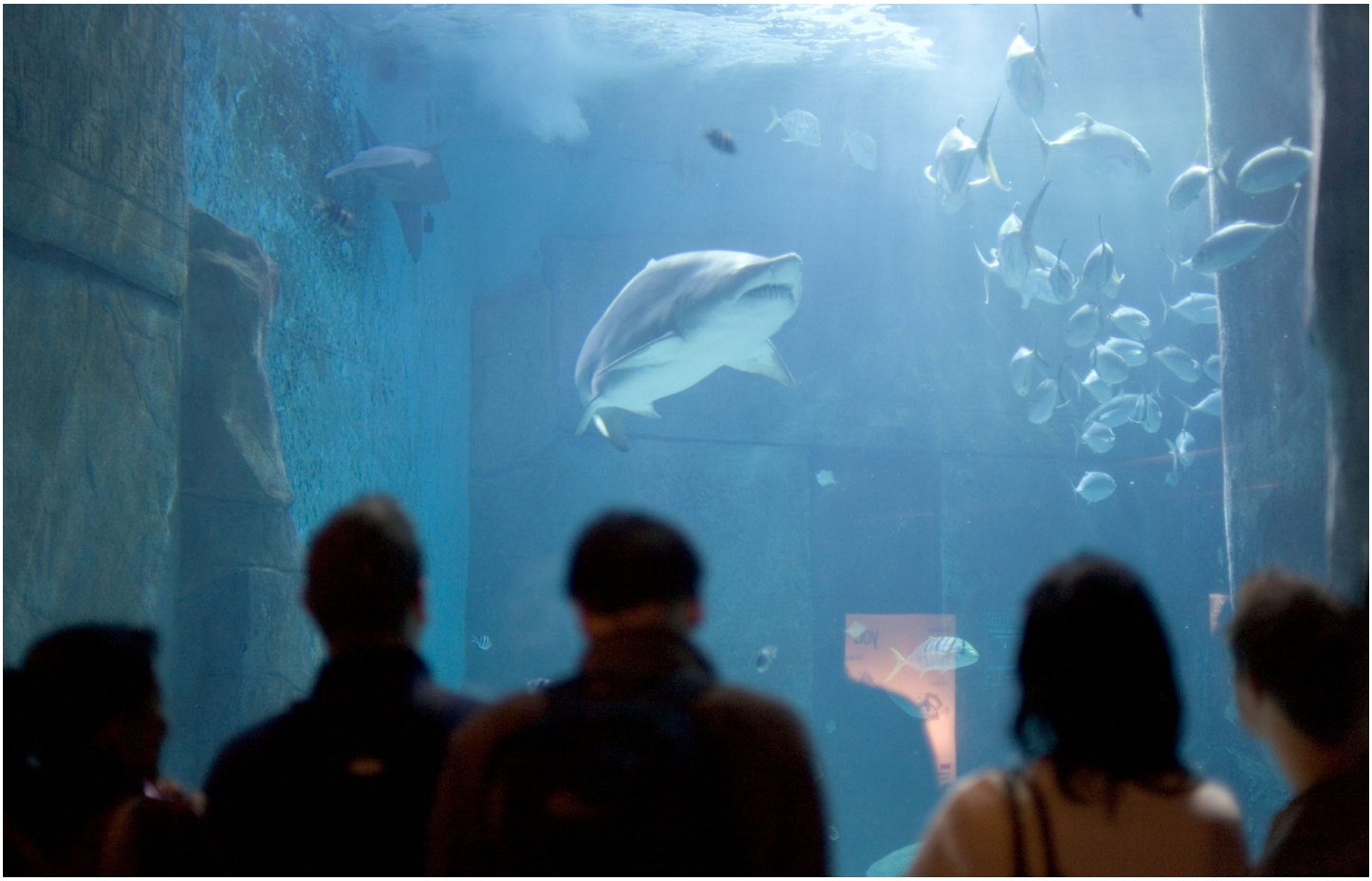
Deloitte.

CFO Insights
October 2018



Extended enterprise risk:
Managing exposure beyond the organization

A large global organization may have tens of thousands of suppliers, accounting for up to 80% of organizational costs.[1] It may also have a number of partnerships, alliances, and other business relationships with external parties, all of which have suppliers, partnerships, and alliances of their own. Indeed, in today's digitally interconnected world, business ecosystems are growing bigger and more complex than ever before—and while this drives a great deal of value, it also inevitably gives rise to extended enterprise risks stemming from external parties' actions.

