Deloitte.

Issue 4, June 2013

Power & Utilities Spotlight

Risk-Talking: Takeaways From Deloitte's May 2013 P&U ERM Roundtable

In This Issue:

The Bottom Line

- As part of its continuing efforts to understand the risks and challenges faced by enterprise risk management (ERM) professionals and their organizations, in May 2013 Deloitte hosted a power and utilities (P&U) ERM roundtable comprising more than 40 ERM professionals from over 20 companies. Participants shared their views on ways to improve, and best practices for, ERM program management at their organizations.
- ERM is a differentiator that may help with strategic decision making and proactive management of operations. When implemented properly, ERM is an effective improvement tool that adds value to an organization. At the roundtable, two of the more notable topics discussed were (1) the incorporation of ERM into an organization's budgeting process and strategic plan and (2) the use of quantitative modeling within an ERM program.
- Various Deloitte and other industry subject matter specialists moderated discussions about the current risks utilities are facing. The discussions centered on five major risk-related topics: cybersecurity, alignment of risk within large capital projects, the practical application of key risk indicators, aging infrastructure (AI), and emergency management.
- Two keynote speakers focused on ERM in the context of the overall business environment. First, an executive officer from a large utility offered his views on risk and ERM, stressing that the go-forward approach for ERM will be more of an enterprise risk and opportunity program than the legacy approach to ERM. Second, a director from a major credit rating agency discussed how credit ratings are determined and how ERM is considered during this process.

The go-forward approach for ERM will be more of an enterprise risk and opportunity program than the legacy approach to ERM.

Beyond the Bottom Line

This *Power & Utilities Spotlight* summarizes the discussion at Deloitte's ERM utilities roundtable. In addition, this publication gives a brief overview of each topic addressed during the three-day event and highlights how it may affect ERM professionals and their organizations.

Overview

ERM is a key function in any business organization, but especially for P&U companies. As part of its continuing efforts to understand the risks and challenges faced by ERM professionals and their organizations, Deloitte has hosted a quarterly P&U ERM roundtable series for the past several years. The primary goal of this series is to discuss leading practices and innovative solutions related to ERM management for P&U entities. Since the inaugural session four years ago, more than 100 ERM professionals from 60 utility companies throughout the United States and other parts of North America have attended the roundtables.

More than 40 ERM professionals from over 20 companies convened in Con Edison's New York corporate headquarters to attend the May 2013 P&U ERM roundtable hosted by Deloitte's Enterprise Risk and Compliance Management Services team. Participants shared their views on ways to improve, and best practices for, ERM management at their organizations. Some common discussion points included understanding the impact of incorporating ERM into a company's strategic planning and operational budget process, methods of enhancing cultural awareness throughout an organization, and views on quantitative modeling of risks.

A more functionally integrated ERM structure throughout a company increases ERM value.

The roundtable also included subject matter specialists from Deloitte and the utilities industry who provided their perspectives on certain major risk themes, including cybersecurity, large capital projects, aging infrastructure, and emergency management. In addition, (1) a utility senior executive officer offered his perspective on managing risk within his organization and gave his views on the go-forward approach for ERM and (2) a speaker representing a major credit rating agency provided insight into how credit ratings are determined and how ERM is considered during this process.

Snapshot of Topics Discussed

Collaborative Discussion of ERM

Moderated by Deloitte's Dmitriy Borovik and Con Edison's Rich Muzikar, the first roundtable discussion addressed the overall goal of ERM and how, when implemented properly, ERM is an effective quality-improvement tool.

ERM's Incorporation in Strategic Plan and Organizational Budget

Successful practices for incorporating ERM into the overall organizational and strategic process were addressed throughout the roundtable discussion. Many participants indicated that their integrated ERM structure increases ERM value at their organizations. Others indicated that their management and operations team still views ERM as an "add-on" and that they therefore consider ERM after the formal budget process.

Modeling of Risks

Professionals at the roundtable wanted to understand how quantitative modeling (e.g., Monte Carlo simulations) could further be incorporated into ERM. Most ERM leaders in attendance indicated their fundamental belief that quantitative risk assessments are valuable to the ERM process.

Major Risk Themes

Cybersecurity

The roundtable consensus was that cybersecurity-related risk[1] is among the greatest risks affecting public utilities. Participants suggested that many companies consolidate cybersecurity risk mitigation efforts by aligning them with ERM activities. With respect to ERM's role in cybersecurity, participants noted that it is important to (1) understand how ERM programs can help in the assessment of organizations' cybersecurity risk mitigation activities, (2) improve understanding of cybersecurity risk throughout an organization's business units, and (3) reinforce the importance of knowing the cybersecurity risks within the organization and potential impact of these risks on the utility's operations. Furthermore, studying cybersecurity from a cross-industry perspective (e.g., banking, health care, defense, telecommunications) may help an organization understand cybersecurity leading practices, lessons learned, risk impacts, and measures to apply in the utilities industry.

