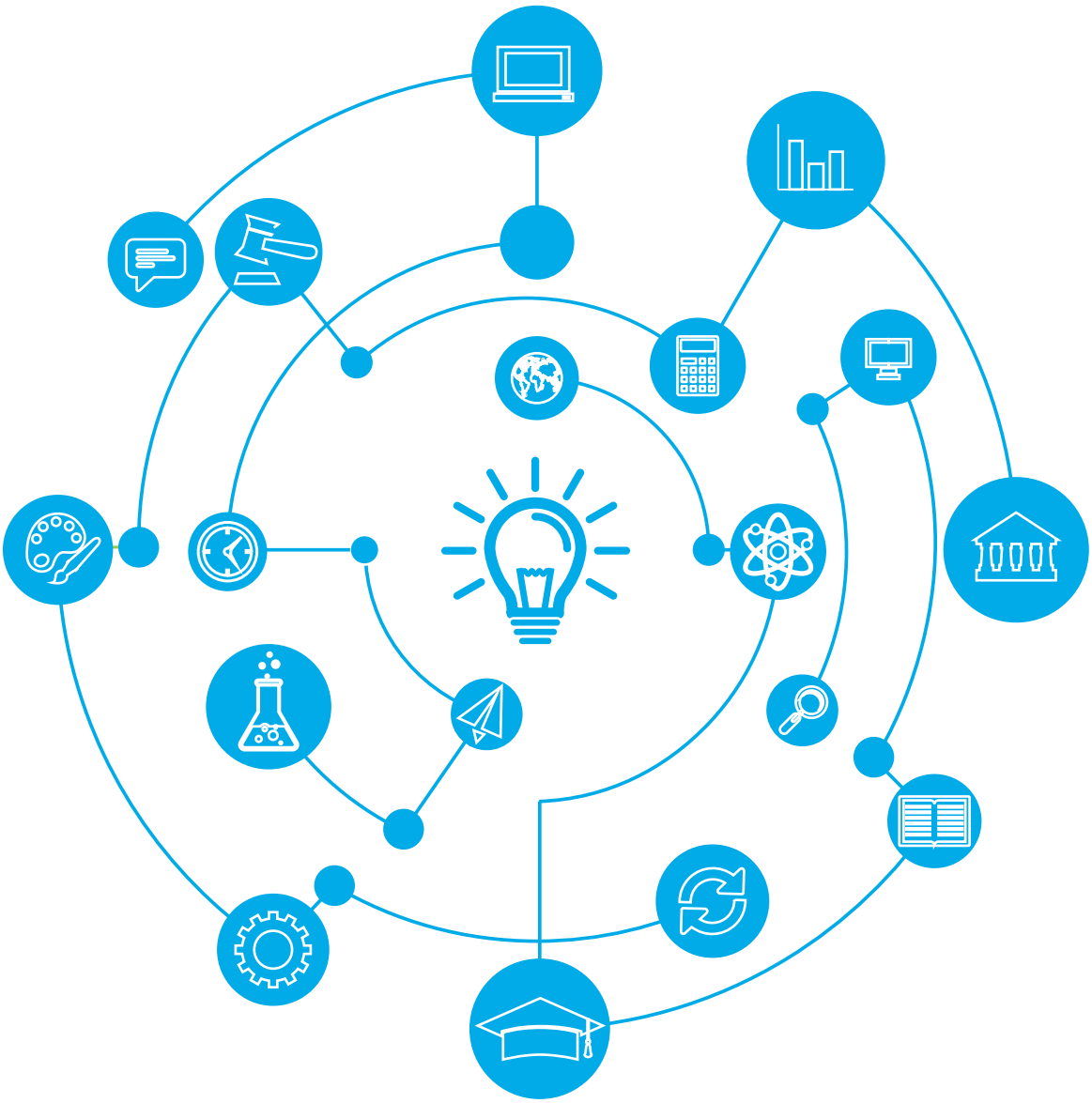
Deloitte.



Extended Enterprise Risk Management

Driving performance through the third-party ecosystem

Taken together, these third parties—who may hail from around the corner or around the globe—constitute what we have termed "the extended enterprise."

In a globalized business environment, no company is an island. The ecosystem of a typical company comprises an exceedingly large number of third parties. In general, a third party is any individual or entity with which the company does business, including customers, partners, agents, affiliates, vendors, and service providers. Taken together, these third parties—who may hail from around the corner or around the globe—constitute what we have termed "the extended enterprise." Already extensive, the reach of the extended enterprise is poised to expand. Outsourcing, for instance, is expected to continue to grow at rates of 12–26 percent per annum across functions, according to the Deloitte Consulting 2014 Global Outsourcing and Insourcing Survey.

