Deloitte.

In This Issue

Making Power and Utilities Companies Resilient in a Changing Risk Landscape

The Bottom Line

- Power and utilities (P&U) companies should build resilient organizations that can monitor uncertainties and trends, adapt to changing operating environments, and recover from significant impacts in a shifting risk landscape.
- There is no "one-size-fits-all" enterprise risk management (ERM) function, and risk teams need to be more aware of the organization's culture, strategic vision, objectives, leadership, operational model, and board expectations.
- A number of risk professionals in the P&U sector are evaluating the alignment of ERM with the resilience portfolio of functions.
- Companies must be able to identify the root causes and consequences of cyber risk and gain a complete understanding of assets that are "crown jewels" within the cyber risk environment. To achieve comprehensive management of cybersecurity risks, ERM and cybersecurity business functions must work together to assess and manage the impact on the organization.
- To stay relevant and achieve greater resilience, market differentiation, and strategic positioning, companies need to build their brand, cultivate stakeholder advocacy, and protect against reputation risk issues.
- Investing in brand risk-intelligent strategies and capabilities should allow companies to take steps now to better position their brand to achieve competitive advantage and to protect and enhance their reputation for a new future.
- Effective board reporting is built on an understanding of what information helps members and leadership to make risk-informed decisions and gives them confidence that risks are being understood and managed.
- A structured approach to quantifying risk can result in risk-informed decision making, which offers an opportunity to better understand future outcomes.
- By developing an understanding of these uncertainties and signals of emerging risk, organizations may be able to better prepare for what lies ahead.

Beyond the Bottom Line

Overview

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

The fall 2016 roundtable was held in November 2016 at Ameren Services in St. Louis. Deloitte and over 40 risk professionals representing about 30 companies discussed (1) the alignment of ERM with crisis management, (2) cyber risk framing, (3) the importance of reputation resilience, (4) executive and board reporting, (5) the quantification of strategic risk, and (6) the results of a poll of roundtable participants that identified their top risks. In addition, in an open session, participants explored how they would build an ERM program if they could start from scratch and what elements they would address differently. The most commonly discussed capabilities were further integration of the ERM function into strategic decision making and the value of ERM to senior executives. Perhaps the prevailing message, however, was that there is no "one-size-fits-all" ERM function and that risk teams need to be more aware of the organization's culture, strategic vision, objectives, leadership, operational model, and board expectations.

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

Alignment of ERM With Crisis Management

Global instability, new threat vectors, and more frequent and severe weather incidents have led to a rise in concern about the effect of major events on organizations. These episodes, combined with increased legislative and regulatory changes and growing customer expectations, are putting pressure on management in the P&U sector. Interest has emerged in aligning various resilience functions, such as crisis management, physical and logical security management, and disaster recovery, under one umbrella. A number of risk professionals in the P&U sector are evaluating the alignment of ERM with the resilience portfolio of functions.

One roundtable participant shared her company's "all-hazards approach," which involves avoiding incidents through risk mitigation actions and responding to incidents with emergency management plans that are tailored to specific events, such as cyberthreats, severe weather, pandemics, and grid or supply disruptions. From her perspective, the key to the ability to respond is the development and integration of a crisis management initiative throughout the organization with ERM efforts to oversee both planning and response. As with any key initiative, organizations would need to provide the appropriate levels of socialization and training to implement an integrated and continuous improvement platform. Clearly allocating roles and responsibilities can also give organizations the flexibility they need to prepare for, respond to, and recover effectively from crises.