Presenters at the cybersecurity session highlighted the importance of understanding emerging cybersecurity issues such as the use of social media, international cyber threats, and information ownership. In addition, they pointed out that aging legacy systems and certain applications may lack the proper security features to mitigate cyber attacks.

Presenters also offered their views on various factors that increase cybersecurity risk, such as the integration of new systems and technologies as a result of a business acquisition. In addition, the use of third-party contractors could potentially expose an organization to new cyber threats because the third and fourth parties associated with these business partners may (1) inappropriately use the available information, (2) not properly adhere to the organization's policies, and (3) inadvertently open access to the organization's systems. Furthermore, if an organization does not have defined policies and practices governing data protection, employees potentially could use removable hardware (e.g., thumb drives) at their workstations, which could make the organization's systems vulnerable to viruses and malware.

The roundtable consensus was that cybersecurity-related risk is among the greatest risks.

Entities need to consider both internal and external cybersecurity risks when developing an effective mitigation plan. Such a plan might include (1) performing sufficiently detailed background checks, (2) performing a cybersecurity risk assessment at all locations where sensitive information is maintained, (3) limiting the information maintained in certain applications to that needed for the role, and (4) considering alternative mitigation risk strategies such as the acquisition of cybersecurity insurance.

Alignment of Risk Within Large Capital Projects

Presenters provided an in-depth look at how risk should be considered and aligned within an organization's large capital project plan. A report from the International Energy Agency highlighted that to meet the demands of population growth, an estimated $38 trillion will be invested in existing and new utility capacity by 2035 ($17 trillion of which will be spent on power generation, distribution, and transmission). Certain risks are inherently associated with large capital projects; understanding these risks is important to a project's overall success.

Projects continue to increase in scope and size, presenting certain challenges and risks. The Construction Industry Institute (CII) has identified its top 107 project risks. The roundtable presenters highlighted some of the more frequent risks from this list that they have encountered, including increases in project sizes/costs, tighter development schedules, introduction of new technologies, scarce resources, regulatory constraints, and heavy reliance on third parties.

[1] Cybersecurity can be defined as a company's internal and external IT systems, processes, and practices that are designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Financial and operational effects of project risks may include cost overruns, schedule delays, unplanned scope changes, contract modifications or related claims, abandoned projects, underused assets, quality issues, lack of stakeholder support or acceptance, and bad publicity. Understanding the root causes of project management breakdowns is the first step to avoiding problems, including inadequate risk planning and monitoring, lack of clear governance structure and accountability, poorly developed project teams, insufficient resources, limited controls, inadequate project planning and reporting, and poor communications.

ERM teams can be the catalyst to managing the risk associated with large capital projects. A key step in improving the success of any capital project is the development and implementation of a comprehensive project plan that contains a structured project risk management framework. A successful framework allows for cross-team integration, including risk governance, people, tools and systems, and project risk management processes and procedures, each of which plays a critical role in the overall project plan.

Practical Application of Key Risk Indicators

Presenters from Deloitte and Con Edison teamed up to discuss the practical application of key risk indicators (KRIs) and their value to the management of risks throughout an organization. KRIs allow management to pinpoint potential areas of focus or concern within an organization and can be used as an early-warning system to identify trends and changes within the organization's risk profile. Further, KRIs are a way of effectively monitoring emerging risks and may help management identify the interdependence between various risks. In short, KRIs can be characterized as a risk trend dashboard.

Key risk indicators allow management to pinpoint potential areas of focus or concern within an organization and can be used as an early-warning system to identify trends and changes within the organization's risk profile.

The presenters pointed out that there was a process for identifying KRIs and highlighted certain key elements to look for, including causal factors,[2] risk events, and consequences. When developing a process and the related criteria for evaluating KRIs, an organization needs business support, a thoughtful approach, sustainable processes, and reliable data. The approach should be customized to the company's specific needs and expectations.

An organization needs to establish a set of thresholds for each KRI since this is a key component for deriving value from KRIs. These thresholds should be linked to specific values and applied by using a consistent approach that allows interested stakeholders to understand the risk and potential changes to risk at any given time. Thresholds are used in the development of an effective monitoring and risk reporting tool.