As the extended enterprise reaches farther, and accordingly becomes more complex, companies acknowledge the need to manage their exposure to the actions of third parties in a strategic and proactive manner. Many businesses turn to point solutions that facilitate regulatory compliance or address high-profile vulnerabilities such as cyber security, often without consistently tying them to strategy. This fragmented approach, when not guided by an overarching vision, is no longer sufficient to mitigate interconnected third-party risks throughout the enterprise and to avoid the consequences, which are escalating. But, how can a company go about formulating strategies for managing the extended enterprise and driving performance at the same time? And perhaps even more challenging, how can it justify the investment required to implement those strategies through a coordinated program?

In our experience, the answers lie in expanding one's view of extended enterprise risk management to include value creation as well as value protection. Extended enterprise risk management can be a proactive lever for driving business performance, although most businesses see it mainly as a reactive means of protecting existing worth. In order for organizations to leverage their risk management processes to improve performance, it is critical to develop an end-to-end approach for sensing risks systematically throughout the extended enterprise so that vulnerabilities can be addressed proactively. This approach is also known as extended enterprise risk management.

Definition of extended enterprise risk management

Extended enterprise risk management is the practice of anticipating and managing exposures associated with third parties across the organization's full range of operations as well as optimizing the value delivered by the third-party ecosystem. What does third-party risk look like? While one often thinks of data breaches involving IT providers, the tentacles of third-party risk extend into the farthest corners of the extended enterprise ecosystem.

Consider these scenarios:

- An outsourced vendor for transaction processing decides to exit the business and provides little notice or transitional support
- An important distributor does not provide the amount of prime shelf space that had been agreed upon and instead leads with a competitor's product
- A contracted supplier does not deliver merchandise on-time, thus disappointing customers and damaging the company's brand reputation
- A customer organizes a boycott of the company's products via social media
- A critical vendor takes on more new accounts than it can handle, degrading service levels and disrupting processes
- A sales agent routinely favors a competitor, causing revenue and market share to decline in an important region
- Several franchisees do not spend co-op advertising dollars as instructed, resulting in a poor consumer response to holiday promotions

Clearly, the spectrum of third-party risk is broad. It is challenging to define and catalog the full range of exposure because third-party risk is not a risk unto itself; rather, it is a combination of diverse risks with various degrees of severity based on the nature of the relationships an organization has with its third parties.

Until recently, incidents related to the behavior and security practices of third parties were often inconvenient, but rarely catastrophic—and few even considered the possibility that proactive management of third-party risks across the extended enterprise could drive performance. Today, three forces are elevating the need for extended enterprise risk management and the benefits associated with it to new heights: 1) social media accelerates stakeholder reactions to third-party events, rapidly raising brand awareness, or conversely inflicting immediate reputational damage, if an incident goes viral; 2) the stakes are much higher, often

affecting profitability for better or worse; and 3) companies are using outsourcing to a greater degree for both core and non-core processes. As a result, third-party incidents today can dramatically impact business performance—positively or negatively—by affecting cost, service quality, revenue, and brand.

