSO framework is still the basis for audits and the starting point for most organizations. However, it is essential to understand the gaps where risk is lurking, and to understand how your risk management practices need to adapt.

The COSO framework divides ERM into five components. Each of the five components are supported by 3–5 practices. If there is a weakness in any one of these practices, that can mean a gap in an organization’s risk management.

The 5 components and 20 practices of ERM

Governance and culture

1. Exercise board risk oversight
2. Establishes operating structures
3. Defines desired culture
4. Demonstrates commitment to core values
5. Attracts develops and retains capable individuals

Strategy and objective setting

6. Analyzes business context
7. Defines risk appetite
8 Evaluation alternative strategies
9. Formulates business objectives

Performance

10. Identifies risk
11. Assesses severity of risk
12. Prioritizes risks
13. Implements risk responses
14. Develops portfolio view

Review and revision

15. Assesses substantial change
16. Reviews risk and performance
17. Pursues improvement in enterprise risk management

Information, communication and reporting

18. Leverages information and technology
19. Communicates risk information
20. Reports on risk, culture and performance

Changes in practice

To update risk management, many organizations need to start with updating their risk management practices.

Pandemic impacts have triggered fundamental changes for practices in each of the five ERM components, and organizations must adapt the practices affected to avoid risk management gaps. Some of the practices most affected by the pandemic include:

#3: Defines desired culture

We are now more aware of the need for both organizational and individual resilience.

The pandemic's ubiquitous impacts have heightened our awareness of many risks. Organizations must deliberately and thoughtfully address these risks, building resilience and bridging gaps at every level. Leaders need to share and support this more risk-aware culture throughout the organization, to make sure it factors into the planning within each function.

#5: Attracts, develops, and retains capable individuals

Human resources professionals and hiring managers are investing heavily to recruit and retain key skill sets, even breaking out of traditional minimum requirements for job candidates.

Organizations are becoming more flexible about candidate geography, hybrid work models and other schedule factors.

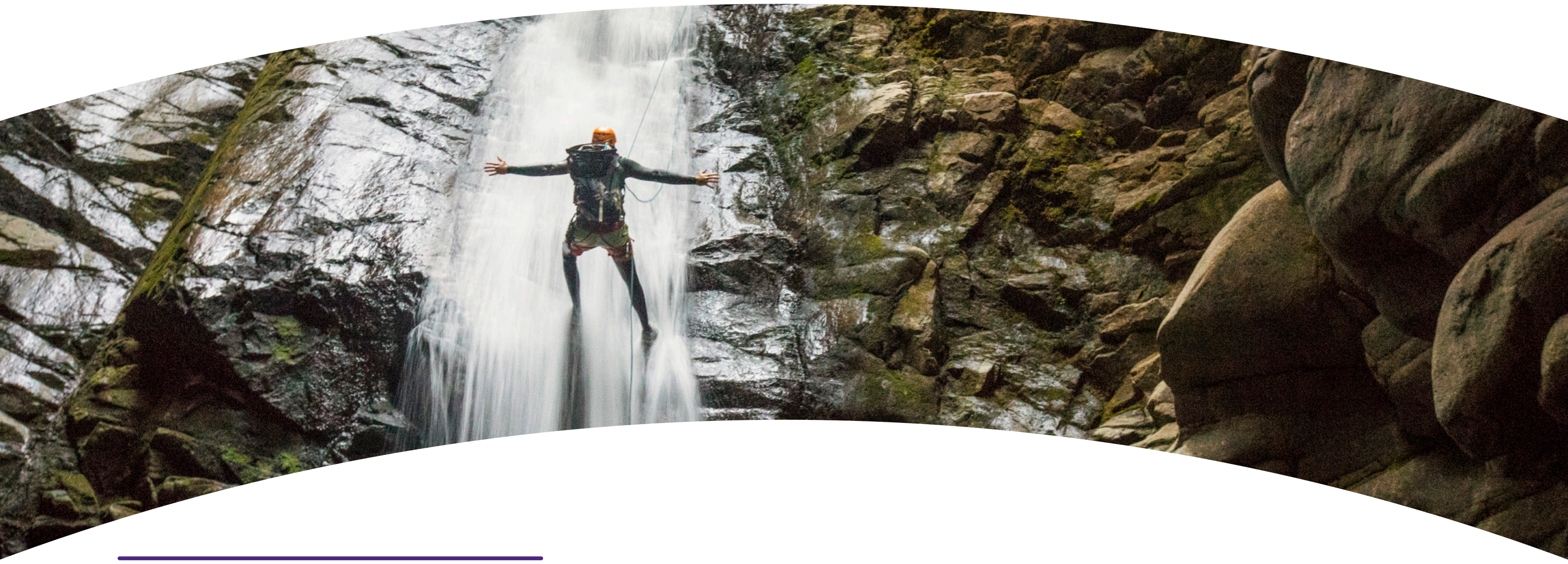
Retention in a tight labor market is critical, as it is easier to keep good employees than find good employees. Too few organizations really understand the needs of their employees. Our State of Work in America study found that half of all employees do not feel their voice is heard at work, and half do not feel the benefits they receive are any different than what they could get elsewhere. By keeping your finger on the pulse of employees, progressive organizations can better align a value proposition to the needs of their people and use this to win the battle for talent.