It is important for organizations to establish a common risk framework that appropriately reflects management's risk appetite. When establishing the framework and developing the overall KRI management plan, it is important for an organization to team with internal business unit owners. Further, it is important to understand that the management of KRIs using a structured framework linked to an individual's performance evaluation or compensation package may become "personal" — that is, viewed negatively by those affected. This may result in organizational resistance in implementing such a program, which can be managed by the effective use of change management techniques.

Aging Infrastructure

Discussion of AI initially focused on how organizations define the related risk. Many participants believe that AI is a risk within their organization, whereas others see it more as a causal factor contributing to specific operational risks. The AI discussion then turned to how the scope of AI is defined. Participants had various suggestions for what the scope of AI could include, ranging from wires and pipes, to IT infrastructure, to people with the knowledge and experience to maintain AI. Several organizations discussed the challenge of balancing reliability in an AI environment with the needs of ratepayers to maintain low cost of service.

[2] Causal factors are all of the trigger events, intermediate events, and conditions that could lead up to a specific risk event.

The consensus was that AI will need to be addressed in the near term. Participants shared their views on how to prioritize the various AI projects as well as the leading practices employed by their organizations to manage AI. They emphasized the types of tools and metrics used to monitor the effects of AI.

Emergency Management

A utility's emergency management team is vital to the ERM team's success. During the roundtable, Deloitte and Con Edison shared the results of their annual Emergency Management Benchmarking Study. The results of the benchmarking study were used to discuss leading practices related to aligning emergency management with ERM efforts. Leading emergency management programs include (1) aligning emergency management risks with ERM risks, (2) prioritizing and developing responses to potentially catastrophic events, and (3) assigning resources and formulating response-and-recovery plans.

The presenters offered their perspective on what constitutes a successful emergency management program, highlighting a benefit of the "centralized robust response system" that offers four levels of response, depending on the nature of the event. This response addresses all aspects of the organization, including media, customer care, operations, and executive management. In addition, the business units throughout an organization are subject to periodic preparedness drills. Further, the utility offers a comprehensive program to train individuals in roles outside of their normal daily responsibilities, allowing them to assume other roles within the organization on an as-needed basis. This strategy provides an added layer of redundancy within the organization that can be implemented when an emergency event occurs.

The presenters offered their perspective on what constitutes a successful emergency management program, highlighting a benefit of the "centralized robust response system" that offers four levels of response, depending on the nature of the event.

Utilities generally plan for catastrophic events that are specific to their geographic area or service territory. The level of planning varies directly with the company's size and the sophistication of its emergency management program. Such plans take into account the frequency of the event and its potential impact on the utility's system and operations. Utilities may choose either to implement the same response to most events (also known as the "all-hazards approach") or to develop specific responses to certain events or to multiple events that occur simultaneously. In some instances, utilities may apply a combination of these two approaches.

General Business Topics

Executive Officer View on Risk and ERM

One of the keynote speakers highlighted that utility business leaders are intimately aware of the risks affecting their organizations. He explained that utilities need to understand and consider the risks specific to their geographic area and business when formulating a risk management program.

Managing a utility and its related risks is often challenging because of the unique nature of its business model (i.e., that of a regulated company). Because of this regulation, utilities as an investment are often limited as a result of restrictions on allowed profits and other rules resulting from robust regulatory oversight. For example, regulators will limit what can be charged to ratepayers, thereby eliminating above-normal profit and returns on investment while imposing other restrictions on the utility, including (1) managing the utility's cost of infrastructure, (2) participating in other types of businesses outside the utility's core operations, and (3) managing the capitalization rules for the utility. The bottom line is that the strict regulatory environment results in the investment in a utility being, at best, similar to that of a bond.

While the upside for investment growth may be capped, there are no limitations on the downside since utilities are subject to various risks both within and outside their control, each of which could adversely affect their operations. The presenter contended that he works to manage this downside, since mitigating and managing these risks has the most impact on his organization.

While linking the concepts of "understanding various risks" with "managing in a regulatory environment," the keynote speaker discussed the role of ERM in his organization. At the board of director (BoD) level, he believes that a robust ERM system allows the board to see how risks are mitigated in relation to the potential "downside" to investors. It is important for the BoD to understand the risks to the company's operations as well as how aggregating such risks will affect the company. In addition, an effective ERM system can allow a company to communicate up to the BoD and down to the employees.

In concluding, this presenter did highlight one shortfall with the current state of the ERM system that he and his team are working to address. That is, the current ERM system often focuses on the "downside" (i.e., potential risks that the company faces) and does not take into account potential opportunities for improving the company's success. He believes that these two concepts can be integrated to some extent, whereas a joint enterprise risk and opportunity management (EROM) approach can be developed to highlight the potential risks an organization faces while identifying potential opportunities. Better alignment with long-term planning and other strategic functions would represent the next generation of ERM (or EROM) within a company.

