Deloitte.

June 2016

Power & Utilities Spotlight

Risk at the Core of Strategic Value Creation

In This Issue:

The Bottom Line

- Risk management should be divided into two categories: value protection and value creation.
- The role of enterprise risk management (ERM) functions in developing risk response plans varies depending on organizations' needs and aspirations, board expectations, and leadership capabilities.
- Understanding the risks associated with engaging third parties is critical to risk management.
- A streamlined risk management approach that includes qualitative and quantitative risk analysis has the potential to improve returns on capital for major projects and sharpen executive decision making.
- Although data analytics has been a recent "hot topic," risk management professionals have yet to tap into its full potential.
- In October 2015, the Institute of Nuclear Power Operations (INPO) released "Principles for Excellence in Integrated Risk Management," which highlights a number of leading practices for identifying and managing current and emerging risks.

Beyond the Bottom Line

Overview

Deloitte has been hosting a risk management roundtable series for the power and utilities (P&U) sector for the past seven years. The primary goals of this series are to discuss leading practices, identify trends, promote innovative solutions, perform benchmarking/studies, and facilitate networking within the industry.

The most recent roundtable was held in March 2016 at Exelon Corporation in Chicago. Deloitte and over 45 risk professionals representing more than 30 companies discussed (1) the role of risk in creating and protecting value for an organization through alignment with various internal functions, (2) exploring the future of the risk organization, (3) using data to identify and manage risks, and (4) leveraging the nuclear safety culture to develop an organization's risk culture and bring about positive behavioral change. In addition, in an open session, participants were asked to share how their risk management functions are helping achieve their organizations' strategic objectives and to discuss the role of the risk function in managing cybersecurity risk. Business model risk is a concern at many organizations, particularly traditional utilities, as the market diversifies and becomes more competitive. Internal barriers, including the perception of the risk management function and governance structures, influence the ability of risk management to support broader strategic objectives.

Deloitte set the stage for the discussion by holding a brief pre-roundtable benchmarking poll on the key attributes of an organization's risk environment. The poll results were incorporated into the discussions.

Industry Perspective

An executive at the roundtable discussed how his company's risk function was established. The company sought to develop a "best in class" risk function by emphasizing a risk-based perspective throughout the organization. Working with the board of directors to set up guideposts, the company was able to create a tight link between strategy and risk and to push the risk management culture down into the organization.

The risk function was developed to enable predictive decision making and minimize unexpected and adverse outcomes within the organization. The team used a three-pronged approach to develop its risk management framework:

1. *Governance* — Use various resources to facilitate timely, insightful risk discussions (e.g., risk management benchmarking, risk governance and policy implementation, risk appetite statement and communication).
2. *Tactics* — Embed risk managers into each function to lead risk assessments; develop risk action plans; and incorporate key risk indicators (KRIs), metrics, and risk dashboards into the broader organization.
3. *Strategy* — Develop an integrated risk program to include analytics and scenario planning, and embed risk discussions into strategic decision making.

In addition, the risk function should (1) invest in education, communication, and change management and be a true partner in building a trusting relationship; (2) secure leadership support to align risk with strategic imperatives; (3) focus on hiring resources with the right expertise; (4) shift its role from a red team that only challenges assumptions to a team that also assists with identifying and evaluating business opportunities; and (5) ensure that risk conversations include tangible actions and outcomes, whenever possible.

Value Protection

Alignment of Risk With Compliance

The risk and compliance functions in the P&U sector are evolving to better complement each other since today's markets demand greater coordination to protect against financial and reputational damage. Regulators have turned to enhanced analytics tools that allow them to home in on specific risks. Programs will now need to better assess and measure risk associated with compliance failures in addition to monitoring strict compliance with the rules.

Although companies are striving to remain compliant, they are often faced with the challenges of restricted budgets and increasing rates of enforcement investigations. Organizations often lose sight of the true purpose of the compliance requirement of managing risk. By considering risk management and compliance oversight from a more holistic perspective, a company can use each to greater strategic advantage.

