Deloitte.

May 2015

Power & Utilities Spotlight

Transitioning ERM Capabilities to a New Level

In This Issue:

The Bottom Line

- Although the implementation of risk appetite frameworks in the power and utilities (P&U) sector is largely in its infancy, P&U companies appear to be expending significant effort to formalize their risk appetite approach and practices.
- An organization should develop a long-term strategy to optimize the value of its enterprise risk management (ERM) program.
- Key performance indicators (KPIs) are valuable tools for assessing whether an organization's ERM program is effective.
- Cyber risk continues to be a major concern in the P&U sector. ERM's role in cyber-risk-related efforts continues to evolve in response to the changing P&U environment.

Thinking It Through

Given the current pace of change in the sector, P&U companies will need to reassess and possibly modify their business models to operate successfully. Such adaptation is linked to understanding the potential catalysts for and barriers to change. Robust risk management strategies and a risk appetite framework can help an organization prioritize resources and support its overall strategic objectives.

Beyond the Bottom Line

Overview

Deloitte has been hosting a P&U ERM roundtable series for the past five 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 at NextEra Energy Inc. in Juno Beach, Florida. Deloitte and over 40 ERM professionals representing more than 25 companies discussed cyber risk, crisis management, ERM strategy approaches, risk appetite methods, operational risk reduction, and KPIs for ERM programs. Participants were asked to consider what their ERM programs were best known for and how they might continue to strengthen their ERM efforts and provide value to stakeholders in the coming year. These two questions were the catalyst for a discussion of common and leading practices in the industry for identifying, monitoring, and reporting on risks and trends.

As it has done in the past, Deloitte set the stage for discussion by holding a brief pre-roundtable poll on the key attributes of an organization's ERM environment. The pre-poll results and live poll questions were incorporated into the discussions.

Industry Perspective

Senior executives at the hosting company offered their insights into risk management at their organization and in the P&U sector as a whole.

Jim Robo, chairman and CEO of NextEra Energy Inc., emphasized the fundamental need to set a "tone at the top" and indicated that the value of ERM is that the risk is managed by business units. In addition, he pointed out that a healthy risk management culture should encourage pushback when necessary.

Mike O'Sullivan, senior vice president of development at NextEra Energy Resources LLC, also homed in on the importance of tone at the top. At his organization, the CEO also functions as the chief risk officer. Further down the chain of command, senior management executives bear an additional responsibility as risk officers.

Role of ERM

If properly implemented, an ERM program can play an important role in educating management about an organization's risks. Understanding the nature and types of risk (e.g., operational versus strategic), as well as the best ways to mitigate or manage risk, is important at all levels of the organization — from business unit management to the C-suite and board of directors.

Risk Appetite

Risk appetite can be defined as the amount of risk an entity is willing to take given its capacity to bear risk and its philosophy on risk taking; risk appetite differs from risk capacity, risk tolerance, and risk thresholds (limits). The concept of risk appetite may help companies further enhance and defend their decision-making processes, prioritize top risks, and develop appropriate risk response plans and overall strategies.

Risk appetite frameworks can assist companies with capital and resource allocation and can provide a basis for more strategic decision making regarding risk. Such frameworks can also foster a more risk-intelligent culture by promoting accountability and transparency. However, most companies have not developed a formal risk appetite statement or documented framework as part of their ERM programs.[1] Implementing a formal framework can be challenging as a result of such factors as inconsistent understanding or application of terms (e.g., internal obstacles such as differing interpretations or legal concerns); determining tolerance to certain types of risks, such as operational health and safety; and difficulties with making risk appetite an integral part of a company's culture.

[1] This statement is based on the results of a polling question asked during the recent Deloitte ERM roundtable.

ERM professionals indicated in a poll that for a risk appetite framework to be successful, it should be structured enough to have a significant impact on management's decisions; however, it does not need to be overly quantitative or formally adopted by the board of directors. In developing a formal risk appetite framework, an organization may conduct internal and external research to review strategies, financial statements, existing delegations of authority, and risk tolerance statements that may already be part of internal policies. An organization can then develop a risk appetite statement, tolerance thresholds, and risk assessment criteria. The risk appetite statement should be aligned with the overall business strategy and should be reviewed against the company's estimated exposure to define effective risk mitigation strategies.