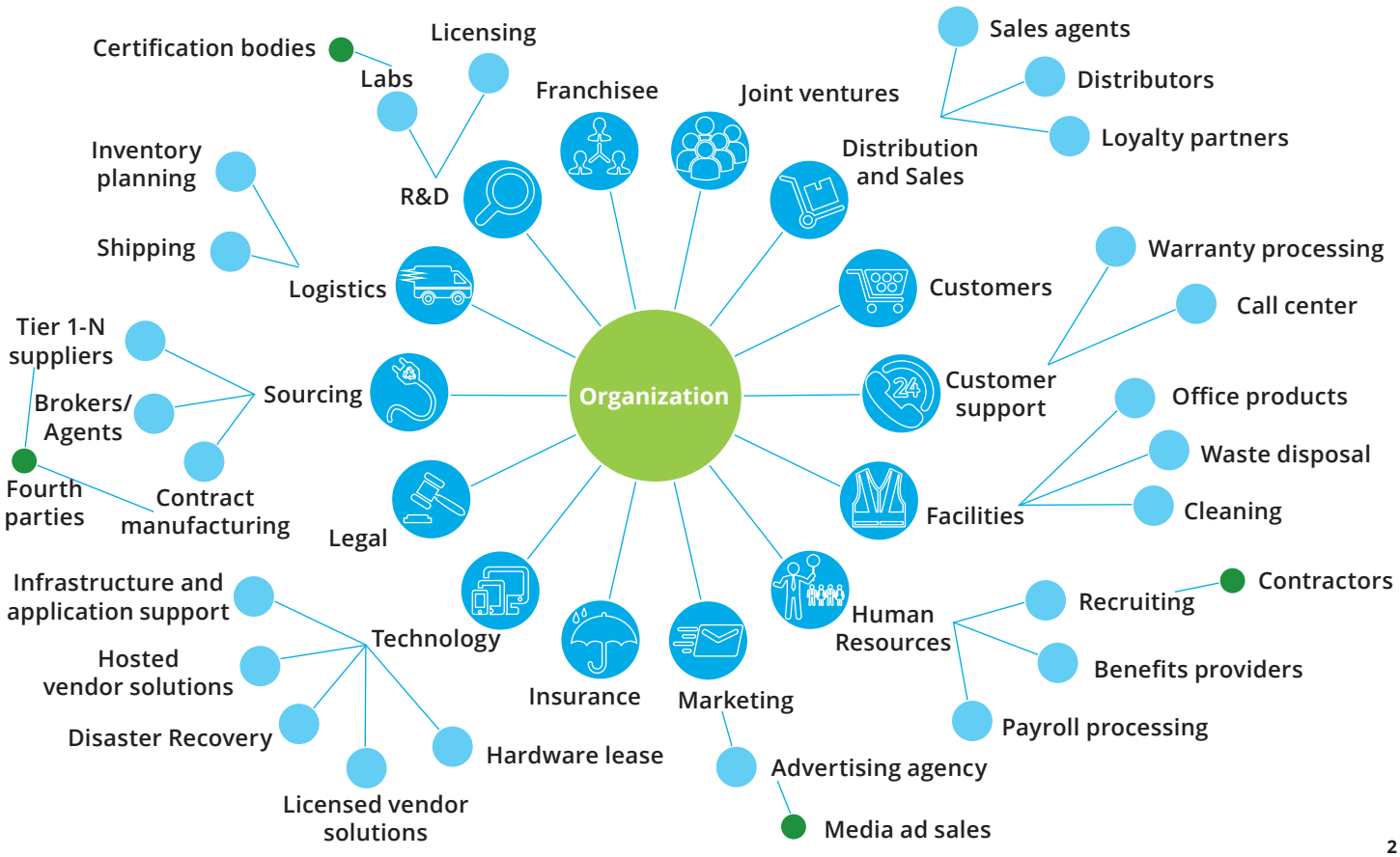
Cost: Escalation vs. containment

Most companies know that a third-party incident can cost them dearly, but few realize just by how much. In terms of downside losses, there are several ways in which companies can incur unnecessary expenses, expose themselves to fines, or be held responsible for restitution—not to mention the opportunity costs associated with not being able to serve existing customers or to pursue new business in the wake of a disruptive event. However, one of the more prominent and more costly risks associated with third parties is regulatory non-compliance. This pressure is unlikely to ease anytime soon since regulatory scrutiny and associated penalties are intensifying throughout the world.

The US Foreign Corrupt Practices Act (FCPA) provides a poignant example. Enforced by the US Securities and Exchange Commission (SEC), the FCPA generally prohibits the payment of bribes to foreign officials to assist in obtaining or retaining business. It also requires issuers to maintain accurate books and records and "have a system of internal controls sufficient to, among other things, provide reasonable assurances that transactions are executed and assets are accessed and accounted for in accordance with management's authorization."[1] The FCPA can apply to prohibited conduct anywhere in the world and extends to publicly traded companies and their officers, directors, employees, stockholders, and agents. Importantly, "agents" can include third parties acting on the company's behalf, such as consultants, distributors, joint-venture partners and others.[2] The sanctions can be significant: since 2010, nine multinational companies have paid more than $100 million each to settle SEC charges and parallel criminal cases relating to FCPA violations.[3]

A network within a network

The Extended Enterprise is the concept that an organization does not operate in isolation, because its success is dependent upon a complex network of third-party relationships.



The consumer relationship is fragile. Customers are more prone to take their business elsewhere when they are disappointed or feel betrayed—even when the offending action was made by a third party several steps removed from company headquarters.

Cyber security is another area of top concern. In addition to bad publicity, the cost of a data breach is escalating, and if a third party is involved, it makes matters worse. According to an annual study conducted by the Ponemon Institute, the average cost paid for each lost or stolen record containing sensitive and confidential information increased more than nine percent from $136 in 2013 to $145 in this year's survey.[4] Notably, third-party involvement increases the cost of the data breach by $14.80 per record.[5] This can be a substantial amount of money, considering the large number of records that are often compromised in an incident.