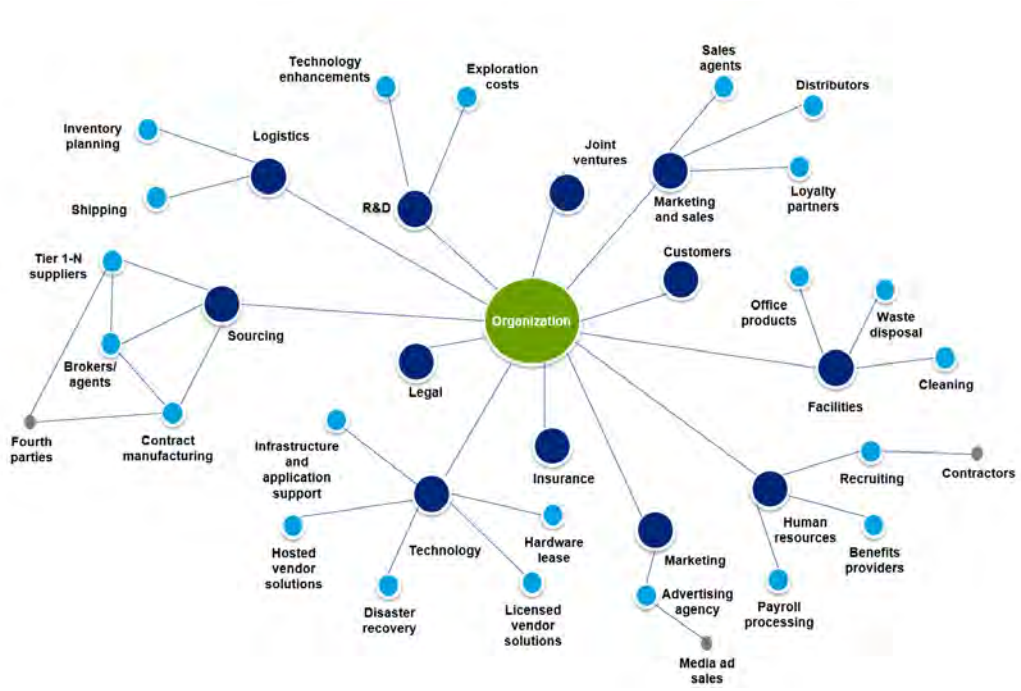
Key Takeaways

- Compliance efforts should not detract from risk management; the two should complement each other.
- Organizations can use risk management efforts to anticipate future regulations and compliance needs and preemptively address those risks.
- There are opportunities to further optimize risk management tools and processes to prioritize resources and evaluate/monitor compliance trends.

Alignment of Risk With Third Parties

P&U entities interact with hundreds or even thousands of third parties, such as vendors, contractors, and other service providers. This "extended enterprise" may also include a network of fourth and fifth parties that are contracted by third parties (see image below); there is often very little transparency into those parties' operations.

A Network Within a Network



The benefits of outsourcing workstreams can include cost savings and access to specialized resources; however, these benefits may be accompanied by vulnerabilities. For example, many high-profile third-party security breaches have recently occurred in the retail industry, resulting in significant data loss, the payment of hundreds of millions in reparations, and significant brand and reputational damage. Organizations have three lines of defense against third-party risks: (1) business units that own the third-party relationship and manage the risk by aligning it with policies and procedures; (2) the centralized, extended ERM program that establishes policies and procedures and creates tools and templates to enable standard practices; and (3) an internal audit program aligned with the most critical extended-enterprise risks and controls.

Industry Perspective

One participant shared her perspective on the involvement of third parties and noted that presenting possible "What could go wrong?" scenarios can pique a board's interest. If boards understand the potential pitfalls of third-party relationships, management may be able to decide where to draw the line in those relationships.

When involving a third party, a company needs to understand the true cost of a contract or relationship, especially when that relationship or contract does not involve payments (e.g., the exchange of information for research). Companies should perform an extensive risk-profile evaluation for certain third-party relationships.