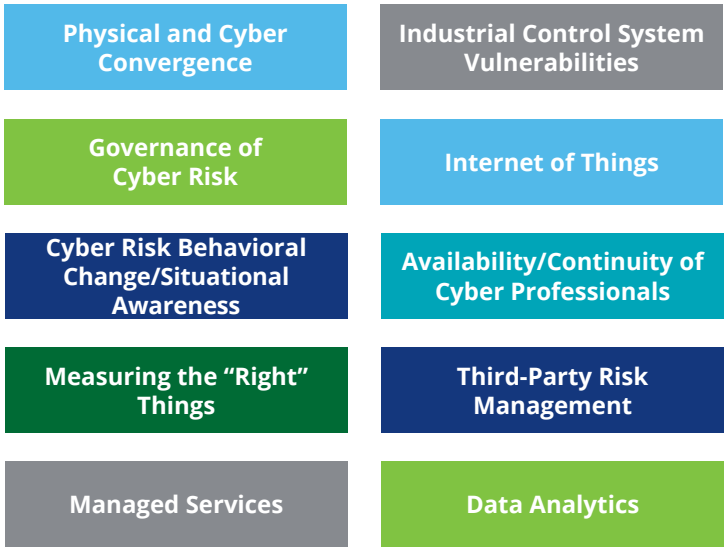
Key Takeaways

- A crisis is an event that has unpredictable consequences beyond widespread and catastrophic damage. It typically has rapid speed or may exhibit a confluence of forces that pose unique challenges.
- Aligning crisis management with ERM functions may provide further insight into the quality of mitigation strategies. In addition, crisis management monitoring capabilities and data analytics can be great resources from which ERM functions can obtain a better understanding of enterprise risk trends.
- In the new risk environment, novel thinking is required about planning for and managing events. The final building block in the design of a corporate resiliency program is the assignment of clear responsibility for planning, training, and the development of response activities as part of an overall strategy to mitigate risk.

Deep Dive Into Cyber Risk

Investments in cyber risk response are at an all-time high, yet successful cyberattacks and cyberthreats are still on the rise, both in number and sophistication. Resource shortages, increased costs, heavy reliance on third-party vendors, and fast-paced strategic technology innovations are some of the conditions that continue to challenge P&U companies. Cyber risks may affect operational assets, financial records, personal data, and intellectual property, and the implications of such risks could have a devastating effect on financial performance, service reliability, and the reputations of companies and the sector as a whole.

Cyber Risk Trends



To develop and execute response strategies that reduce the impact of cyber risk, companies must be able to identify the root causes and consequences and gain a complete understanding of assets that are "crown jewels" within the cyber risk environment. To achieve comprehensive management of cybersecurity risks, ERM and cybersecurity business functions must work together to assess and manage the impact on the organization.

Companies must reach a consensus on what is important to them and establish a consistent understanding of cyber risk throughout their organizations. What are the crown jewels? Why are they significant? Once organizations have identified the crown jewels (some categories may include information technology, operations technology, research and development, third

parties), they should understand what major factors could lead to unforeseen outcomes (risks) and what those overlooked outcomes are.

Understanding the crown jewels, the major root causes of unforeseeable outcomes, and the impacts of those outcomes may help entities develop a consistent cyber risk profile. Such knowledge may also help them establish the key risk indicators and matrices to monitor cyber risk trends and resource allocation.

Industry Perspective

One category of cybersecurity risk that can be hard to address and is therefore often overlooked is insider threats. Employees or contractors are often in positions to cause far more damage, either intentionally or unintentionally, than are outside actors. While cybersecurity departments may institute tools for identifying such actions and training to prevent them, organizations can also address threats through their employees and contractors directly. Carelessness by employees or a drop in morale can increase the chances of insider threats. By understanding its culture and monitoring employee sentiment, an organization can identify potential threats before they become actions and address them accordingly.

Key Takeaways

- An understanding of which group of assets is the most important to an organization can allow better measurement and mitigation of cyber risks.
- Predictive analytics can help entities identify, prepare for, and respond to cyber events.
- Understanding what senior leadership and the board need to know about cyber risk is key to aligning ERM with the rest of the organization as well as to understanding how cyber risk affects the business and ways in which the business can mitigate its exposure to cyber risk.

Reputation Risk

"It's reputation risk, not crisis, that matters most."

While most companies agree that reputation is critical to their success, the majority are not doing enough to manage it. In the pre-roundtable poll, only 27 percent of companies felt that they were well prepared to handle brand and reputation risk, and 62 percent had reputation risk in their risk registry. Being purely reactive not only leaves companies vulnerable but also limits their ability to seize value-creating opportunities. As a P&U risk manager said, "It's reputation risk, not crisis, that matters most." To stay relevant and achieve greater resilience, market differentiation, and strategic positioning, companies need to build their brand, cultivate stakeholder advocacy, and protect against reputation risk issues.