Virtually every aspect of an organization is vulnerable to extended enterprise risk, and as organizations continue to evolve toward more complex ecosystems, these risks will likely only grow. Yet, while this is widely acknowledged, extended enterprise risk management (EERM) practices have remained relatively immature. At too many organizations, EERM processes fail to adequately consider extended enterprise risks—which not only exposes an organization to harm, but, worse, may even blind them to the possibility that harm could arise.

Why this failure? Partly, it's because of the sheer difficulty of monitoring and managing the myriad of value-creating activities that take place outside one's own legal control. However, the whole explanation isn't simply that EERM is difficult. It's also because many management teams and boards have yet to

›

powered by
The CFO Program

reset their concept of the "front line of defense" to include suppliers, customers, and others in the organization's broader system of stakeholders. At organizations where leaders have embraced this necessity, however, we have seen EERM efforts transform from peripheral, siloed activities[2] with an almost exclusive inward focus into enterprise-spanning programs that help protect organizations by collaborating with business partners across their industries.

The good news is that the pragmatic difficulties of managing extended enterprise risk are lessening, thanks to new technological and organizational approaches that can reduce the necessary investments and establish clear accountability for executing EERM activities. In this issue of *CFO Insights*, we describe three important areas of innovation—emerging technologies, cooperative relationships, and organization and governance models—that leading companies are pursuing to reset the front line of defense.

Emerging technologies: Monitoring and safeguarding the extended enterprise

Today, new technologies take the capacity to manage external-party risks to a whole new level. Moreover, such innovations are becoming ever-more accessible and cost-effective (see table 1). Among them:

- **Cloud computing.** The shared or private computing infrastructures that comprise today's "cloud" can be far more reliable, as well as more rapidly scalable, than traditional on-premise and proprietary computing. Risk-related data-sharing among multiple parties is one important activity that cloud computing can facilitate. The cloud can also play an important role in enabling third-party risk management service providers to efficiently deliver services, such as vendor background checks, vendor and risk monitoring, payment solutions, and the like—at a much lower cost than building and maintaining proprietary solutions.[3]
- **Robotic process automation (RPA).** RPA enables organizations to integrate information from disparate sources and systems without manual intervention. Some organizations are beginning to deploy RPA for sophisticated risk analysis. For example, critical data about external-party relationships can reside in multiple procurement systems and in emails, spreadsheets, and text documents. RPA tools can extract, highlight, and reconcile the information across multiple systems, improving EERM efficiency and scalability. RPA can also embed control mechanisms into an automated process, thus increasing efficiency and streamlining third-party transaction risk management.
- **Cognitive technologies.** Cognitive technologies, an umbrella term for a broad range of tools based on the science of artificial intelligence, can find a range of applications in EERM. For example, natural language processing now enables organizations to perform textual analyses that can yield early signals of critical risks, enabling third-party contracts to be automatically reviewed for potential risks arising from inadequate or unclear language.
- **Additive manufacturing (AM).** AM, also known as 3D printing, is a manufacturing technique that builds objects layer by layer using materials such as polymers, metals, and composites. In sectors where complex, reliable manufacturing is necessary, AM has helped simplify the extended enterprise supply chain by enabling companies to manufacture complex end parts onsite and on demand instead of sourcing them from a supplier. Some airlines, for instance, are selectively 3D printing certain small parts, rather than sourcing them from vendors.[4]
- **Internet of Things (IoT).** The IoT enables physical objects to communicate with each other. Sensors embedded across a value chain can be connected to the internet to monitor critical objects and their physical state in real time, reducing adverse selection and moral hazard risks in the supply chain. Furthermore, sensor data can be used to assess risks. For example, some insurance companies are using data feeds from sensors embedded in autos to adjust owners' risk premiums according to their driving habits. This capability is disrupting the traditional insurance model, which requires specialized third parties to manually collect data to calculate premiums.[5]

Table 1. Emerging technologies can help organizations execute and improve EERM

Technology	Description	Examples of EERM uses
Cloud computing	Subscription-based access to digital capabilities	• Data-sharing • Risk management provider service delivery
Robotic process automation (RPA)	Automated task execution across one or more information systems	• Data consolidation • Control automation
Data visualization	Visual representations of complex data	• Risk dashboards
Cognitive technologies	Tools based on artificial intelligence	• Textual analysis
Blockchain	Distributed digital ledger	• Contracting • Product tracking
Additive manufacturing (AM)	Building physical objects layer by layer	• Onsite manufacturing
Internet of Things (IoT)	Sensors connecting physical objects to each other	• Product tracking • Behavior monitoring

Source: Deloitte analysis of client experience

Cooperative relationships: The rise of collaborative risk management platforms

Third parties to facilitate risk management—for instance, credit bureaus that provide consumers' credit scores, payment

histories, and other risk information to lenders—aren't new. What has changed,however, is the greater scale and scope of risk control that new digital technologies and platforms now enable. Given the extensive economies of scale that can be realized by pooling risk management activities, organizations are becoming more open to establishing cooperative agreements to share the costs of complex technology-enabled third-party risk management.

