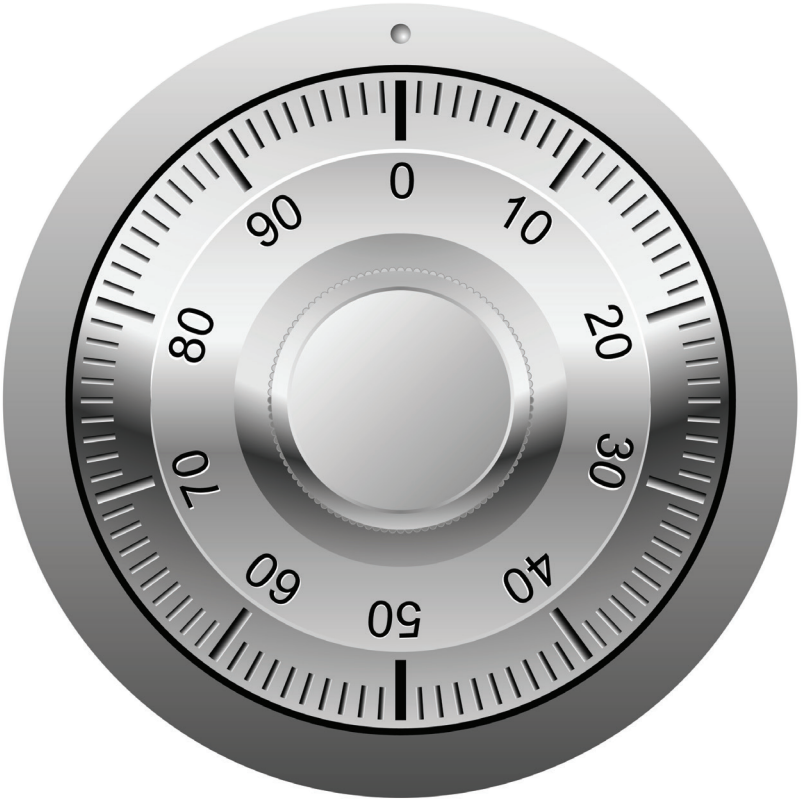
Deloitte.



Unlock the value in your technology investments

Use the right combination to elevate your extended enterprise risk management program

As business environments become more and more complex, organizations are focusing on core competencies and increasingly outsourcing non-core functions to third-party providers. These functions often involve customer interactions and other services where sensitive information is shared or service levels are business critical. Extending the enterprise by outsourcing these functions to providers for whom they are core makes good business sense. However, the associated risk levels, which vary widely, must be carefully identified and managed. At the highest level, third-party incidents can result in reputational damage, non-compliance, or even criminal activity, which can negatively impact earnings and shareholder value.

To address this challenge, many organizations are investing in technology to support extended enterprise risk management. As organizations embark on this journey, many want to understand the return on investment and the lessons to be learned from the mistakes others have made. Technology isn't the entire answer. But the right technology or collection of technologies, coupled with optimal processes, can enable organizations to create an inventory of third-party providers, assess those based on level of risk, incorporate controls, and provide ongoing oversight and management.

Where's the ROI from technology investments?

Many organizations that have invested heavily in risk management technologies still struggle to maximize the value of those investments. Risk executives have turned to technology solutions to help them manage third-party risk. But in many cases, they are underwhelmed by the results (see Figure 1). Even sophisticated organizations with extended enterprise risk management programs in place often end up with process-heavy, workflow-driven technologies when they align technology decisions to broken processes. As a result, risk managers still spend the majority of their time gathering data, leaving little time to actually manage risk.

Figure 1. Mind the execution gap

Source: Deloitte 2016 global survey representing eight major industry segments (over 170 organizations): financial services; energy & resources; manufacturing; public sector; technology, media & telecommunications; consumer business; health care & life sciences; business, infrastructure, and professional services.

So how do risk managers use technology to help to reduce the manual effort involved in collecting risk data? Integrating robust data feeds and innovative, cognitive technologies, such as robotic process automation and artificial intelligence, into an extended enterprise risk management program can greatly reduce time-consuming manual labor and analysis. Incorporating risk sensing using advanced analytics to gather information from private and public sources allows organizations to create a near-time, comprehensive view of the risks related to their third-party relationships or engagements at any given point in time. This enables risk managers to focus significantly more time analyzing data rather than gathering it, so they can aggressively manage those risks most critical to the organization. This near-time risk information aids third-party and category managers in making key decisions, such as identifying third parties that should set the standard for a given category, which can reduce the overall cost of doing business.