Factors Influencing a Company's Reputation

- Emotional connection.
- Pride in affiliation.
- Promise of quality.
- Confidence of delivery.
- Legacy and longevity.
- Established trust.

Reputation risks are natural consequences of strategic and operational decisions and are typically influenced by factors outside the entity's direct control (see the list above). Damage to reputation can occur from intentional or unintentional acts by employees, customers, third parties, or unanticipated events, or simply from untimely or improper responses to issues and events. Reputation risks can be internal or external. Common internal risks include employee or executive misconduct, inconsistent messaging, or lack of compliance. External risks include cyberattacks, regulatory changes or scrutiny, or economic shifts.

Given the wide variety of sources of reputation risk, leading companies take a holistic and programmatic approach to managing reputation. This helps them align resources and capabilities to activate the brand, deepen brand advocacy, and protect their reputation. Key steps in this alignment are linking brand and reputation to business strategy, engaging stakeholders to shape reputational perceptions, and developing action plans to respond to reputation-threatening events. One P&U risk professional noted that with the increasing importance and integration of reputation throughout an organization, the chief risk officer is assuming the role of chief reputation officer as well.

Investing in brand risk-intelligent strategies and capabilities should allow companies to take steps now to better position their brand to achieve competitive advantage and to protect and enhance their reputation for a new future.

Industry Perspective

One P&U risk leader made the point that while businesses in competitive industries have to closely protect their reputation, P&U companies frequently operate as monopolies and therefore are not at substantial risk of customer loss. Is reputation risk as significant if the business is not going to lose customers?

Participants responded to this question in a number of ways. A representative from a P&U entity that had gone through a major environmental event described the demoralizing nature of working for a company that wasn't respected in the community and the challenges that can come from trying to recruit new talent when the company's reputation has been tarnished. Other participants noted advantages brought by a strong reputation, such as fewer obstacles to acquisitions, good standing among regulators, and greater resilience after future compromising events. Furthermore, competition is increasing as a result of new technology, which is likely to enhance the importance of reputation in the future.

Key Takeaways

- Reputation management is both a risk and an opportunity.
- External perceptions drive reputation.
- Trust and communication are key.
- As the risk environment evolves, organizations must adapt their approach to reputation management.

Board and Leadership Reporting

According to the pre-roundtable poll, nearly all (94 percent) of chief risk officers or their equivalents report to the board periodically, generally on a quarterly basis (50 percent). With the rise in prominence of the chief risk officer's role, there is an increased need for entities to showcase the value of ERM and tie risk reporting to company objectives by focusing on key risks to a company's business, strategy, and reputation as well as the trends, velocity, and potential impacts of those risks. A few characteristics of strong risk reporting include:

- Application of a balance between qualitative and quantitative information.
- Use of top-down principles but reliance on bottom-up data.
- Continual evolvement to account for emerging risk trends, the needs of the business, strategic priorities, and deep dive risk analysis.
- Integration of analytics and deployment of data discovery and data reorganization.

The challenge for risk professionals lies in understanding stakeholders' needs and providing them with predictive reporting that covers both what they want and what they need. One ERM professional shared how his reporting ties into strategic imperatives, such as operational excellence, project excellence, financial strength, and social license. According to the pre-roundtable poll, 57 percent of the organizations use manual dashboards to report on risk and feel that interactive dashboards would help improve their reporting processes. The value for risk professionals in continually changing and adapting their reporting is that they are able to incorporate emerging risk trends and risks to the strategic priorities as well as to integrate analytics directly into processes to further augment reporting.

Leading Practices and Hot Topics in Board and Leadership Reporting

Board of Directors	Executive Management
• Risk program is directly tied to "value killer" or critical strategic risks. • Risk oversight is the entire board's responsibility. • Require specific competencies, frequency, and depth of timely discussions. • Reputation risk is the "meta" of all risks, and top-of-mind topics include cyber risk, risk appetite, and innovation/risk/compliance culture.	• Dashboard reporting (i.e., predictive analytics, risk sensing, key risk indicators). • Risk culture and the people side of risk management are critical and often overlooked. • Social media is a risk and an opportunity. • Chief risk officer's role is increasing, with visibility to full board and alignment with strategy. • Risk is a defined agenda item within executive management team meetings.

