Deloitte.
Insights

FEATURE

Resetting the front line of defense

Managing risk across the extended enterprise

Dan Kinsella, Ajit Kambil, Sanjoy Sen, and Charan Puneet Singh

Today's broad business ecosystems create undeniable value—but they also generate risks. How can organizations better manage extended enterprise risk to limit exposures arising from external parties in their network?

A discipline ripe for innovation

A LARGE GLOBAL organization may have tens of thousands of suppliers, accounting for up to 80 percent 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 arising from external parties' actions.

Virtually every aspect of an organization—shareholder value, brand and reputation, profit and loss, employee engagement, operations—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, our experience suggests that 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, in our view, isn't simply that EERM is difficult. It's also that many management teams and boards have yet to reset their concept of the "front line of defense" to include suppliers, customers, and others in the organization's broader system of stakeholders. Granted, this shift in mindset entails accepting and addressing the challenges of managing risk across a dizzying array of external parties—but the results can be dramatic. At organizations where leaders have embraced this necessity, 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 and mitigating extended enterprise risk are lessening, thanks to new technological and organizational approaches that can bring the necessary investments down to a manageable level and establish clear accountability for managing and executing EERM activities. In the pages that follow, we describe three important areas of innovation that we have seen leading companies pursue to "reset the front line of defense":

- **Emerging technologies** that help mitigate risks, enhance trust, establish a single version of the truth, and facilitate monitoring and coordination
- **Cooperative relationships** that give organizations access to economies of scale and specialized EERM capabilities
- **Organization and governance models** that clearly guide execution and assign responsibility, authority, and accountability for EERM

Emerging technologies: Monitoring and safeguarding the extended enterprise

Historically, digital technologies found their earliest use in enabling companies to coordinate with and monitor third parties to reduce transaction costs. New technologies available today, however,

now take the capacity to manage external-party risks to a whole new level.

Imagine the following scenario. Certain diabetes patients need an injectable medicine that must be maintained at between 45 and 70 degrees Fahrenheit to be effective. Temperature sensors on the boxes of injection pens note the boxes' temperature every 15 minutes, and write the recorded temperatures to a blockchain record at each stage of delivery and distribution. This record allows pharmacists to verify that the medicine's efficacy has not been compromised due to temperature before dispensing it to a patient. By scanning or photographing a bar code on an injection pen, patients can also review the blockchain record to confirm the medicine's quality and provenance. Further, sensors on the pens record when patients inject themselves, again using blockchain technology to store the information. Connected to physicians' record-keeping systems via the Internet of Things (IoT), the sensor data allows doctors to monitor their patients' adherence to their treatment regimen.

While this scenario may be hypothetical, the technologies to enable it already exist (see table 1), and they are becoming more accessible and cost-effective with each passing year. Among them:

Cloud computing. Today, ready access to off-the-shelf, subscription-based, cloud-enabled digital capabilities can enable small companies and startups to achieve competencies similar to those of their larger rivals at a fraction of the cost, with almost no wait time, and potentially at a lower risk of failure. The shared or private computing infrastructures that compose 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 help make cheaper and easier. 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 risk monitoring, payment solutions, and the like—at

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.

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 business systems without manual intervention. Many organizations are already using RPA for processing invoices and conducting compliance checks; some are beginning to redeploy it to more sophisticated risk analysis. For example, critical data about external-party relationships can reside in multiple procurement systems as well as in emails, spreadsheets, and text documents. Where manually consolidating this data would be prohibitively labor-intensive, RPA tools can extract, highlight, and reconcile the information across multiple systems with relatively little human intervention, 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. One company used RPA to reduce the time needed to generate a purchase order across multiple third parties from several days to less than five minutes.

Data visualization. Data visualization tools are becoming increasingly important in focusing attention on critical risks, enabling organizations to build risk dashboards that can help them identify extended enterprise risks that may otherwise be difficult to systematically spot and address. For example, a data visualization tool could help an agricultural company identify patterns in disease progression that might impact crop yields and the supply and price of critical inputs.

Data visualization tools are becoming increasingly important in focusing attention on critical risks.