Although the practical implementation of risk appetite frameworks in the P&U sector is largely in its infancy, the benefits of such a framework are often viewed as outweighing the challenges. A consistent definition of risk appetite can help an organization take a more strategic approach to risk taking, risk mitigation, and overall decision making.

Industry Perspective

Organizations have various approaches to using and optimizing risk appetite practices. One ERM professional indicated that her organization uses a framework to provide a holistic view of risk appetite while a set number of appetite categories are linked directly to the organization's strategic objectives. The framework is instituted by the board, establishes guidelines for current and future risk management activity, and sets target risk appetite levels for each appetite category. Appetite levels are established on the basis of qualitative statements rather than numbers or other quantitative metrics.

Certain professionals shared their formal risk appetite statement as well as the qualitative and quantitative measures that are used to define their risk appetite. One particular company has a risk appetite statement and a set of 15 measures designed to be a "one-stop shop" for sharing the company's risk appetite with stakeholders such as regulators, customers, or investors. The company also considers risk appetite when evaluating business and strategic alternatives, aligning objectives with business strategies, and managing the related risks. Further, the company's risk appetite framework is updated and reviewed by the executive team annually and is one of many tools used in the decision-making process.

Key Takeaways

- A risk appetite framework serves as a basis for risk-based decisions and can help companies enhance capital and resource allocation efforts. Risk appetite can also be leveraged to "defend" a company's strategy or strategic initiatives.
- Companies should compare their risk appetites with their estimated risk exposure when developing risk mitigation strategies.
- Although the practical implementation of risk appetite frameworks in the P&U sector is largely in its infancy, risk appetite is generally believed to play an important role in a company's business strategy and strategic initiatives.

Perspectives on ERM Strategy

Each organization has its own approach to incorporating risk management elements into its overall corporate strategy. One such approach is to develop an official mission statement or vision statement for an ERM program (40 percent of the organizations surveyed indicated that they have such a statement). This statement is used to articulate the program's value and manage expectations.

Similarly, many organizations have a formal ERM strategy, which is one of the foundations of a successful ERM program. Without a formal strategy, ERM functions may become responsive rather than strategic. Further, it is hard to recruit and attract the right talent, invest in tools, and acquire capabilities without having a long-term vision. ERM strategies seem to be fairly common in the P&U sector. More than 60 percent of the ERM professionals surveyed indicated that their organization has a specific ERM strategy. Further, 40 percent of the surveyed participants indicated that they had three- to five-year strategic plans.

The ERM strategy often takes into account such elements as the ERM program's value/objective, key initiatives, stakeholder communication plans, and the capabilities and competencies needed to support the organization's mission. A number of ERM programs are closely tied to other functions such as strategy, long-term resource planning, capital projects, emergency management, and insurance. In addition, some of the ERM strategies include near-term, mid-term, and long-term initiatives. Near-term initiatives address tactical and operational matters, mid-term initiatives focus on foresight and contingency activities, and long-term initiatives comprise strategic and resilience efforts.

Industry Perspective

Participants offered their perspectives on ERM strategy at their organizations. One professional indicated that his organization's ERM program focused on such activities as promoting risk-informed decision making, establishing infrastructure, developing and growing partnerships, and increasing risk awareness. In this way, the organization was able to systematically measure, prioritize, and respond to risks and opportunities affecting the achievement of its strategic objectives.

A second professional shared his organization's development of a robust ERM strategy on the basis of a clear vision and objectives that align with the organization's strategic goals. The focuses of his organization's ERM program included integrating the business, enhancing the risk culture, increasing risk-based decision making, resilience, and continually improving the risk management framework. This professional also emphasized what he characterizes as the three "A's" of a successful ERM program:

- Alignment with the company's strategic and business planning direction.
- Agility to meet challenging business needs and respond to a shifting environment.
- Ability to provide credible insight and facilitate meaningful dialogue.