The harsh realities of risk materialization, and the need for strong risk management know-how, have even created a war for talent in ERM itself — and in related disciplines like audit, controls, cybersecurity and compliance. Many employers are encouraging employees to pursue risk management skills and certifications.

#6: Analyzes business context

Many organizations have been forced to shift more focus to the business context around them.

The COSO ERM Framework defines "business context" as "the trends, relationships and other factors that influence an organization's current and future strategy and business objectives." Around the world, organizations now need to realign because of impacts on customer preferences, the competitive landscape, and employee morale, retention and performance.



#7: Defines risk appetite

As organizations reconsider risk management practices, they must also reconsider their true risk appetite.

Leaders need to drive an honest self-appraisal of how much risk the organization is willing to take, or not take, in various areas. Some organizations have discovered that they had gaps in risk management and are now devoting resources to strengthening those capabilities. Others are modifying their historical risk tolerances, tightening the reins in some risk areas, while loosening them in others, to grow and thrive in the new business environment.

#12: Prioritizes risks

Organizations have a greater appreciation for effective risk prioritization — but at the same time, the priorities of risk types have shifted.

For example, executives and board members need to focus more keenly on external and emerging risks such as ESG, geopolitical turmoil and macroeconomic trends. Decision makers need to make some tough calls on funding certain key risk response initiatives at the expense of lower-priority risk areas.

.

#13: Implements risk responses

We've seen that proactively implementing risk response capabilities can help you weather challenging events, creating a competitive advantage in resilience, productivity and customer service.

Organizations need to update and revitalize outdated business continuity plans, but they should also go further. Proactive organizations should get independent assessments and testing of their risk response effectiveness and control structures, to identify gaps and address them.

#15. Assesses substantial change

We've seen how substantial change can affect strategy and business objectives, and we need to recalibrate on what a substantial change can be.

Risk assessments should consider a broader scope of possible risk events, including some that might have seemed unlikely in the past. Now, leaders must identify these risks and assess them in ways that drive informed decision-making on proactive resource allocation. Conduct a post-event analysis to review how the organization responded and consider lessons learned for future events.

#16. Reviews risk and performance

Leaders need to re-examine the potential impacts on performance.

A fresh examination needs to identify which risk events affected (or may affect) the achievement of performance targets, tolerance levels for key risk metrics, and overall effectiveness of ERM activities. This examination can reveal required adjustments in areas like the allocation of resources to competing risk initiatives and even in the risk strategy itself. Organizations without a mature ERM program have recognized that their risk management capabilities are not providing the risk identification, assessment and informed actions needed to cope in times of crisis.