Supply chain disruption, too, is frequently tied to third parties, and it is also becoming more costly. In an annual study conducted by the Business Resiliency Institute in 2014, almost one quarter of respondents (23.6%) reported annual cumulative losses of €1 million or more due to supply chain disruptions.[6] Additionally, 13.2 percent of respondents have recorded losses of €1 million or more arising from a single incident, up from 8.6 percent in last year's survey.[7] Who was to blame when things went wrong? Outsourcer service failure ranked among the top three causes of disruption, cited by 35.8 percent of respondents.[8]

Service quality: Degradation vs. optimization

Under pressure from boards and the C-Suite, upper-level managers today need not only to avoid the aforementioned financial consequences of third-party risk but also to manage contracts and performance in a manner that optimizes returns for the extended enterprise. Vendor management, however, is all too often neglected in terms of resource allocation. Deloitte's 2014 Global Outsourcing and Insourcing Survey indicated the market is currently underinvested in the area of vendor management, particularly when it comes to tools, methods and processes.[9] It is therefore not surprising that many survey respondents reported dissatisfaction with vendor performance. Nearly half said they are facing issues related to their service providers being reactive rather than proactive (49%), and delivering poor service despite achieving service levels (48%).[10]

In addition to not getting what they've paid for in terms of service, companies are often unaware of whether or not third parties are complying with their contracts and if they are remitting fees, royalties, etc., as required. As a means of enhancing third-party performance and optimizing revenue capture, more and more companies are discovering they can unlock value and reduce costs from a contract risk and compliance (CRC) program, which assesses contract terms and audits related transactions. Companies also have a tendency to underutilize or overutilize assets licensed from third parties, where software and IT represent a particularly egregious area of overspending or exposure to major fines. Here, a software asset management (SAM) program can help organizations mitigate the risk of inadvertently violating the terms of their licensing agreements while helping them avoid being over licensed. By some estimates, an effective SAM program has the potential to reduce company IT costs by up to 30 percent.[11]

Revenue: Contraction vs. expansion

The consumer relationship is fragile. Customers are more prone to take their business elsewhere when they are disappointed or feel betrayed—even when the offending action was made by a third party several steps removed from company headquarters. A study conducted by Javelin Strategy & Research found that consumers avoid doing business with organizations after a security breach, with financial and banking institutions, health care providers, and retailers losing up to a third of their customer/patient bases in the wake of an incident.[12]

While driving away customers is an unpleasant prospect, the revenue implications of a company's third-party risk management practices can just as well be positive. For instance, proactive efforts to manage the extended enterprise can open doors to revenue opportunities by qualifying a company to do business with other entities. For instance, a leading multinational retailer recently tightened its sourcing standards to include a "zero tolerance policy" for unauthorized subcontracting. Additionally, the retailer now requires its suppliers to validate that all input materials and components have been obtained from permissible harvests

While the focus is often on protecting the organization from downside losses, companies that proactively manage their third-party risks across the extended enterprise also stand to reap substantial upside benefits in terms of increased productivity

consistent with international treaties and protocols. From the supplier's point of view, tighter sourcing standards such as these could be a blessing or a curse—precluding some, while including others. From the buyer's standpoint, well-defined supplier standards, along with governance processes and enabling technologies, can form the backbone of a supply chain compliance optimization program. Such programs not only seek to ensure third-party adherence to policies and standards but also to drive revenue by aligning the extended enterprise with the company's broader business objectives such as improving product quality, entering new markets, and satisfying customer demands for sustainable sourcing.

Brand: Diminishment vs. enhancement

Last but not least, every type of third-party exposure discussed thus far ties into an overarching risk: the ever-present threat of brand damage. In today's interconnected world, trust equals value, with business leaders increasingly acknowledging the high financial impact of brand image and reputation. According to a study by the World Economic Forum, on average more than 25 percent of a company's market value is directly attributable to its reputation.[13] Furthermore, Deloitte Touche Tohmatsu Limited's 2014 Global Survey on Reputation Risk found 87 percent of executives rated reputation risk as more important than other strategic risks, and 88 percent said their companies are explicitly focusing on managing reputation risk.[14] Despite this focus, companies are still concerned about their readiness, saying they are least prepared to manage reputation risk drivers in areas beyond their direct control, such as third-party ethics and competitive attacks.[15] These types of situations, should they come to pass, require effective crisis management and decisive leadership not only to "fix the problem" but also to take advantage of associated opportunities to improve processes, strengthen vendor relations, and uphold the brand by being transparent and responsive.