Industry Perspective

Roundtable participants discussed various ways that risk reporting catered to different audience levels in the organization. Closing the gap between "information" and "action" with critical insights was deemed the most valuable method of improving an organization's reporting process. One P&U professional shared a story of "dumbing down" a presentation. When the chief risk officer deemed a first draft too data heavy to be included in board reporting, the P&U professional made it simpler. The second version was still too detailed, so he eliminated more, leaving only key points. After he made one final edit to delete all but the critical elements, the report was presented and proved to be extremely effective at piquing the board's interest and successfully communicating the desired information. It is critical to know one's audience and report the right level of detail to engage boards and executives.

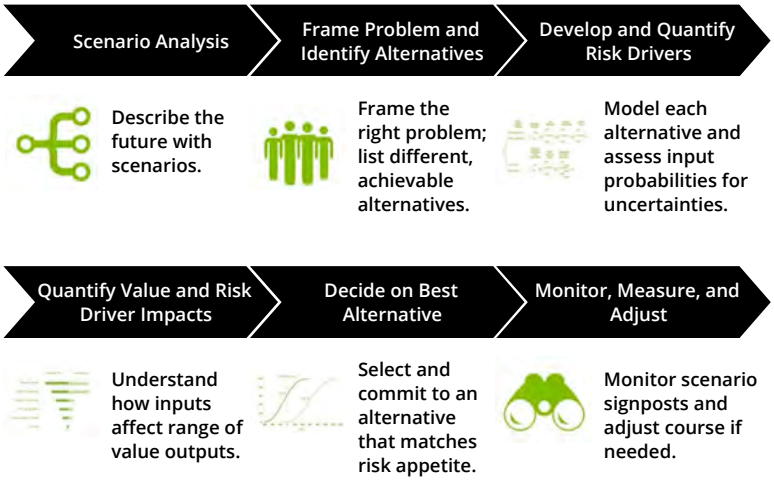
Key Takeaways

Effective board reporting is built on an understanding of what information helps members and leadership to make risk-informed decisions and gives them confidence that risks are being understood and managed. Leading practices include:

- Focusing on key risks to a company's business, strategy, and reputation.
- Closing the gap between "information" and "action" with critical insights.
- Using internal and external information that is more predictive than reactive.

Strategic Risk Quantification and Decision Analysis

As leaders acknowledge the challenges of dealing with uncertainty, a structured approach to strategic decision making can help achieve consistency in decision quality and better resource prioritization.



Traditional ERM approaches to strategic risks can often come up short. Lack of predictive ability, biases in decision making, and the absence of a clear understanding of the risk universe limit an organization's capacity to adequately take risk into account during strategy setting and make truly risk-informed decisions. Nearly half (45 percent) of the roundtable participants do not have a consistent method for quantifying risk, and only 11 percent use probabilistic simulation or decision trees. An inability to consistently quantify risk can result in imprecise tracking of trends and potentially inaccurate prioritizations. While the probabilistic approach is not infallible, it provides a range of data that illuminates potential outcomes,

thereby permitting an organization to enhance the focus of its risk decisions and achieve consistency in their quality.

Industry Perspective

One industry risk professional shared an approach to strategy risk assessment that is built on the concepts of a traditional risk assessment. Under this approach, the ERM function facilitates conversation for each risk associated with a strategic initiative. The professional highlighted major differences between the strategy and risk functions and focused on (1) an integrated assessment of internal and external enablers and disablers, (2) an ERM function review of signposts to key strategy assumptions, and (3) the use of scenario analysis to refresh or test plausible future states. This interaction between the strategy and risk function helps foster an integrated approach to stakeholder decision analysis, including the quantification of potential outcomes.

Thinking It Through

In conversations with stakeholders, it is important to clearly describe uncertainty. Metrics alone can't be used for successful modeling; a risk professional needs to sit down with the experts and learn what could affect the probability of certain outcomes. To demonstrate the importance of using standard language with clear meanings, one risk professional gave members of the audience a list of phrases and asked them to assign a percentage of certainty to each. The certainty levels for "doubtful," "good shot," "fighting chance," "fairly likely," and "risky" ranged from 0 to 90 percent, showing that terms expressing probability might be construed one way by one person and an entirely different way by another.