#18: Leverages information and technology

Opening the aperture on risk considerations also means that organizations need to efficiently filter an increased volume of data into decision-driving insights.

Skilled analysis, interpretation and distillation is vital, but technology is increasingly essential. The more automated you can be in capturing and acting upon risk information, the greater your competitive advantage. Technology can help ensure that the data is relevant, accurate, well protected and easily accessible to decision makers. Ultimately, leaders need to make sure they can focus on predictive risk metrics, governance and culture information, emerging risk trends, and business context indicators.

#20: Reports on risk, culture and performance

Unprecedented events can mean that historical models must be updated.

Historical views remain important, but emphasis should shift to forward-looking views of risk, culture and performance. Middle management needs to provide new and more robust risk reports to the board. Reports need to meet the specific needs of the target audience, especially those in strategic decision-making and governance roles.

Changes across your business

When updating your ERM framework practices, you must also coordinate changes for risk management practices in each of the following functions.

Cybersecurity

The pandemic triggered a quick rise in online traffic for remote work, commerce and other critical functions. Unfortunately, cybersecurity at some organizations did not scale up to match the expanded traffic, new use cases and new threats. Even as pandemic restrictions recede, much of the new traffic, use cases and threats will continue to grow. Organizations have a growing dependence upon their online capabilities, and that means cybersecurity risks are business risks.

Cybersecurity changes in practice

Cybersecurity can intersect with all of the ERM changes in practice listed earlier and can be especially important for #18: Leverages information and technology. Consider actions like:

- **Reassessing your cybersecurity strategy**
  The pandemic accelerated the trend where organizations were updating their infrastructures to support remote work. However, these infrastructures often need further advancement to support the long-term hybrid work models that will continue to evolve. Organizations need to reassess their cybersecurity to consider whether and where to implement new analysis, identity access management, and tools and processes like cybersecurity mesh, zero-trust security, and remote-first security. The environment, use cases and tools for daily work have changed so fundamentally in the past few years that it's important to get out of the mindset of simply updating cybersecurity and identity access management models. Even existing tools might need to be applied in different ways.

- **Evolving your data governance**
  Many organizations have evolved new data demands, due to new customer demands, interfaces, business models, compliance requirements and other factors. That means that organizations need to evolve their data governance, too. As data demands and risks continue to change, organizations need to move from a purely rule-based reactive approach to a broader approach that integrates risk management and risk responses, creating a culture of mitigating risks and informing decisions.

- **Building resilience**
  Make sure that your organization has a comprehensive, effective and ready response plan. A cybersecurity plan is incomplete if it only protects the organization without including any guidance on how to respond to and mitigate incidents that occur. With the increasing dependence on business data and the increasing threats against security, you cannot afford to be left without guidance after a breach.

Privacy

Privacy is increasingly seen as a risk domain, rather than compliance. Privacy, and the handling of personal data, is critical for organizations to manage their regulatory and reputational risks. By formalizing privacy — defining controls, applying inherent risk values and measuring success — an organization can have a more holistic view into and management of their privacy risks.

Privacy changes in practice

Privacy can intersect with all of the ERM changes in practice listed earlier, and can be especially important for #13: Implements risk responses. Consider actions like:

- **Keeping processes evergreen through rapidly changing engineering environments**
  This requires technology to support and maintain privacy operations, allowing discovery efforts to happen without manual intervention. Teams must be able to operate lean — meaning efficiencies benefit stakeholders, business, and risk by reducing the time required from resources. This frees people up to innovate, address higher-priority activities and improve accuracy by enabling technology.

- **Avoiding questionnaire and workshop burnout**
  Between data inventory exercises, managing individual rights requests, developing retention and minimization programs, and enabling purpose limitation for the handling of data, burnout can easily develop. Privacy teams need to streamline the questions being asked of the business and enable business-as-usual risk management processes to obtain and sustain the information necessary to reduce and manage privacy risks.