Key Takeaways

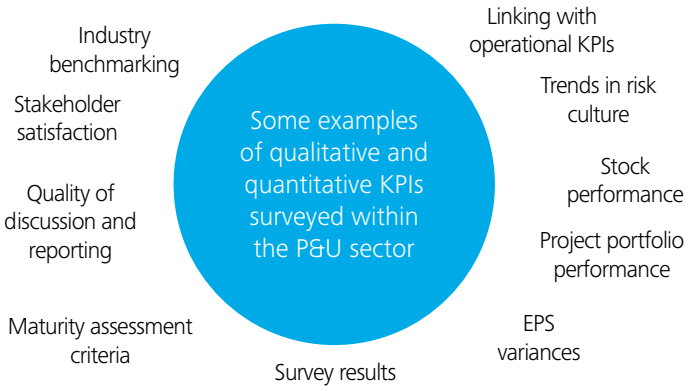
- It is critical to solicit customers' and stakeholders' views, obtain executive support, and establish business partnerships before developing or redefining an ERM strategy.
- Organizations should consider developing specific vision and mission statements for an ERM program and incorporating these into a formal strategy that can be used to articulate the program's value and manage expectations.
- A formal risk strategy is important to a company's success. A formal ERM strategy should incorporate both immediate tactical elements and strategic long-term initiatives.
- Without a formal strategy, ERM functions may become responsive rather than strategic. Further, it is hard to recruit and attract the right talent, invest in tools, and acquire capabilities without having a long-term vision.

Key Performance Indicators and Success Evaluation

KPIs have become increasingly important as a way of evaluating the effectiveness of an organization's ERM program. While KPIs are one of management's fundamental tools for measuring an organization's efficiencies in the P&U sector, KPIs are not widely used in ERM functions. Survey results indicated that only about one-third of the ERM professionals use formal KPIs to measure ERM program performance, though most are aware of informal or qualitative KPIs that are indicative of their ERM program's success.

Both quantitative and qualitative KPIs are helpful to an organization's assessment of its ERM program's performance. Some of the more notable quantitative KPIs used for this purpose include stock performance, project portfolio performance, variances in earnings per share, and customer survey results. Qualitative KPIs that may apply to ERM programs include feedback received or discussions held at various levels within the organization (e.g., C-suite, board of directors, audit committees).

Most P&U companies focus on establishing both quantitative and qualitative KPIs as part of their ERM programs to drive growth and innovation and improve analysis of operational risk. The following chart illustrates KPIs that are commonly used in the P&U sector:



More than two-thirds of the organizations surveyed indicated that their KPIs are results-driven; other organizations may use action-driven KPIs. A properly designed KPI should take into account both action-driven and result-driven performance.

Thinking It Through

As ERM gains a greater foothold throughout an organization, KPIs can serve as a scorecard of an ERM program's success by allowing key stakeholders to more systematically measure returns on their investments. However, while organizations have made great strides in using KPIs to manage the success of their ERM program, there is still room for improvement.

Key Takeaways

- Executives appear to be focusing more on systematic ways to measure the value and performance of ERM functions; as a result, the use of KPIs to evaluate the success of ERM programs may become more common in the future.
- KPIs can be a valuable tool for evaluating the ongoing value and success of an organization's ERM program.
- A properly designed and effective KPI should take into account both action-driven and results-driven performance.

Mitigating Risk in Capital Planning

Many utilities are facing challenges as their infrastructure ages. Regulators generally support utilities' efforts to overhaul their systems given the increased risks posed by aging infrastructure. However, utilities must also be cognizant of the financial impact on their stakeholders (e.g., customers, residents, shareholders), since there is often negative press about the impact of high-cost infrastructure replacement plans. Consequently, state regulators are under pressure to defend the cost increases and are demanding transparency regarding how infrastructure improvement decisions are made and about the degree of risk reduction achieved for each dollar spent. To challenge such rate recovery plans, regulators are using more sophisticated tools, including experts.

To secure the approval of their rate recovery plans, utilities will need to develop a sound cost structure plan that is reviewed and updated periodically. In creating this plan, a utility must weigh competing concerns such as safety, reliability, legal requirements, financial performance, environmental needs, and its overall image.

Organizations have adopted general approaches to addressing the challenges of capital planning:

- *"Technical view"* — Projects are analyzed according to their technical merits and on a project-by-project basis rather than at a portfolio level.
- *"Economic view"* — The most common of the three approaches; cost benefit or project cash flow measures are used to analyze a project.