Key Takeaways

- Use a structured approach to achieve consistency in decision quality.
- Assess uncertainty because outcomes are not the same as decisions.
- Ensure that in conversations with stakeholders, probability is described clearly.

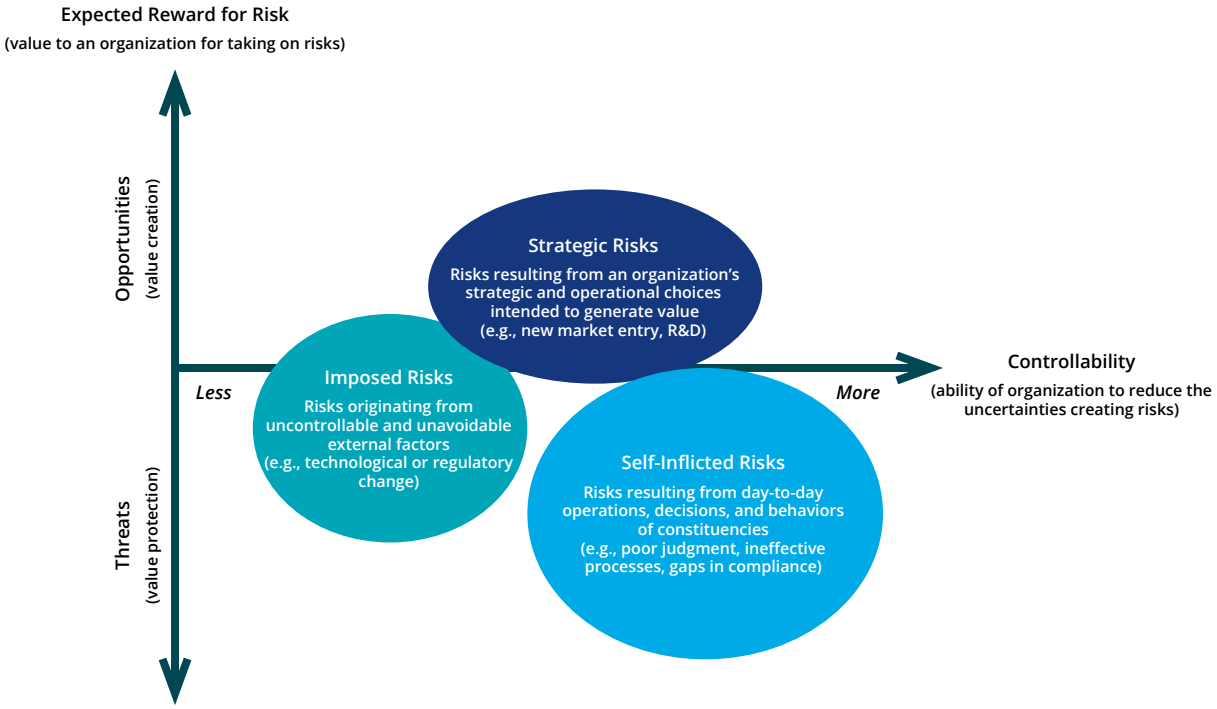
Recent Sector Trends and Top Risks

In 2013, roundtable participants were asked to name the top 10 risks to their organization. The risks listed reflected a fairly stable portfolio of P&U risks, including infrastructure reliability, financial performance, and health and safety. When the same poll was conducted again in 2016, it revealed some significant shifts in risk priorities for the participating organizations.