The financial services industry is on the cutting edge of these agreements, partly because risk management and regulatory controls in this sector have grown in recent years following significant regulatory fines. For example, a number of banks participate in IHS Markit's Know Your Third Party platform (KY3P)[6]—the first centralized cloud-based community for simplifying and standardizing third-party risk management.

As new technologies proliferate and organizations become more aware of the potential to realize economies of scale, we expect more third-party risk services like KY3P to emerge. One approach may be to offer "shared utilities" where the risk service provider conducts standard assessments that are shared across a group of organizations. Another approach is a more "bespoke utility" model in which the service provider conducts specialized assessments tailored to a particular organization's risk tolerance. In all cases, when constructing "utilities" for cooperative risk management, organizations should be careful to avoid any collusion for setting prices, reducing competition, or exercising monopoly power through the collaboration.

Organization and governance: Driving execution and accountability

To effectively leverage new technologies and cooperative arrangements for EERM, top management needs to organize to effectively execute EERM, and boards should provide risk oversight to verify that effective EERM practices are in place. For these leaders, this means finding answers to two often-difficult questions: *Who owns external-party risks in the organization?* And *where does external-party risk management sit in the enterprise?*

At many organizations, EERM has historically been managed in silos or using a distributed structure that disperses EERM activities by category of risk. However, as various external-party risk incidents expose significant vulnerabilities, top management and boards in industries such as pharmaceuticals and financial services are reconsidering this approach. The current trend is toward federated and centralized models of EERM organization (see Figure 1). In a federated model, EERM guidelines and oversight are centralized, while process execution remains distributed. A centralized model further consolidates process execution into a single group, which can enable the greatest amount of risk control and cross-firm risk visibility and the least variance in risk management processes across business units.

Beyond the importance of top management putting in place a federated or centralized operating model for EERM, boards of directors also play a key role in corporate risk oversight. This need, however, has not always been recognized. In the standard

Figure 1. Many organizations are moving toward more centralized EERM operating models

	Distributed	Siloed	Federated	Centralized
EERM anchored	Business unit/ geographic unit	Risk domain-specific (e.g., financial, cyber)	Centralized oversight and distributed execution	Centralized planning, oversight, and execution
Pros	Agility, empowerment	Simplicity, independence	Transparency, empowerment	Highest visibility, assurance
Cons	Lack of enterprise- level visibility, control, and consistency	Potential for unprioritized increases in compliance requirements	Requires management commitment to EERM	Least flexible from business point of view

Source: Deloitte analysis of client experience

"three lines of defense" model issued by the Institute of Internal Auditors (IIA) in 2013,[7] EERM is viewed as primarily a first or second line of defense activity. Staff in the business functions compose the first line, responsible for owning, managing, and taking corrective action for extended enterprise risks in their respective areas. Staff in organizational functions that oversee and guide common risk management processes, such as risk management and compliance, make up the second line. The third line of defense, composed of teams that provide independent assurance on risk management—typically represented by internal audit functions—then evaluate and report on extended enterprise risks as part of their overall risk assurance activities.

As extended enterprises grow and more external-party risk events lead to significant value losses, some risk experts believe that the "three lines of defense" framework should be updated to include a "fourth line of defense" that places explicit responsibility on boards and senior management to get ahead of risk events. Indeed, the 2018 Deloitte Global EERM survey (see sidebar) highlights the growing need for enhanced accountability for EERM at the board and the C-suite levels: More than half of this survey's respondents, in fact, viewed the board, CEO, CFO, and CRO as accountable for external-party risk management.[8]

The board's role as the fourth line of defense is, first, to ask management to establish a clear organizational model and process for EERM. The board also should require management to provide a clear line of sight to the organization's most significant extended enterprise risks, as well as an explanation of how management intends to manage these risks. For their part, senior management should create an accountable EERM organization where processes, technologies, and external-party relationships are efficiently and effectively managed. Another critical management responsibility is to establish an effective reporting system to keep the board informed of how management is addressing critical risks. Many of an organization's greatest value losses occur from a series of cascading and interdependent risk events.[9] Elevating systemic EERM review to boards and senior management can do a great deal to limit risk events from escalating into material events.