Key Takeaways

- While organizations often focus on protecting themselves from losses, companies that proactively manage their third-party risks stand to reap substantial benefits, including increased productivity, contract and asset optimization, flexibility, expanded growth opportunities, and better cost management.
- The first steps in evaluating existing third-party risks are to (1) take inventory of the extended enterprise, (2) perform a risk assessment to determine areas of focus, and (3) develop a strategy and program to manage and monitor third-party relationships.
- Before establishing a relationship with a third party, a company should perform an extensive risk-profile evaluation to identify potential risks (e.g., to brand/reputation).
- As crucial as it is to monitor the onboarding stages of the extended enterprise, it is equally important to evaluate and address the risks associated with data retention and destruction, connection to information systems, and other control concerns during, and after the end of, the third-party relationship.

Alignment of Risk With Insurance

One-fifth of the participants described the alignment between their risk management and insurance functions as "very limited." This alignment is important because understanding their current risk exposure can help companies determine the type and amount of insurance coverage they need to manage that exposure. Coverage may not be required in areas in which controls are well established and routinely tested, and insurance may be reduced or changed when incidents are declining, processes have changed, activities have been reduced, and replacement costs have decreased. As an organization's business model or strategy changes, the company may need to reassess its insurance needs.

Insurance selection strategy should include the following:

- Evaluation of risks to understand their causes and consequences as well as the strategies for responding to those risks.
- Assessment of existing controls to evaluate risk exposure.
- Analysis of coverage requirements on the basis of assessment results.
- Comparison and evaluation of policies and coverage offered in the market.

While insurance policies may assist with risk transfer, organizations should conduct a cost-benefit analysis to determine the appropriateness of their investment in coverage. A sound understanding of controls and procedures will allow a business to obtain the appropriate level of insurance coverage for the risks or parts of the risk that cannot be addressed in house.

As P&U entities continue to learn more about the importance of cyber risk and its impact, their ERM functions will have greater opportunity to assist with framing cybersecurity risk and tracking insurance information to identify trends. Given that only 34 percent of the participants currently engage in this activity, there is significant potential for the risk function to play a more proactive role and enable risk-informed decisions.

Industry Perspective

More than half of participants said that both the risk management and insurance functions reported to the chief risk officer. Increasing the coordination between these functions can improve risk management and aid in the development of a better insurance strategy.

Key Takeaways

- Risk professionals need to work closely with the insurance function and the business's leaders to clearly articulate risks and implement the appropriate controls, tools, and solutions.
- Standardized insurance clauses in third-party contracts can help improve the consistency of risk and exposure framing as well as benchmarking related to different policies and coverage offered in the market. Specifically:
  - A company should evaluate its exposure to understand the type and amount of insurance coverage required.
  - Coverage may not be required in areas in which controls are well established and routinely tested.
  - Coverage may be reduced/changed when incidents are declining/processes have changed (e.g., owing to technological advances).
- A company should reassess its insurance needs as its business model and strategy change.
- A company should understand any policy exclusions.

Creating Value With ERM

Alignment of Risk With Capital Project Planning

In a Deloitte survey of over 10,000 financial executives, more than 60 percent reported that they were not confident that their return on capital was optimized in their company, with five out of six believing that human bias posed a threat to their organization's capital deployment decisions.[1] At the roundtable, half of the participants reported human bias (e.g., narrow framing, confirmation bias, expert bias, and optimism bias) in decision making to be the dominant challenge in the capital planning process.

Typically, organizations report varying degrees of risk involvement in capital planning decisions, and a lack of agreement regarding objectives and outcomes is considered the most common impediment to making such decisions. Risk professionals should consider the following five components in their capital planning life cycle to ensure that large-scale decisions are analyzed and that they incorporate risk-informed decision-making principles:

- *Plan* — Improve confidence in decision making through planning (e.g., define risk appetite and create links between desired financial and strategic objectives and operable key performance indicators, or KPIs). Translate big-picture strategies into concrete guidance, criteria, and metrics, and link risk appetite to the planning process.
- *Propose* — Include (1) risk-adjusted business cases for improved decision quality and (2) risk insights to facilitate comparisons and identify trade-offs.
- *Prioritize* — Analyze trade-offs to prioritize and optimize the whole portfolio; enable risk scenarios to make dynamic adjustments.
- *Implement* — Assign ownership of metrics to specific individuals to increase accountability and promote course corrections. Create dynamic risk dashboards of metrics to help monitor and course-correct throughout a project's life cycle.
- *Provide feedback* — Encourage iterative learning and continual improvement by capturing lessons learned and case studies from previous projects.