Cognitive technologies. Cognitive technologies, an umbrella term for a broad range of technologies 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. Such automation can save companies time and money, not only by reducing the need for attorneys and other specialized human service providers, but by driving greater consistency. One organization with more than 12,000 third-party relationships is using natural language processing technology to review contracts and standardize their language, allowing for standardized reporting procedures that help the organization manage its contracts much more efficiently.[4]

Blockchain. Blockchain offers organizations a way to create a distributed digital ledger that is shared among a network of participants to hold "a single version of the truth." By enabling a single, shared, immutable transaction record, blockchain can help organizations shorten lengthy and expensive settlement and reconciliation times, avoid system breakdowns, and improve clarity about risk exposures. Blockchain-enabled "smart contracts" with external parties can be partially or fully executed and enforced with minimal human interaction, enabling greater efficiency. The transparency into events that blockchain affords—making visible actions across the entire extended enterprise—can also have a significant impact on EERM efficacy.

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 reduce lead time and 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, as sourcing these from vendors is costly, takes a long time, and causes inventory problems.[5]

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 (such temperature or stresses) in real time, reducing adverse selection and moral hazard risks in the supply chain. As in our illustrative pharmaceuticals example, sensors writing to a blockchain can provide tracking and compliance information across the value 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, awarding lower premiums to drivers with safe records and charging higher premiums to drivers with riskier driving habits. This capability is disrupting the traditional insurance model, which requires specialized third parties to manually collect data to calculate premiums.[6]

The evolution of managed service providers, together with shared utility providers for third-party management, is offering client organizations flexible options for addressing their extended enterprise risks.

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—have existed for years. What is different today, 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 types of cooperative 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).[7] The platform is the first centralized cloud-based community for simplifying and standardizing third-party risk management. It enables organizations to communicate multilaterally or on a one-to-many basis to support vendor due diligence and ongoing monitoring, making it more efficient to manage vendor risks.

As new technologies proliferate and organizations become more aware of the potential to realize economies of scale, we expect more collaborative platforms and 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. Some of these shared utility providers appear to be broadening their scope to act as managed service providers, thus offering their client organizations flexible options for addressing their third party-related challenges. Another approach is a more "bespoke utility" model in which the service provider conducts specialized assessments tailored to a particular organization's risk tolerance and specialized risk assessment needs. 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

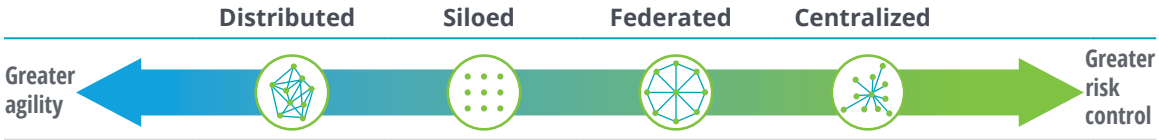
To effectively leverage new technologies and cooperative arrangements for EERM, top management needs to organize to effectively execute EERM, and boards should provide risk oversight and governance to verify that effective EERM practices are in place. For these leaders, this means finding solid answers 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 we have seen, 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, financial services, automotive, and industrial products are reconsidering this approach. The current trend is toward federated and centralized models of EERM organization (figure 1), with many organizations increasingly recognizing the need to move toward at least a federated model to effectively control EERM risks. 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 and risk management governance. This need, however, has not always been recognized. In the standard "three lines of defense" model issued by the Institute of Internal Auditors (IIA) in 2013,[8] EERM is viewed as primarily a first or second line of defense activity. Staff in the business functions—typically reporting to operating management—compose the first line of defense, responsible for owning, managing, and

FIGURE 1

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.

taking corrective action for extended enterprise risks in their respective functional areas. Staff in organizational functions that oversee and guide common risk management processes such as risk management and compliance—often reporting through multiple layers to executive management—make up the second line of defense. The third line of defense, composed of teams that provide independent assurance on risk management—typically represented by internal audit functions that report to an independent audit committee—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 through concerted risk management efforts and governance. Indeed, the 2018 Deloitte Touche Tohmatsu Limited global EERM survey 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 viewed the board, CEO, CFO, and CRO as accountable for external-party risk management.[9] (While the CRO role today is largely limited to financial services organizations, some other industries, such as hospitality and manufacturing, are also starting to appoint CROs.)