Resetting the front line of defense

The modern organization is growing ever more complex as actors in today's networked economy seek scale and specialization advantages. As value and risk from the extended enterprise grow, the front line of defense should be reset beyond organizational boundaries to the broader network that delivers value to customers. Fortunately, new technologies and cooperative arrangements make possible dramatic improvements in EERM. To take advantage of these new technologies, it is critical for boards to hold management responsible for building an effective EERM organization and to establish, when needed, formal mechanisms to exercise oversight. In turn, senior management should consider creating federated or centralized EERM organizations, leverage emerging technologies, and create cooperative relationships to safeguard the value derived from relationships with external parties, and to protect the organization.

Global EERM survey: Growing awareness, slowing pace to maturity

Even as organizations grow increasingly dependent on third-parties to achieve their goals and objectives, their progress toward developing a mature extended enterprise risk management (EERM) program may not be advancing at the expected pace.

That finding, among others, emerged from Deloitte Global's third annual EERM survey, "Focusing on the climb ahead." The survey responses reflect the views of 975 senior leaders from a variety of organizations in 15 countries across the Americas, Europe, Middle East, and Africa (EMEA), and Asia Pacific.

Reliance on third parties continues to rise, with 53% of respondents reporting "some" or "significant" increase in their level of dependence on third parties. While 70% believe that business and macro-economic uncertainties have increased the risks of managing an extended enterprise, just 20% of respondents say their organizations have streamlined their EERM systems and processes.

As for organizations that have yet to do so, 53% now believe it will take two to three years or more to achieve EERM maturity. That time-frame represents a significantly longer journey than anticipated in earlier surveys, when respondents reported that this could be achieved in six months to a year.

The pace may accelerate if boards were to grow more engaged. The survey found that globally 38% of board members have lower to insignificant levels of engagement on the EERM agenda. Among US respondents, 23.5% say their board members have lower to insignificant levels of engagement.

But boards may become more attentive as the business case for EERM investment evolves. Among US respondents, more than 46% of respondents considered investment in EERM a revenue-generating opportunity—compared with just 21% globally.

Endnotes

1. Institute of Risk Management, *Extended enterprise: Managing risk in complex 21st century organizations*, 2014.
2. By "siloed," we mean that risks are owned and managed by multiple groups within the enterprise. These groups may fall along organizational lines, with each function or business unit managing its own risks in its own way, or they may organize around individual risk areas, such as financial risk or cyber risk.
3. Deloitte, Mastering the migration to cloud computing: Survey of federal leaders, November 2017.
4. Emirates, "Emirates brings in a step change in 3D printing for aircraft parts," November 16, 2017.
5. Chris Nordlinger, "The Internet of Things and the end of the auto insurance industry as you know it," Medium, March 17, 2015.
6. IHS Markit "Barclays, Goldman Sachs, HSBC and Morgan Stanley invest and obtain equity stake in KY3P® by IHS Markit," press release, MarketWatch, June 6, 2017.
7. The Institute of Internal Auditors North America, "The three lines of defense in effective risk management and control: Is your organization positioned for success?," January 14, 2013.
8. Deloitte, Focusing on the climb ahead: Extended enterprise risk management survey 2018, 2018.
9. Deloitte, The value killers revisited: A risk management study, 2014.

*For an expanded version of this article, please see "Resetting the front line of defense," Deloitte Insights, Deloitte LLP, September 20, 2018.

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career—helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

Contacts

Dan Kinsella
Partner, Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
dkinsella@deloitte.com

Ajit Kambil
Global Research Director, CFO Program
Deloitte LLP
akambil@deloitte.com

Sanjoy Sen
Head of Research and Eminence, Extended Enterprise Risk Management practice
Deloitte LLP
sanjsen@deloitte.co.uk

Charan Puneet Singh
Senior Consultant
Deloitte Canada
chandrsingh@deloitte.ca

For more information about Deloitte's CFO Program, visit our website at: www.deloitte.com/us/thecfoprogram.

Follow us @deloittecfo

Deloitte CFO Insights *are developed with the guidance of Dr. Ajit Kambil, Global Research Director, CFO Program, Deloitte LLP; and Lori Calabro, Senior Manager, CFO Education & Events, Deloitte LLP.*