Extended enterprise risk management drives value

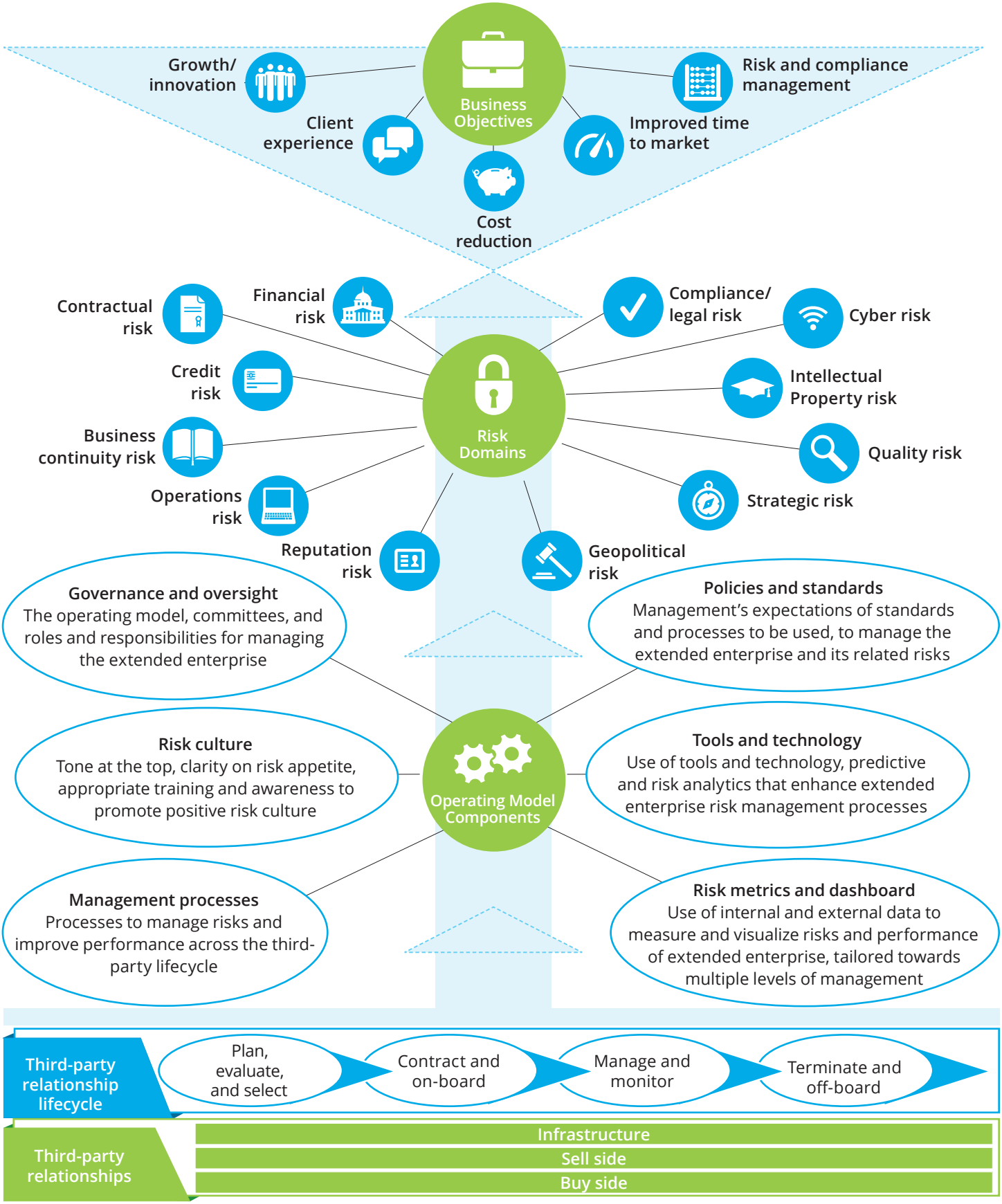
Third-party risk is causing much unease among executives and board members, and for good reason. A typical Fortune 500 organization may use as many as 10,000 suppliers to meet its business objectives.[16] Small- and mid-sized organizations may use hundreds of suppliers, if not thousands. Executives are increasingly realizing that each and every one of these relationships has the power to affect shareholder value, negatively or positively—and often exponentially in relation to the vendor's size and type of service provided. While the focus is often on protecting the organization from downside losses, companies that proactively manage their third-party risks across the extended enterprise also stand to reap substantial upside benefits in terms of increased productivity, contract and asset optimization, flexibility, and expanded growth opportunities. Put another way: an awareness is dawning that extended enterprise risk management drives value.

The case for a holistic approach

The risk management landscape is often fragmented and decentralized. Accordingly, many organizations approach third-party risk management on an ad-hoc and selective basis through point solutions, addressing prominent pain points such as cyber risk and mandatory regulatory compliance as they arise. In our experience, a broad, cross-enterprise view is often missing, with lack of ownership being a common theme. For instance, despite the increasing focus on risk management, some organizations still do not have a dedicated risk officer. We've also observed that many companies have not fully considered how to leverage the "three lines of defense" for managing risk and driving performance across the extended enterprise. The first line of defense is the business unit, which owns the third-party relationship and is accountable for managing associated risks in alignment with policies and procedures. The second line of defense is a centralized governance program for extended enterprise risk management, which is responsible for establishing and enforcing policies/processes to ensure that third parties are managed consistently by the business. And, the third line of defense is internal audit, which is charged with administering a robust audit program aligned to the most critical extended enterprise risks and controls as well as