While the upside for investment growth may be capped, there are no limitations on the downside since utilities are subject to various risks both within and outside their control, each of which could adversely affect their operations.

Understanding Credit Ratings

A representative from a predominant credit rating agency gave an overview on how a credit rating is calculated, highlighting that such ratings should be viewed as "relative rankings among issuers and obligations of overall creditworthiness" and not as a way of measuring the absolute potential for default. He noted that an entity considers various qualitative and quantitative factors when determining a credit rating and that these factors are grouped in two broad categories: (1) business risk factors (mostly qualitative) and (2) financial risk factors (mostly quantitative). Business risk factors are often weighted more heavily in the determination of a rating, although both business risk and financial risk factors are considered to some extent. Because of the nature of a utility, most will be considered investment-grade (BBB or higher).

Over the past couple of years, utilities have been focusing heavily on the growth of the core business as part of their strategic plan. While credit ratings analysts from other industry groups might focus on cash flows for servicing debt and cash levels held, this approach does not apply to utilities. Rather, utilities place more emphasis on understanding certain aspects of management and governance credit factors when determining a rating.

From the standpoint of management metrics, the ratings agency will consider the strategic planning process; consistency of strategy with the organizational capabilities and marketplace conditions; ability to track, adjust, and control execution of strategy; comprehensiveness of enterprise-wide risk management standards and tolerance; standards for operational performance; management's operational effectiveness; management's expertise and experience; and management's depth and breadth. Regarding governance credit rating metrics, ratings agencies will consider board effectiveness; entrepreneurial or controlling ownership; management culture; regulatory, tax, or legal infractions; communication of messages; internal controls; and financial reporting and transparency.

In response to an ERM professional's question, the presenter acknowledged that there is no formal framework for incorporating ERM into the determination of a company's credit rating, although understanding the ERM system and process is considered in the analysis of the business risk factors. Further, it was emphasized that while ERM system information is not directly considered, there is an intersection between governance risk compliance and ERM that would be considered in those instances in which something went wrong within a company (i.e., how will the ERM system and process address the issues).

Thinking Ahead

The Deloitte Power and Utilities industry team will continue to monitor current and future activity associated with (1) ERM-related matters, (2) regulatory rulemaking and compliance requirements, (3) accounting standard setting, and (4) any other significant matters that may affect this industry sector. These periodic communications will be in the form of (1) multiday industry seminars, (2) *DBriefs* webcasts, (3) industry spotlights, and (4) future roundtable discussions.

Topics that are being considered for future roundtable discussions include:

- Alignment of ERM with long-term planning and budgeting activities.
- Risk culture within a business organization.
- Disrupting forces, emerging risks, and potential opportunities.
- Risk appetite.
- Risk quantification.
- Risk-based project prioritization.
- ERM BoD level reporting.
- Risk life cycle process (regulatory risk).
- ERM value through alignment with other functions and departments (e.g., Information Technology, Treasury, Internal Audit, Procurement, Vendor Management, Compliance).

For more information about this roundtable series, please contact us at 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:

Bill Graf
U.S. AERS Sector Leader, Power & Utilities
Industry Professional Practice Director, Power & Utilities
Deloitte & Touche LLP
+1 312-486-2673
wgraf@deloitte.com

Dmitriy Borovik
Enterprise Risk and Compliance Management Services
Deloitte & Touche LLP
+1 212 436 4109
dborovik@deloitte.com

Kim Detiveaux
Enterprise Risk and Compliance Management Services
Deloitte & Touche LLP
+1 713 775 6471
kdetiveaux@deloitte.com

Subscriptions

Don't miss an issue! Register to receive Spotlight and other Deloitte publications by going to www.deloitte.com/us/subscriptions, choosing the Industry Interests category, and checking the boxes next to your particular interests. 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 & tax.
- Corporate governance.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Risk intelligence.
- Sustainability.
- Technology.
- Transactions & 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.

Registration is available for this upcoming *Dbriefs* webcast. Use the link below to register:

- Quarterly Accounting Roundup: An Update of Important Developments (June 27, 2 p.m. (EDT)).

Technical Library: The Deloitte Accounting Research Tool

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, the EITF, the AICPA, the PCAOB, the IASB, and the 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.

In addition, Technical Library subscribers have access to Deloitte Accounting Journal entries, which briefly summarize the newest developments in accounting standard setting.

For more information, including subscription details and an online demonstration, visit www.deloitte.com/us/techlibrary.