The sidebar, "Before and after," illustrates what many companies experience today versus what extended enterprise risk management tools and technologies can offer.

An extended enterprise risk management technology solution can help pull all this together and enable an organization to move from the "before" scenario toward the "after."

Start with the end in mind when selecting technology

Defining the capabilities needed to achieve the desired outcomes helps create a structure and process for evaluating technology options that fit the needs of the organization. Before selecting a technology or set of technologies, it's critical to first define the business requirement in terms of the problem that needs to be solved, the areas of risk within the lifecycle, and the types of third parties that need to be managed. Rather than mapping technology needs to current business processes and functional or technical requirements, organizations must identify the capabilities that need to be enabled through technology. And then work backward to identify the proper tools and technologies. Understanding how well (or how poorly) processes are working today can make the difference between using technology as a true enabler versus merely automating a broken process. This is also an opportunity to streamline existing processes.

Before and after

Current extended enterprise risk management program

1. Send questionnaire to vendor.
2. Follow up with phone calls, emails, or site visits to the third party to gather data necessary to assess controls around compliance, privacy, information security, etc.
3. Risk manager assesses the level of risk that exists based on information gathered from questionnaire and follow-up efforts.
4. To the extent technology platforms exist, they are modeled to replace manual steps. This helps with data gathering but does not address follow-up with vendors.
5. Risk manager spends 90 percent of time on data gathering and 10 percent on analyzing and addressing risks.

New world extended enterprise risk management

1. Technology platform mines private and public data sources—including third-party data hubs that are becoming increasingly prevalent—to gather information about the third party's reputation in the market, such as negative press, economic sanctions, complaints, compliance violations, and cyber security threats the third party is facing.
2. Technology platform interfaces directly with the third party to gather additional information not found in public and private data sources.
3. Analytics capabilities extract inherent risks and key risk considerations based on knowledge of the third party from mined and gathered data.
4. Cognitive and natural language processes are used to review evidence and produce an aggregated view of results for the extended enterprise as a whole.
5. Time can be reinvested into managing risks, allowing risk managers to make data-driven decisions based on a comprehensive risk assessment.

Start with the end in mind

- Reduce the amount of time spent manually collecting data
- Don't automate your broken processes
- Think about core capabilities you need and develop a combination of technologies to bring them together under one umbrella to address your risk management objectives

Integrated technologies enable third-party risk management

When building a third-party risk management program, executives should consider several dimensions of technologies:

- *Architecture enabling technologies,* which are broader in scope and may include existing operational/enterprise resource planning platforms for accounts payable, procurement, supply, contracting, or sourcing workflow.
- *Risk assessments and controls testing,* which use off-the-shelf niche applications or homegrown point solutions that address risk areas such as financial viability, sanctions, or cyber security. These solutions often incorporate online, subscription-based data sources that provide fact-based, objective insights into a third party's financial health, compliance violations, or sanctions.
- *End-to-end risk and control management,* which includes third-party management applications that inventory and track the corrective actions resulting from risk assessments and control breakdowns across the third-party environment. These applications enable continuous monitoring and risk intelligence gathering by integrating any number of innovative tools into the workflow that then feed into the risk management platform. The integrated view from that platform can provide early warning detection when the third party isn't meeting objectives.

Regardless of the scenario, a capabilities approach to technology investment decisions can achieve far better results than automating broken processes. With the right technologies in place, companies can implement and manage extended enterprise risk management programs that drive efficiency, reduce costs, improve service levels, and increase return on equity. In our experience, organizations with a sound extended enterprise risk management program realize an average 4 percent to 5 percent return on equity.

Take action, proceed with caution

As with any new investment in transformative solutions, executives need to be clear about goals, objectives, and the ideal end state. What many have called a failure of risk management technologies can most closely be attributed to ineffective technology implementation, adoption, and integration.

As organizations elevate their extended enterprise risk management program with technologies and analytic enabling solutions, they should prepare to:

- Start with the end in mind and clearly define the desired outcomes, business case, key performance indicators, and return on investment metrics.
- Get key stakeholder buy-in and address the change management required to achieve success.
- Assess the impacts on functional areas of your organization and gain organizational sponsorship.
- Define the business architecture by identifying the core capabilities required to achieve the desired outcomes and mapping those to enabling tools and technologies.
- Leverage the opportunity that extended enterprise risk management brings to reinvent, streamline, and simplify processes instead of automating broken ones.
- Determine a risk tolerance threshold. Risk is inherent and cannot be eliminated, but it can be managed to an acceptable level when enabled by tools and technologies that optimize the time spent on managing risk versus gathering data.
- Don't expect to address everything with one technology product. Acquire a suite of technologies that enable the business architecture and create a single view of third-party risk.
- Make sure the extended enterprise risk management program is tied to other risk programs within the organization, such as operations, to maintain consistency.

A sneak preview …

Deloitte recently concluded its annual 2017 Global Extended Enterprise Risk Management Survey with some interesting results:

- Organizational confidence in tools and technology used in extended enterprise risk management has not improved since 2016—90.6 percent of respondents reported a low to moderate level of confidence in their effectiveness.
- While many survey respondents desire a single extended enterprise risk management tool to address third-party risks, they recognize that no one tool currently exists. Instead, they use a "bricolage" of technologies:
  - ERP (44 percent of respondents)
  - Bespoke solutions (20 percent)
  - Off-the-shelf packages (23 percent)
- Survey participants feel that better extended enterprise risk management tools and technology can significantly reduce pre-contract, post-contract and ongoing tracking/monitoring activities with third parties.

Stay tuned: Full survey results will be published in spring 2017.

With heightening regulatory expectations, compliance-related sanctions, and increased scrutiny relative to third parties, extended enterprise risk management is top of mind as organizations strive to lessen their exposure to third-party incidents and protect their reputation in the market. Developing an integrated enterprise technology infrastructure, coupled with clear processes, can optimize risk management and enable organizations to leverage third-party relationships to create value across the enterprise.

How Deloitte Advisory can help

Deloitte Advisory brings together the full breadth of its capabilities to help you increase the performance of the extended enterprise and achieve your strategic business objectives.

Figure 2. Deloitte Advisory's Extended Enterprise Risk Management framework

Strategy and program development Solutions to assess, design, and implement strategically aligned extended enterprise program	• Compliance program benchmarking and gap analysis • Controls testing • Third-party compliance training • Regulatory compliance	• Governance and operating model design • Strategic risk assessment, tiering, and segmentation • Crisis management and simulation modeling
Evaluation and continuous monitoring Solutions to assess third parties and proactively sense and respond to extended enterprise risks and opportunities	• Anti-corruption health checks • Background checks and integrity due diligence • Internal corporate investigations • Third-party FCPA assessments and investigations • Litigation and dispute support • Third-party vetting and screening	• Risk sensing • Contract compliance assessments and optimization • Benchmarking • Analytics and visualization • In-depth market assessments • Supply chain forensics and A/P analysis • Sanctions screening and program assessments
Technology enablement Solutions to transform and continuously enhance extended enterprise risk management by designing, implementing, and deploying technology solutions	• Analytics platform and compliance dashboard • Vendor portfolio and transaction risk scoring • Data visualization • Advanced and predictive analytics	• Economic and statistical analytics • Risk and compliance • Intelligence • Governance/program management • Knowledge management

Contact us:

Jan Corstens
Partner | Deloitte Advisory
Global Extended Enterprise Risk Management Leader
Deloitte Belgium
jcorstens@deloitte.com
+32 2800 2439

Kristina (Krissy) Davis
Partner | Deloitte Advisory
US Extended Enterprise Risk Management Leader
Deloitte & Touche LLP
kbdavis@deloitte.com
+1 617 437 2648

Kristian Park
Partner | Deloitte Audit
EMEA Extended Enterprise Risk Management Leader
Deloitte UK
krpark@deloitte.co.uk
+44 7920 591507

Adam Thomas
Principal | Deloitte Advisory
Deloitte & Touche LLP
adathomas@deloitte.com
+ 1 773 677 1074