Although we recognize that they are already very busy, as extended enterprises expand and third-party networks grow in strategic importance, we expect that boards will understand the need to play a more active role in reviewing third-party risks. Today, the board's risk oversight responsibilities typically rest with the audit committee. However, audit committees in a post-Sarbanes–Oxley world are not only extremely busy, but tend to focus on accounting and financial risks. A board-level "fourth line of defense," therefore, should dedicate separate resources to conducting more systemic and broader oversight of strategic and operational EERM risks. Some leading boards, for instance, are creating dedicated "risk committees" whose mandate includes oversight of EERM. Others may establish committees focused specifically on overseeing external-party risk management, while others may wish to examine these risks as part of the work of the whole board.

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 mitigate or 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 without letting key risks fall through the cracks of the first, second, or third lines of defense. Another critical management responsibility is to establish an effective reporting system to keep the board informed of critical external-party and other risks and of how management chooses to address those risks.

Many of an organization's greatest value losses occur from a series of cascading and interdependent risk events.[10] Elevating systemic EERM review to boards and senior management can do a great deal to enable risk mitigation strategies that limit risk events from escalating into material events.

Resetting the front line of defense

The modern organization is an extended enterprise that 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 existing and future customers. Fortunately, new technologies and cooperative arrangements make possible dramatic improvements in EERM. To take advantage of these new technologies and approaches, 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 over EERM oversight. In turn, senior management should consider creating federated or centralized EERM organizations, leverage emerging technologies, and create cooperative relationships to deliver an EERM process that is thoughtfully managed, safeguards the value derived from relationships with external parties, and protects the organization.

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. Deloitte, *Cognitive advantage: Driving real business outcomes with cognitive technology solutions*, accessed August 21, 2018.
5. Emirates, "Emirates brings in a step change in 3D printing for aircraft parts," November 16, 2017.
6. Chris Nordlinger, "The Internet of Things and the end of the auto insurance industry as you know it," Medium, March 17, 2015.
7. 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.
8. 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.
9. Deloitte, *Focusing on the climb ahead: Extended enterprise risk management survey 2018*, 2018.
10. Deloitte, *The value killers revisited: A risk management study*, 2014.

About the authors

DAN KINSELLA, a Deloitte Risk and Financial Advisory partner, is the extended enterprise and third-party assurance leader for Deloitte & Touche LLP. He combines business and technology experience to help organizations create and optimize their extended enterprises through cost and revenue recovery services. Kinsella also leads the Advisory Service Delivery Transformation practice, helping organizations improve their shared services and outsourcing efforts.

AJIT KAMBIL is the global research director of Deloitte LLP's CFO program, overseeing its diverse research initiatives in areas such as leadership, capital markets, and risk. He created CFO Insights, a biweekly publication serving more than 35,000 subscribers, and also developed Deloitte's Executive Transition Labs, which help CxOs make an efficient and effective transition into their new role. Prior to this, Kambil was the global director of Deloitte Research.

SANJOY SEN is the head of research and eminence for the Extended Enterprise Risk Management practice at Deloitte LLP. He has over 26 years of experience in risk and governance in the United Kingdom, Gibraltar, and various countries in the Middle East and in India. He has assisted clients with strengthening their corporate governance mechanisms, establishing enterprisewide risk management frameworks to support governance, and reviewing and addressing specific business and technology risks. Sen is also a doctoral research scholar at Aston Business School, UK, specializing in strategic governance related to third-party risk.

CHARAN PUNEET SINGH has over 10 years of experience in corporate strategy, business development, and business consulting across the United States, the United Kingdom, and India. He has worked on large risk advisory engagements, helping clients with issues around strategic risk, brand and reputation risk, enterprise risk management, and third-party risk management.

Contact

Dan Kinsella
Partner
Deloitte Risk and Financial Advisory LLP
+1 402 997 7851
dkinsella@deloitte.com

Jan Corstens
Global leader
Extended Enterprise Risk Management
+32 2 800 24 39
jcorstens@deloitte.com

Kristian Park
EMEA leader
Extended Enterprise Risk Management
+44 20 7303 4110
krpark@deloitte.co.uk

Jimmy Wu
Asia Pacific leader
Extended Enterprise Risk Management
+88 6225459988
jimwu@deloitte.com.tw

Deloitte.
Insights

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

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Junko Kaji, Abrar Khan, Rupesh Bhat, Blythe Hurley, and Preetha Devan

Creative: Kevin Weier, Adamya Manshiva

Promotion: Shraddha Sachdev

Cover artwork: Jesús Sotés

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