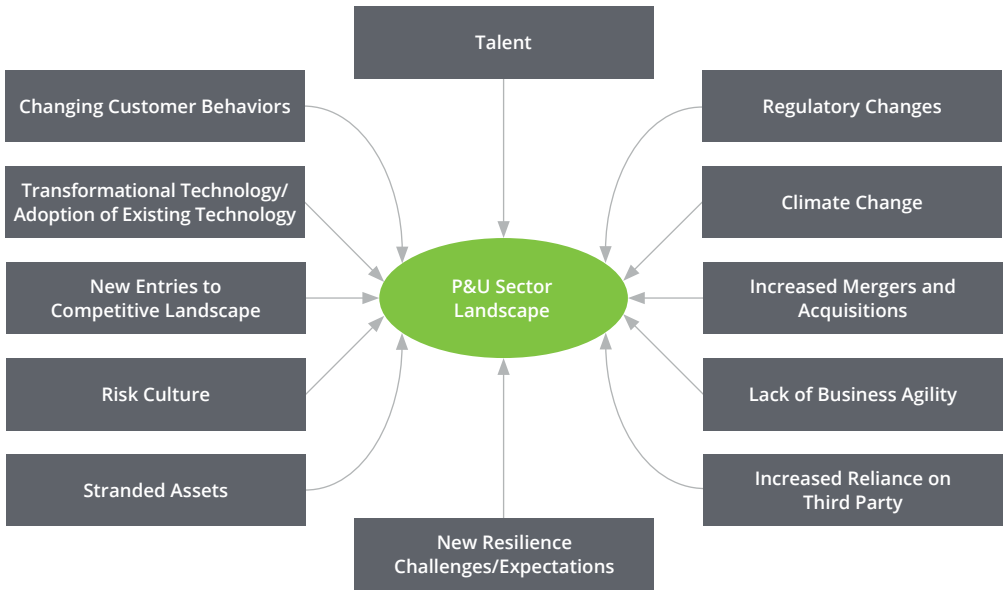
Of the five most commonly listed risks, only two appeared in both 2013 and 2016: cybersecurity and changing regulations. While the 2013 top five had been rounded out with infrastructure reliability, strategy/business growth, and financial performance, these had been replaced in 2016 with market price change, business model/industry transformation, and business resilience.

Perhaps the most striking shift was business resilience. While in 2013 it was the 18th most frequently identified risk, it was the 3rd in 2016. Other risks identified significantly more frequently include reputation risk, customer relationships, rogue insiders, and physical security.

Taken together, the risks that are most rapidly shifting illustrate a P&U sector less concerned about the long-term viability of its assets than about a fluctuating risk landscape in which changing customer demands and technological advances result in industry change, the swift onset of reputation-damaging events, and a constant threat of a cybersecurity incident. In the 2013 survey, respondents characterized 5 percent of risks as strategic, 22 percent as imposed, and 73 percent as self-inflicted. Those statistics can be contrasted with the results of the 2016 survey, which indicate that 20 percent were strategic, 30 percent were imposed, and only 50 percent were self-inflicted. The graphic below shows how each of these risk types are characterized.



How much of this risk shift could have been predicted in 2013? What will the top risks look like in 2019? The graphic below shows some of the key factors and trends that could shape the risk landscape in the near future. By developing an understanding of these uncertainties and signals of emerging risk, organizations may be able to better prepare for what lies ahead.



Key Takeaways

- It is important to be aware of uncertainties and signals of emerging events to understand their potential effect on an organization.
- A look outside the P&U sector (e.g., to the auto, health care, or financial industry) can help an entity identify emerging risks.
- The P&U sector is increasing its focus on risks that are strategic and imposed rather than self-inflicted.

Common Theme

Although topics as seemingly disparate as board reporting and cybersecurity were discussed, the roundtable conversation centered on a common theme: the rapid evolution of the environment in which P&U companies operate. Changing regulations have the potential to reshape the industry, and new technologies have the potential to disrupt traditional ways of doing business. In this environment, risk leaders have little choice but to prepare for change and to be ready to adapt and recover when the unpredictable comes to pass. Such preparation cannot be done in a vacuum. Those responsible for monitoring and reporting risks must be able to engage the right stakeholders, use experts, and make the case to boards and executives for why they must consider risk and how they can build a more resilient organization.

Contacts

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

Dmitriy Borovik
Managing 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.
- Controllership perspectives.
- Driving enterprise value.
- Financial reporting.
- Financial reporting for taxes.
- Governance, risk, and compliance.
- Tax accounting and provisions.
- 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.

DART and US GAAP Plus

Put a wealth of information at your fingertips. The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, IASB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and navigation system that, together with its powerful search and personalization features, enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's FASB Accounting Standards Codification Manual, and can also elect to receive *Technically Speaking*, a weekly publication that highlights recent additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.

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 those 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!