Fraud

The pandemic had a major impact on fraud risk in several important ways. First, it demonstrated that inherent fraud risk is very high. As government pandemic stimulus programs rolled out funds with very limited controls, they were overwhelmed by fraud — signaling that many organizations may be underestimating their level of fraud risk.

Fraud changes in practice

Fraud can intersect with all of the ERM changes in practice listed earlier and can be especially important for #12: Prioritizes risks and #15: Assesses substantial change. Consider actions like:

- **Updating fraud risk assessment methodology**
  The pandemic incentivized a new generation of fraud actors. Synthetic businesses and identities used to commit fraud against pandemic benefit programs will be used in the future to conduct fraud scams against other targets, suggesting a new wave of fraud activity in the coming years. Organizations need to look for this activity with a proven methodology and a library of fraud schemes. This can help them assess true fraud risk, uncover critical control gaps, and identify the people, processes, and technology necessary to protect the organization from fraud.
- **Leveraging fraud threat intelligence**
  Fraud actors continuously evolve their tactics by probing for weaknesses and exploiting vulnerabilities through trial and error. They often share their techniques with fellow fraud actors in dark web message boards and social media platforms. They sell stolen data and credentials in dark web marketplaces. Organizations need a proactive threat reconnaissance capability to gain access to these intelligence sources and monitor this activity. This capability can help organizations identify new and emerging fraud threats in real time, so they can update their control environment accordingly and mitigate their risk to these rapidly changing schemes.

Compliance

The pandemic created an evolving risk landscape for many reasons, including more reliance on outsourced services. As a result, organizations are seeing higher risk levels and impacts in some key business areas. For instance, security and cyber-related incidents have exposed organizations and their third-party providers to greater risks. These threats may compromise the ability to deliver secure and reliable systems and services to customers. Many organizations need to re-examine and re-define their risk appetites and risk responses for new emerging risk areas.

Compliance changes in practice

Compliance can intersect with all of the ERM changes in practice listed earlier and can be especially important for #16: Reviews risk and performance and #20: Reports on risk, culture, and performance. Consider actions like:

- **Integrating reviews of third-party SOC reports**
  SOC reports provide a means for organizations to get insight into the control environment of their third-party providers and get an independent and objective assessment on the design and operating effectiveness of their controls. It is important for management of organizations that rely on outsourced services to include the review of third-party SOC reports in their compliance function and in the ERM process to assess and monitor third-party risks.
- **Assessing third-party risks and controls as part of your ERM**
  Many organizations use third-party providers to deliver part of their services, and the organizations retain responsibility over the risks associated with the outsourced services and with using such providers. As part of ERM, organizations need to assess, monitor and mitigate the risks associated with outsourced services. They also need to understand how their third-party providers manage processes and controls, related to internal controls over financial reporting or systems and services obtained.
- **Assessing your risks and controls that affect your customers and business partners**
  Third-party providers need to consider the risks that their customers face to provide adequate coverage in their SOC reports, as they are integral in their customers' risk mitigation strategies.

HR and workforce

The pandemic triggered many impacts for HR and workforce managers, including the "Great Resignation" and a turbulent job market that has left many sectors with more openings than candidates. That's why talent risks have risen to the attention of CFOs and other enterprise leaders and is a board-level concern.

HR and workforce changes in practice

HR and workforce can intersect with all of the ERM changes in practice listed earlier and can be especially important for #3: Defines desired culture and #5: Attracts, develops, and retains capable individuals. Consider actions like:

- **Assessing work-life balance**
  Salary is important, but it's not the only factor that employees consider. You might need to devote more attention to other incentives that help you stand out among potential employers. In the recent Grant Thornton State of Work survey, more than one third of full-time U.S. workers said they selected their new job because it offered a better work-life balance.