[1] These survey results are derived from six separate Deloitte *Dbriefs* webcasts from 2011 to 2015.

Industry Perspective

Participants indicated in the poll that the "plan," "propose," and "provide feedback" stages of their capital planning process could be improved. Only 3 percent indicated that their company does a fairly good job of establishing specific objectives and KPIs during the capital planning process.

One participant also discussed the project risk process, highlighting the value of data analytics during project approval and execution. The participant observed that if capital planning issues are presented without an accompanying numerical value (e.g., dollar amount or data point), they are not always properly addressed. Therefore, for quantitative decision making to become the norm, certain improvements will need to be made; only 21 percent of participants rated their company's risk analysis capabilities related to capital planning as "about average for the industry."

Key Takeaways

- Project risk management should be streamlined throughout the project's life cycle, with clear transitions from development to construction and then to operations.
- During the construction phase, the risk management program should be reinforced at the project level; there should be clear ownership and accountability for risk mitigation actions.
- Robust qualitative and quantitative risk analysis over the project's life cycle promotes effective decision making.
- The biases during the decision-making process should be recognized and properly challenged.
- A company should consider KPIs and KRIs to identify potential threats to projects.

Use of Data in Identifying and Managing Risk

Certain trends have accelerated in the P&U sector over the past 10 years, including the use of wind, solar, and shale gas. Each of these trends poses a different set of risks that could have been possibly identified and assessed sooner. For example, even though the rise of alternative energy was predicted multiple times in the past, such predictions failed to materialize.

In the past decade, however, notable technological advances and the introduction of government-backed incentives aimed at encouraging the use of alternative energy have turned those initial predictions into reality. A company's business model and strategic objectives are continually challenged in this ever-changing energy environment.

Assumptions that are critical to a company's strategy must be identified, evaluated, and monitored. Approximately 75 percent of roundtable participants monitor fundamental changes in their company's business model; however, only 25 percent have a corporate-wide strategy related to data analytics. Risk teams can better evaluate, communicate, and mitigate risks and uncertainties by expanding their capabilities to include data analytics, correlation, and visualization.

Thinking It Through

Companies that have a clear corporate-wide data analytics strategy and scan internal and external sources for trends in risks and uncertainties can get ahead of this challenge. Even though 75 percent of the risk professionals polled use scanning capabilities, there remains a clear need to better track existing and emerging risks.

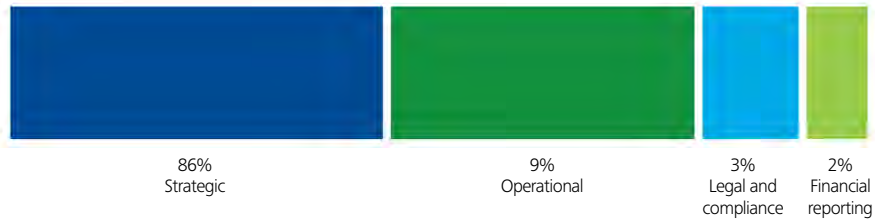
Key Takeaways

- Identify and monitor risks that could undermine strategic objectives, challenge management's assumptions, or exceed the organization's risk appetite.
- Perform external analysis to neutralize cognitive biases and uncover the true consequences of risks and trends.
- Oversee analytics activities to avoid siloed, narrowly focused, or overly tactical uses of data. Challenge the existing data, search for new inputs (both internal and external), and seek new correlations.
- Implement risk sensing for better evaluation, communication, and mitigation of risks.
- Combine human analysis with data analytics and technology to provide credible insights.