- *"Strategic view"* — Few organizations hold this view, which holistically examines the project's impact on business strategy. This view allows organizations to balance the achievement of strategic goals with the management of risk exposure.

Capital planning must include strategies that address risk management, solution planning (i.e., obtaining the value and risk information for each potential spend option), and portfolio optimization (i.e., prioritizing spending on the basis of business objectives). Structured asset investment planning processes will enable a business to:

- Develop a clear link between the strategic direction of the business and the selection and funding of projects and investments.
- Use quantification and option analysis to establish a common framework for effective investment decision making.
- Employ rigorous, credible, and powerful tools to communicate with executive teams and external stakeholders.

Key Takeaways

- Capital planning must include strategies that address project risk management, risk valuation, solution planning, portfolio optimization, and spend prioritization.
- Asset management must have a "common framework" under which option analysis is used to support decision making.

Cyber Risk

Cyber risk continues to be a major concern in the P&U sector. Because technology is increasingly evolving, organizations must continually think about how to define, identify, evaluate, monitor, and report on cyber risks so that they can defend their *core* assets and protect value for stakeholders. Understanding the types of cyberattacks, as well as the motives behind such attacks, is the starting point for identifying, assessing, and mitigating cybersecurity risks.

Responding to Cyberattacks

In the P&U sector, cyberattack perpetrators typically affect an organization through theft of customer data, disruption or destruction of critical infrastructure, or threats to life and safety. Each of these outcomes can have significant regulatory, financial, operational, and reputational implications.

When an organization's defenses are compromised, quickly and efficiently identifying and reacting to such compromise can prevent or significantly limit damage. This can be difficult, however. While it generally takes just hours from the time of initial attack to initial compromise, post-incident investigations have revealed that it can take weeks or even months for an organization to identify the activity. And containment and recovery can take even longer.

An Evolving Corporate Incident Response Strategy

Organizations' strategies for responding to cyberattacks continue to evolve, in part because of their ever-increasing reliance on technology. In formulating incident response strategies, organizations can profit from an examination of how the military uses intelligence to respond to cyberattacks. Deloitte's Captain (Ret.) John Gelinne[2] offered insights into how the U.S. 10th Fleet leverages its cyberintelligence partners — including the National Security Agency, U.S. Cyber Command, and others — to determine a cyberattacker's tactics, techniques, and procedures. Using such high-fidelity intelligence, the navy has synchronized network maneuvers to defeat adaptive and persistent cyberattackers.

It is not uncommon for the military to "fight hurt" against cyberattacks, assessing whether it is able to execute its mission despite network risk. This approach largely contrasts with incident response in the corporate world, where organizations, which generally lack the military's high-fidelity intelligence, are more inclined to combat cyberattacks by using a risk-averse strategy in which they isolate entire network segments that have been attacked. In such cases, an approach that relies on business continuity plans and interim manual processes to compensate for extended network outages may provide certain benefits.

[2] Captain (Ret.) John Gelinne is a director at Deloitte & Touche LLP and a former leader within the U.S. Navy's 10th Fleet (i.e., U.S. Fleet Cyber Command).

The risk-averse approaches often employed in the corporate world may not be viable or sustainable over the long term, given the difficulty of disconnecting and rebooting technological systems to eliminate cyberthreats. Thus, organizations may need to apply the lessons learned from the military to adapt to the new cybersecurity norms.

Incident Response Comparison Summary

	Detection	Triage	Respond	Recover	Sustain
Military	• "Tunable" sensors; deep intelligence partnerships • Leverage the intel capabilities of cyber partners	• "Fight hurt" • Unity of command; battle rhythm • Crisis action planning	• Deliberate planning • Strategic communications • Compartmentalize with intel "overwatch"	• Focus on "core" • Constrained by funding • Identify architecture adjustments to protect	• "Expect what you inspect" • Readiness framework
Corporate	• "Organic" sensors • Immature intel partnerships • Government "tippers" • Threat sharing and analysis centers	• Risk averse • Interim processes • Isolate • Crisis action planning defaults to IT department	• Rule by committee • Delegated authority • Ingenuity • Heavy reliance on third-party vendor management and expertise	• Focus on continuity, regulatory, legal, reputation, security enhancement • "Damage control"	?

ERM and Cyber Risk

Cyber risk is considered at all levels of the organization, including ERM. More than 90 percent of ERM professionals surveyed indicated that cyber-related risks are considered and included in their organization's risk register (with more than 75 percent indicating that they have two or more cyber-related risks). While most ERM programs in the P&U sector take cyber risk into account, views differ on the extent of ERM's role in cyber-risk-related efforts, which may include assisting with monitoring, developing reports, evaluation, identification, and reporting to management. More than 90 percent of ERM professionals surveyed indicated that their team provides regular updates to the organization's risk committee and the board of directors, though the frequency varies from as little as annually to as much as monthly.

Shared Corporate Responsibility

Cyber-risk response represents a shared corporate responsibility. Setting a "tone at the top" establishes accountability and fosters a cyberaware corporate culture. Further, because employees are a potential entry point for cyberattacks, they should be trained to identify possible threats and act accordingly. Such training can help an organization gauge how quickly and well it would respond to a potential attack.

Cyberintelligence groups, though currently rare in the P&U sector, are increasingly being used to provide advance warning and to help an organization understand potential risks. In addition, regular reporting on topics such as intelligence, the regulatory environment, and viruses and other incidents can help an organization understand the magnitude of cyber risks.

Key Takeaways

- Understanding the types of cyberattacks, as well as the motives behind such attacks, is the starting point for identifying, assessing, and mitigating cybersecurity risks.
- While it generally takes just hours from the time of initial attack to initial compromise, post-incident investigations have revealed that it can take weeks or even months for an organization to identify the activity. And containment and recovery can take even longer.
- Because of their increasing reliance on technology, organizations often cannot afford to go offline while investigating potential cyberattacks. Thus, they may need to adopt new incident response strategies, including "fight hurt" techniques.
- Cyberintelligence groups are increasingly being used to provide advance warning and to help organizations understand potential risks.

Link Between Crisis Management and ERM

Recent studies appear to indicate that the crisis management function is a natural extension of ERM efforts and has become one of the more important facets of an organization's risk assessment strategy. Although organizations can identify and mitigate the risk of potential cyberattacks or physical disasters, risk can never be entirely eliminated; it is therefore important to implement emergency management plans and consider preparing integrated plans to protect against multiple crises.

When evaluating risk, the ERM function at an organization should consider the organization's emergency response plan as well as its ability to respond to a significant crisis when assessing its capabilities. Almost 40 percent of the ERM professionals polled believe that the weakest link in responding to a significant crisis is *coordinating the response across the organization*, while more than 25 percent think that *understanding how the crisis is evolving* is the key aspect of crisis management that needs to be improved.

Thinking It Through

Deloitte has identified nine leading crisis response capabilities. Almost 30 percent of the ERM professionals polled believe that *response organization* is the least developed of these capabilities. Other capabilities that ERM professionals believe are in need of further development include *the decision-making process* (18 percent), *crisis communication* (12 percent), *ongoing crisis monitoring* (12 percent), *information management* (12 percent), and *other* (16 percent).

Key Takeaways

- Risk cannot be entirely eliminated. Research has shown that an organization can expect a value-destroying event at least once every five years.
- A crisis is a major catastrophic event, or a series of escalating events, that threatens an organization's strategic objectives, reputation, or viability.

Thinking Ahead

The Deloitte P&U sector team will continue to monitor current and future ERM-related activities. As an industry leader, Deloitte will continue to host these roundtable events so that P&U ERM professionals can share prevailing practices with others in the industry. The next ERM roundtable is scheduled for October 13–15, 2015, and will be held at Sempra Energy in San Diego, California. Keep an eye out for the pre-roundtable survey; the results will be a catalyst for discussion. 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

Paul Campbell
Principal
Deloitte & Touche LLP
+1 713 982 4156
paulcampbell@deloitte.com

John McCue
Principal
Deloitte & Touche LLP
+1 216 830 6606
jmccue@deloitte.com

Asma Qureshi
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.

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

- Mid-Year Outlook: Balancing the Bullish U.S. Deal Market With Regulatory Pressure and Global Risks (May 13, 2 p.m. (EDT)).

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!