- **Offering the benefits that matter**
  Benefits can be expensive — about about a third of your cost for compensating an employee. But often, there's a disconnect. Employees don't use, or value, all of their benefits, and organizations don't track or receive a return on this investment. Many organizations waste thousands of dollars every year, per employee, on benefits that go unused or even unnoticed. The pandemic changed many employee perspectives and needs, so make sure your benefits are aligned and valuable.
- **Thinking of your brand like a brand**
  In a turbulent job market, it's important to think of your organization's "brand" as an employer. Think of an employee perspective the same way you think of a customer perspective: What makes your brand stand out? Why would people choose to join or stay with your organization? How do your competitors compare? What could your communications do to improve that perception?
- **Checking your culture**
  In the State of Work survey, 28% of employees said that dealing with their manager is the most stressful part of their day. What is your management culture, and are you losing productivity or value to ineffective behaviors? In the current war for talent, the effort you put into recruitment and retention can be poisoned by a toxic culture within your organization.

ESG and strategic risk management

Leaders, boards, investors, employees and customers have developed a much greater interest in ESG topics since the pandemic began. This interest means a heightened focus on ESG assumptions, data accuracy and reporting at the enterprise level. Organizations need to quickly consider and apply leading ESG frameworks in order to improve their overall ESG resilience, and to help inform the broader strategic risk management (SRM) plan that proactively assesses, mitigates, tracks and adapts for emerging risks

ESG and SRM changes in practice

ESG and SRM can intersect with all of the ERM changes in practice listed earlier and can be especially important for #6: Analyzes business context and #7: Defines risk appetite. Consider actions like:

- **Measuring your performance**
  Many organizations have not traditionally tracked or published metrics for their performance on ESG risks and results. However, growing interest and questions from many parties are pushing organizations to not only change their messaging but to show the metrics to back it up. Even if your organization is not ready to share ESG metrics, you might need to share your plan for when you will do so in the future — and you should consider how those metrics will look and what data you need to reliably inform the metrics.
- **Accelerating your analysis**
  The continued growth of business technology has introduced new risks, but it also introduces new possibilities. To truly evolve and apply your SRM, you need decisions that are driven by real-time analysis and insights. Your teams need more than numbers. They need actionable insights which can help them take proactive measures against a risk landscape which has become more complex and volatile — and which will continue to evolve as your organization transforms through workforce changes and technology transformation.

Evolve your ERM

Risk management teams across your organization need to collectively participate in strengthening and evolving your ERM to gain a competitive edge in and build value for the future. The landscape of risks has changed, threat velocity has accelerated, and the tolerance for material failures has decreased.

Most organizations experienced losses from risk gaps during the pandemic. While some of these risks might be unprecedented, organizations are still accountable to factor the lessons learned into their current and evolving ERM program. "Board members have said 'We learned we need to become much more risk intelligent and work to improve our understanding of how risk could impair all aspects of our business at any one time. That means we need to proactively understand our material risks and solve for what could impair our strategy and financial goals,'" Connor said.

Your cybersecurity, privacy, fraud, compliance, workforce, ESG, SRM and other risk management teams need to help ensure that evolved risk management becomes integrated into your culture, from long-term priorities to daily business decisions.

Contacts

Graham Tasman
Risk Advisory
Services Principal,
Banking Sector Lead
T +1 215 376 6080

Yvette Connor
Principal,
Strategic Risk Management,
National Practice Leader,
Risk Advisory
T +1 316 636 6525

Derek Han
Principal and Leader,
Cybersecurity and Privacy
T +1 312 602 8940

Lindsay Hohler
Principal,
Privacy and
Data Protection
T +1 703 847 7529

Khadyja Johnson
Partner,
Advisory – Governance
risk and compliance
T +1 303 813 4017

Tim Glowa
Principal,
Human Capital Services
T +1 832 487 1452

Sharon Whittle
Principal,
Human Capital Services
T +1 7034 632 6884

Grant Thornton