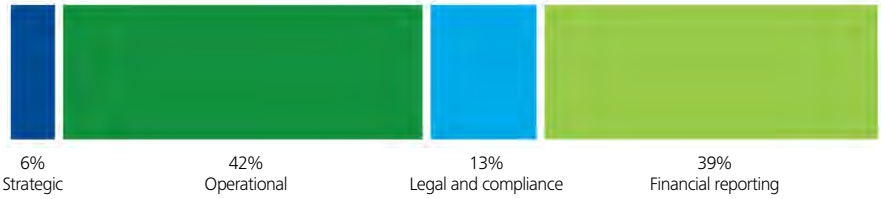
Risk Function of the Future

Strategic risk has proved to be the risk type that can cause the most significant value loss (see graphic below[2]). Therefore, risk functions are shifting from their traditional role as value custodians to that of enablers of thoughtful decision making throughout organizations that will help them bounce back from unexpected risks.

The Proportion of Significant Losses in Market Value Caused by Each Type of Risk Over the Past Decade



The Proportion of Time Spent on Each Type



Risk professionals must consider what they can do differently as the role of the risk function in their company evolves so that this function can provide the best possible value to the organization. For instance, the risk function could:

- Have more influence within the organization (have a "seat at the table").
- Perform real-time evaluation of emerging risks.
- Act as a risk facilitator.
- Integrate with other functions (e.g., internal audit and compliance).
- Align efforts with the strategy function.

One of the most effective ways to put these considerations into practice may be for the future risk function to think about acquiring different resources, competencies, and capabilities to expand the risk management focus beyond assurance to include resilience and strategy.

Industry Perspective

Participants discussed recent positive advances in organizational risk awareness. These advances came about because leadership played a role in breaking down siloes and regarded risk as part of the decision-making process and not simply as part of the assurance process. In addition, participants reported that the risk function cannot operate successfully without the support of the board or of C-suite executives because of the perception that risk professionals are not collaborators.

[2] Adapted from "Reducing Risk Management's Organizational Drag" (CEB, 2015). (Source: "How to Live With Risks" (*Harvard Business Review*, July–August 2015).)

Key Takeaways

- When empowered with quality information and insights, a risk leader can challenge strategic decisions and help create value for the enterprise.
- The future role of the risk organization may be seen as (1) helping translate insight into action, (2) providing informed and objective perspectives for strategic decision making, (3) elevating the vantage point from which risk is viewed within the organization, and (4) protecting value through risk mitigation.

Alignment of ERM With Nuclear Risk Approach

Many of the near disasters in the U.S. nuclear industry have resulted from the failure to understand full consequences of a risk. In response to those incidents, the INPO was established with funding from the U.S. nuclear industry to set industry-wide performance objectives, criteria, and guidelines for nuclear power plant operations and to promote operational excellence and improve the sharing of lessons learned.

As nuclear operators struggle to remain competitive by striking a balance among safety, reliability, and economic performance, the INPO principles of identifying risk, measuring and prioritizing risk, managing and mitigating residual risk, and adapting given the lessons learned provide a baseline from which to view nuclear risks through an enterprise lens. A company's assessment of risk from a consequences — rather than just a probability — perspective can facilitate apples-to-apples comparisons of competing operational priorities and enable risk-informed decision analysis.

One participant shared his organization's approach to continual risk management. His organization created a forum for robust discussion of key risks, mitigation actions, and trend analysis. The organization's risk assessment approach focuses on understanding potential consequences and generating risk maps to engage the right level of management in strategic discussions.

Participants also shared their thoughts on the benefits of a culture that promotes risk awareness, accountability, and personal commitment to safety and risk management. One approach that participants deemed effective is to hold employees to high standards of risk recognition and embed management and mitigation into field policies, programs, and processes. Periodic effectiveness reviews performed to promote continual learning and to improve risk management throughout the organization are also methods that are known to be effective catalysts for the right risk behaviors.

Industry Perspective

Even though the INPO's view on aligning ERM and nuclear risk management functions is still in its infancy and the nuclear industry is trying to identify improvements to implement efficiency initiatives, many participants believed that utilities could benefit from an INPO-like institution geared toward other fuel generation and distribution assets. Such an institution could help organizations report and share information on incidents and near misses and could encourage benchmarking, sharing of lessons learned, and collection of data and KRIs that can be used to develop dashboards for risk trending.