A holistic approach

The Extended Enterprise management operating model presents a holistic approach to managing third-party relationships at various life cycle stages, while considering business objectives and risk domains across your Extended Enterprise.



performing independent assessments. Beyond underinvesting in the three lines of defense, many companies are additionally prone to focus on their spend, or looking for the low-cost provider, when engaging a third party, as opposed to focusing on the vendor's risk profile, control environment, and ability to drive performance. In short, many companies are attempting to "patch the leaks" in managing the extended enterprise as opposed to repairing the whole structure. In addition to the emphasis placed on cost reduction over the last few years, some believe this state of affairs can be attributed to the proliferation of third-party relationships and the escalation of risks that accompany them. The environment has changed, and few organizations have been able to keep up. At this point the question becomes: What should an organization do now?

In our view, companies increasingly need to move toward a holistic extended enterprise risk management program that emphasizes value creation as well as value protection. Organizations now have the opportunity to establish a systematic and proactive approach to managing risks across the third-party lifecycle, and in so doing, to unlock value and improve business performance. An operating model for implementing and integrating the various components of risk management across the third-party relationship lifecycle forms the foundation of this approach. To facilitate value realization, this model links the risk-management components to business objectives and risk domains across the extended enterprise.

Four cornerstone capabilities

Many companies believe they cannot take an end-to-end approach to managing the extended enterprise because securing executive sponsorship and getting people to take ownership can be an uphill climb. Furthermore, many businesses assume the task is too vast and they do not have the expertise and resources to build, execute, and sustain a comprehensive third-party oversight program. In our experience, these barriers are more perception than reality. It is neither necessary nor possible to do everything at once. It is rather a matter of identifying some practical steps to take toward establishing an extended enterprise risk management program or evolving an existing one. Most organizations can get a sense of what those steps might be by considering the extent to which they have developed the following cornerstone capabilities:

Strategy and governance: Creating an agile and flexible governance model
Does your organization link its risk management practices to value drivers? Does it have a formal strategy and governance model for managing third-party risk? Does it understand where the breakpoints are in its third-party relationships? Does it have a prescribed means of assessing and staying ahead of them? Does your organization proactively seek to bridge the gap between business executives and compliance and risk professionals?

People: Managing relationships, compliance and regulations
Does your company have dedicated roles for managing third-party risk across the extended enterprise? Has your organization aligned and strengthened its three lines of defense? Does executive ownership exist at the enterprise level? Are employees keeping up with emerging regulatory requirements? Are your third parties keeping up?

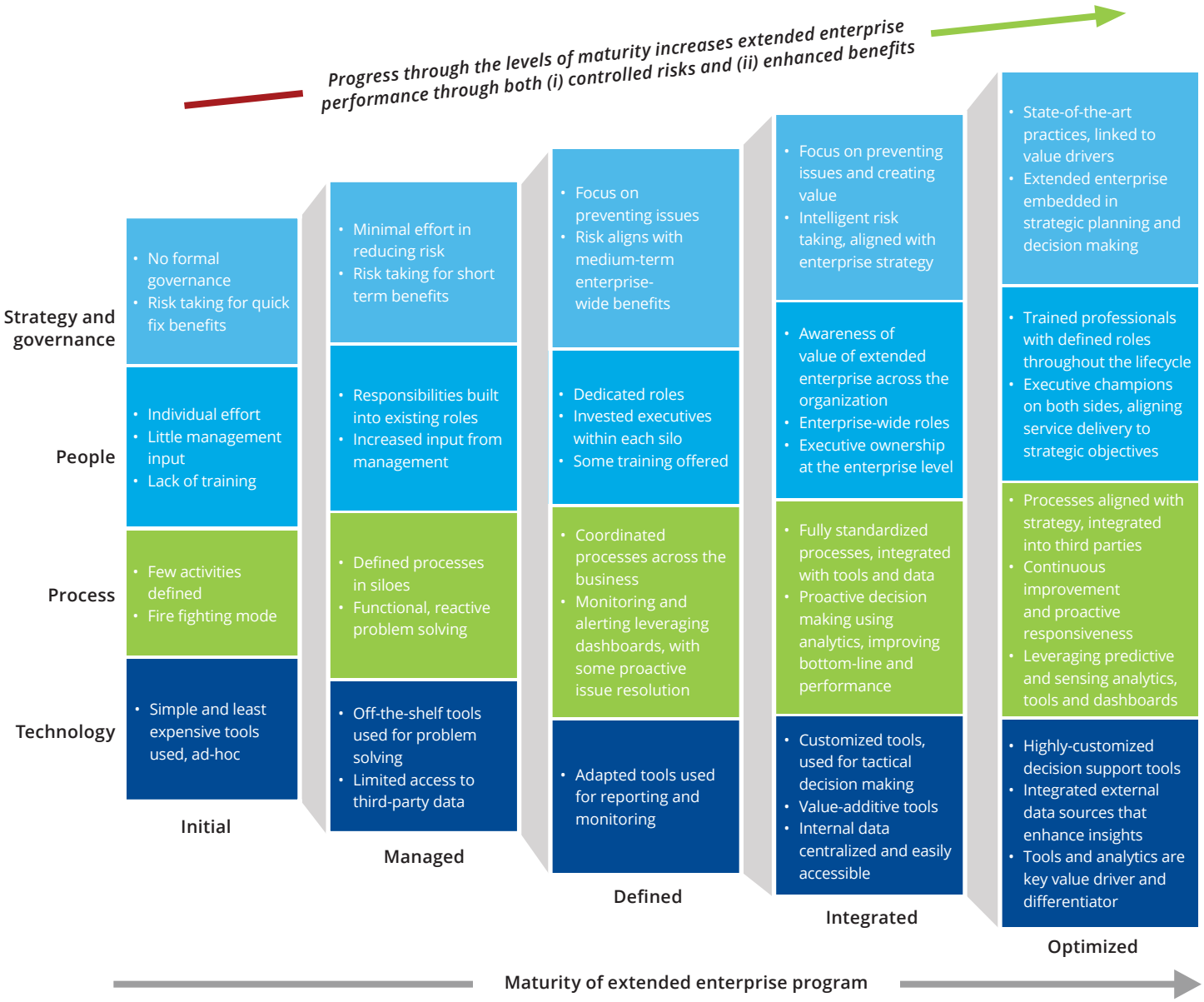
Process: Navigating events that shape the extended enterprise
Does your organization react to third-party events or does it actively seek to prevent them? Are risk management processes standardized across the enterprise and integrated with tools and data? Does your organization regularly consider how evolving technologies, market trends, and disruptive forces present opportunities and challenges to its third-party relationships? Does your organization have appropriate contracts in place with its third parties? Do you know if they are meeting expectations and complying with their contractual commitments? Can you readily assess the appropriateness of future delivery models? Are executives confident in their decisions to outsource or insource, build, or buy?

Technology: Using data and analytics to make informed decisions
What tools and technologies does your organization leverage to make informed decisions about its third-party relationships? What data does your organization already have access to? Can leaders make real-time decisions? If so, what key performance indicators does your organization monitor and analyze to support those decisions?

If you answered "no" to most of these questions, your company's extended enterprise risk management program is likely in the earlier stages of development, where the organization may be managing some third-party risks on an ad-hoc basis, using a few off-the-shelf tools, and perhaps beginning to implement dedicated roles and processes. More "yes" answers suggest it is further along the path toward integration and optimization—later stages of maturity that are generally characterized by greater use of customized tools, proactive monitoring and decision-making, and the connection of leading practices to value drivers.

How does your approach stack up?

The Extended Enterprise maturity model below is designed to help you understand where you are today, your ideal future state, the value the future state can bring to your organization.



Destination known: Improved business performance

Third-party risk is increasing for many enterprises, as are stakeholder demands for accountability and return on investment (ROI). When existing or impending regulations in certain industries are added into the mix, the potential cost of inaction becomes high. In this environment, complexity and resource constraints are no longer sufficient reasons to avoid taking an integrated approach to third-party risk management across the extended enterprise—neither is fear of the unknown. Wherever your organization stands on the maturity curve, there are some "next logical steps" that can be taken now to establish an extended enterprise risk management program or to move your existing risk-management practices to the next level. While the journey may be different, the destination is the same: improved business performance through controlled risks and enhanced benefits.

Risk management solutions

Deloitte brings together the full breadth of its capabilities into a comprehensive suite of solutions designed to increase the performance of the extended enterprise and help your organization achieve your strategic business objectives.

Strategy and program development

Solutions to assess, design, and implement strategically aligned extended enterprise program

- Governance and operating model design
- Strategic risk assessment, tiering, and segmentation
- Crisis management and simulation modeling
- Regulatory compliance

Evaluation and continuous monitoring

Solutions to assess third parties and proactively sense and respond to extended enterprise
risks and opportunities

- Third-party vetting and screening
- Risk sensing
- Third-party assessments
- Contract compliance assessments and optimization
- Benchmarking
- Analytics and visualization

Technology enablement

Solutions to transform and continuously enhance extended enterprise risk management by designing, implementing, and deploying technology solutions

- Intelligence
- Governance/program management
- Risk and compliance
- Knowledge management

The solutions range from those that can be integrated across the organization and/or to specific risk domains and specific third-party relationships.

Extended Enterprise risk management in action

From supply chain assessments to compliance audits and leading vendor-management practices, the following case studies illustrate the power of extended enterprise risk management strategies to drive business performance.

Case #1: Supply chain food safety assessment

A global Fortune 500 quick-serve restaurant chain sought to better manage supplier risks and to improve food safety in emerging countries. The company was particularly challenged to understand and sense food-safety risks not typically considered in the supply chain framework. To achieve these objectives, Deloitte assisted the company in defining a macro-environmental risk framework covering areas such as food safety hazards, third-party exposure, infrastructure and resources vulnerabilities, and local and international regulations. It also conducted brainstorming workshops to identify "unknown known" risks that may be emerging or currently under-appreciated. Based on the risks identified, a supplier risk assessment was developed and 15 international site visits were completed. Through these visits, Deloitte identified several improvement opportunities that could be broadly applied in emerging countries around the world. Deloitte also helped the company develop a future state framework for managing food-safety supply chain risk, giving the company a roadmap for better sensing risks and for transitioning from a rigid standards-based approach to a more-proactive model for managing the extended enterprise.

Case #2: Software license compliance

A global software company suspected that it was losing revenue through customer non-compliance with its licensing arrangements. The company engaged Deloitte to stem this revenue leakage. To do so, Deloitte first analyzed large volumes of data to identify high-risk third parties. It then performed compliance assessments of end customers, distributors, original equipment manufacturers (OEMs) and other third parties to identify revenue leakage in the extended enterprise. Ultimately, Deloitte assisted the organization in recovering lost revenue and provided guidance on prioritizing ongoing compliance audit activities. Building upon the success of these initiatives, the engagement has branched into similar assessments of other contractual relationships including licensing and royalty arrangements, hardware distribution channels, and working with end customers on software asset management (SAM) initiatives to help them maintain compliance with their contractual agreements and stop revenue leakage at the source.

Case #3: Vendor management assessment and performance dashboard development

Over the last five years, a large insurance company had reduced its gross expenses by 20 percent, while simultaneously increasing its dependency on third-party expertise. As a result, its extended enterprise expanded to comprise more than 2,400 vendors. However, its vendor management practices, including on-boarding and risk assessments, had not kept pace with the expansion. The company engaged Deloitte to conduct a holistic review of its vendor management strategy, lifecycle, and organizational structure, with the goal of helping the organization to maintain its bottom-line improvements while appropriately managing future demands, performance, and risks associated with third parties. To achieve these objectives, Deloitte conducted a leading-practice assessment of the company's vendor management operating model, including governance, organizational design, operational risk management, procurement authorization, and technology deployment. The main deliverable was a target-state operating model for vendor management, toward which the company is moving today. Additionally, Deloitte developed business requirements for performance dashboards to monitor key vendors and risks, and made recommendations on how the company could better use its third-party management technology.

Endnotes

1. "Spotlight on US Foreign Corrupt Practices Act," US Securities and Exchange Commission, https://www.sec.gov/spotlight/fcpa.shtml, accessed Jan. 20, 2015.
2. Ibid.
3. "SEC Enforcement Actions: FCPA Cases," US Securities and Exchange Commission, https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml, accessed Jan. 20, 2015.
4. "2014 Cost of Data Breach Study: Global Analysis," benchmark research sponsored by IBM, independently conducted by Ponemon Institute LLC, May 2014, pp. 1-3.
5. Ibid.
6. "Supply Chain Resilience 2014: An international survey to consider the origin, causes, and consequences of supply chain disruption," The Business Continuity Institute, p. 4.
7. Ibid.
8. Ibid.
9. "Deloitte's 2014 Global Outsourcing and Insourcing Survey: 2014 and beyond," pp. 11-12.
10. Ibid.
11. Fischer, Matt. "Saving Money Through Software Asset Management," Computer Weekly, http://www.computerweekly.com/opinion/Saving-money-through-software-asset-management, accessed January 21, 2015.
12. Sales Drop as Corporate Data Breaches Rise According to New Study from Identity Finder: Javelin Research Findings Quantify the Costs of a Data Breach and Effect on Consumer Spending," press release, April 29, 2014, http://www.identityfinder.com/us/Press/20140428164358
13. World Economic Forum, 2012.
14. "Deloitte 2014 Global Survey on Reputation Risk: Reputation@risk," October 2014, www.deloitte.com/reputationrisksurvey, pp. 4, 11.
15. Ibid.
16. "Vendor Management Program Office — Five Deadly Sins of Vendor Management," Deloitte 2013The long-term global trend toward lower levels of violence is explored in Steven Pinker, The Better Angels of Our Nature: Why Violence Has Declined (Penguin Books, 2012).

Contacts

For more information, please contact:

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

For further information, visit our website at www.deloitte.com/us/extendedenterpriserisk

Deloitte.