Participants also discussed how individuals can be incentivized to take action on risk. Companies may encourage more "bottom-up risk reporting" and "top-down feedback" by tying individual compensation and reputation to risk response actions as well as by having the overall performance of different functions affect leadership's compensation and reputation.

Key Takeaways

- The INPO's risk management guidance can enhance enterprise-wide risk practices by:
  - Helping drive risk-informed decisions on the basis of evaluating consequences rather than focusing heavily on likelihood or probability.
  - Leveraging a historically strong culture of safety to help guide risk culture efforts.
  - Guiding behaviors through empowerment and judgment rather than through rules.
  - Helping identify the critical behaviors and habits people need to commit to so that they can positively contribute to the risk culture vision and core values.
  - Aligning ERM and nuclear risk function efforts — such as risk identification, evaluation, escalation, and monitoring — to improve the efficacy and transparency of resource allocation.

Thinking Ahead

The Deloitte P&U sector team will continue to follow current and future risk-related activities. As an industry leader, Deloitte will continue to host these roundtable events so that P&U risk professionals can share prevailing practices with others in the industry. The next risk management roundtable is scheduled for October 2016. Keep an eye out for the pre-roundtable survey; the results will be a catalyst for future discussions.

For more information about this roundtable series, please contact nationalutilitiesermroundtable@deloitte.com or reach out directly to Dmitriy Borovik at dborovik@deloitte.com.

Contacts

If you have questions about this publication, please contact the following Deloitte industry professionals:

Andrew Blau
Director
Deloitte & Touche LLP
+1 415 932 5416
ablau@deloitte.com

Dmitriy Borovik
Director
Deloitte & Touche LLP
+1 212 436 4109
dborovik@deloitte.com

Brian Murrell
Partner
Deloitte & Touche LLP
+1 212 436 4805
bmurrell@deloitte.com

Asma Qureshi
Senior Manager
Deloitte & Touche LLP
+1 212 436 7659
aqureshi@deloitte.com

Subscriptions

Don't miss an issue! Register to receive Spotlight and other Deloitte publications by going to www.deloitte.com/us/subscriptions. Publications pertaining to your selected industry (or industries), along with any other Deloitte publications or webcast invitations you choose, will be sent to you by e-mail.

Dbriefs for Financial Executives

We invite you to participate in *Dbriefs*, Deloitte's webcast series that delivers practical strategies you need to stay on top of important issues. Gain access to valuable ideas and critical information from webcasts in the "Financial Executives" series on the following topics:

- Business strategy and tax.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance, risk, and compliance.
- Technology.
- Transactions and business events.

Dbriefs also provides a convenient and flexible way to earn CPE credit — right at your desk. Join *Dbriefs* to receive notifications about future webcasts at www.deloitte.com/us/dbriefs.

Technical Library and US GAAP Plus

Deloitte makes available, on a subscription basis, access to its online library of accounting and financial disclosure literature. Called Technical Library: The Deloitte Accounting Research Tool, the library includes material from the FASB, EITF, AICPA, PCAOB, IASB, and SEC, in addition to Deloitte's own accounting and SEC manuals and other interpretive accounting and SEC guidance.

Updated every business day, Technical Library has an intuitive design and navigation system that, together with its powerful search features, enable users to quickly locate information anytime, from any computer. Technical Library subscribers also receive *Technically Speaking*, the weekly publication that highlights recent additions to the library. For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.

In addition, be sure to visit US GAAP Plus, our free Web site that features accounting news, information, and publications with a U.S. GAAP focus. It contains articles on FASB activities and updates to the *FASB Accounting Standards Codification*™ as well as developments of other U.S. and international standard setters and regulators, such as the PCAOB, AICPA, SEC, IASB, and IFRS Interpretations Committee. Check it out today!

The Spotlight series is prepared by members of Deloitte's National Office. New issues in the series are released as developments warrant. This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited.