Understanding Enterprise Risk Management for Utilities

Committee of Chief Risk Officers

May 2007

Executive Summary

Changes in the utility industry, such as deregulation, have been key drivers in changing the way companies, and the outside world, view utilities. These changes are precipitating an expanding interest in Enterprise Risk Management (ERM) by utilities as they express interest and conviction about the need for robust risk management frameworks and capabilities. A previously published CCRO paper entitled "Enterprise Risk Management and Supporting Metrics" outlined many of the concepts of ERM in considerable depth. However, upon completion of that effort, it became evident that further focus on this topic was needed specifically for utilities. While the fundamental ERM concepts are generally applicable across all types of entities, CCRO members recognized that the magnitude of and emphasis on specific components of the ERM framework are quite different for a regulated versus un-regulated entity. Therefore the CCRO commissioned a working group to develop this paper addressing the specifics of ERM for regulated utilities (including self-regulated public power utilities).

The objective of this paper is to provide an understanding of ERM and assist executives in developing and applying an ERM framework unique to the business of a regulated utility. For the purpose of this paper, a utility is defined as an entity that has rates that must be approved by a regulatory authority, be it local, state, regional or federal (including public power entities' self-regulating governance), and tends to have extensive exposure to operative risks. Further, this paper focuses only on energy-related utilities that offer products or services to the power and gas sector.

The CCRO has defined ERM as the program or process enacted to identify, assess, quantify and respond to the complete set of risks facing a firm in an integrated fashion. Risk is defined as the likelihood and severity of an event or action that will adversely affect the company's ability to achieve its business objectives and execute its strategies successfully. The utility considering the implementation of an ERM framework can view it as the aspirational destination on a Risk Management Continuum (see Figure E.1). On all parts of the continuum, the traditional activities associated with identifying, assessing, quantifying, controlling and mitigating specific market, credit, operative or business risks will exist.[1] The main differentiator across the spectrum lies in the level of integration achieved in the firm.

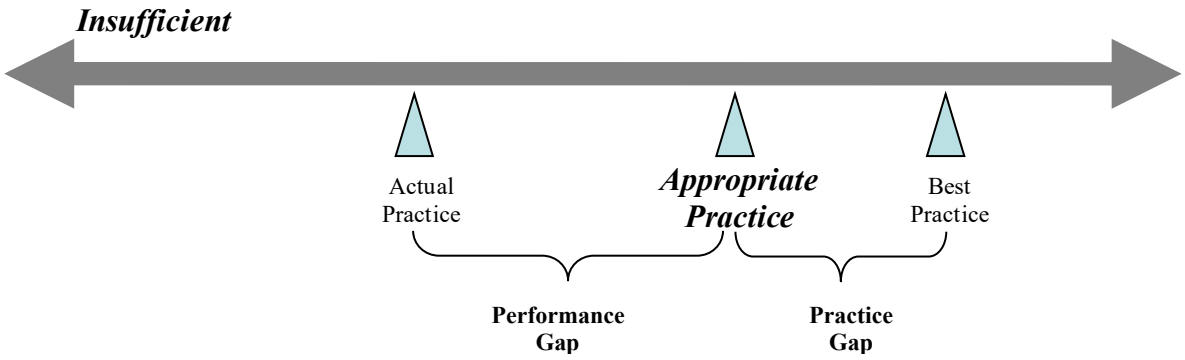
[1] Earlier white papers provide a comprehensive discussion of what the CCRO members consider "best practice" in several of these areas such as Analytics and Valuation, Credit Risk Management, Governance and others. Readers interested in reviewing these documents can find them at www.ccro.org.

Figure E.1: RISK MANAGEMENT CONTINUUM

This continuum demonstrates that risk management practices can vary from individual business unit or even departmental risk management to fully integrated cross-company risk aggregation, monitoring and management.

The intent of this paper is to provide guidance to utilities that are implementing or improving ERM frameworks. Such frameworks are not prescriptive, one-size-fits-all endeavors. Rather an ERM framework must balance the utility's risks, business and regulatory structures and current risk management practices and governances. The guidelines published herein are intended as objectives to strive toward, only to the extent that it is practical and useful in managing the individual utility's risk. Further, the full implementation of an effective ERM framework may be iterative, with each iteration improving on the framework. Therefore, each utility must consider where they are on the Risk Management Practices Continuum.

Figure E.2: Risk Management Practices Continuum



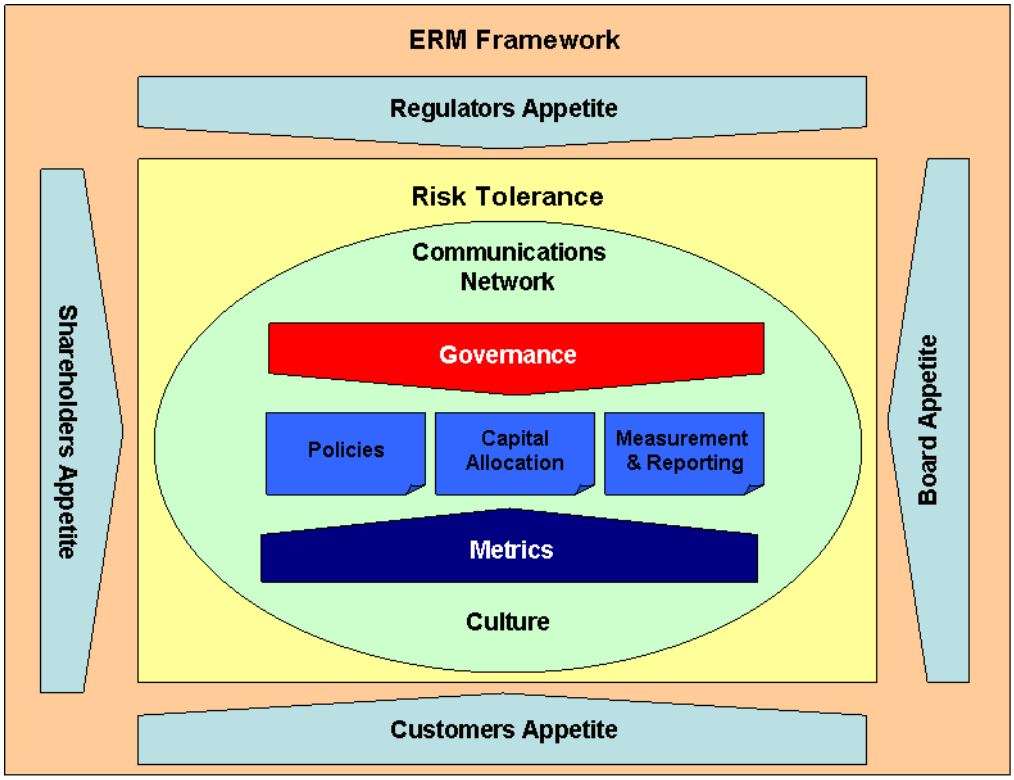
Many utilities may be tempted to strive for 'industry best practice' in developing all aspects of an ERM Framework. However, some particular 'industry best practices' may in fact not be a necessary part of the most efficient and effective ERM program for an individual utility. Instead, the utility must aspire to implement those practices that close performance gaps by identifying and effectively managing the risks it faces. Unlike 'industry best practice', *appropriate* practices will vary from utility to utility depending on business model, size, etc. Figure E.2 demonstrates that utilities should be cognizant of the differences between their current

actual practice, best practice, and what is appropriate practice for their business and risk portfolio. In short, it can be okay to select a 'practice gap' for specific aspects of your ERM framework.

The general structure of the ERM framework is shown in Figure E.3. As this diagram demonstrates, the complexity of each component is not emphasized. Rather, it establishes that, when implementing an ERM framework, it should have the components noted, but the sophistication of these components should depend on the complexity of the firm's portfolio and the available risk management resources. The key components that must be included for a successful ERM framework are:

- Identification of Risk Appetite
- Definition of Risk Tolerance
- Development of a Risk Awareness Culture
- Establishment of Corporate Governance
- Definition of Risk Metrics
- Creation of Risk policies
- Establishment of a Capital Allocation process
- Implementation of measurement and reporting consistent with the metrics, governance, and strategy

Figure E.3: ERM Framework



The key benefits of an ERM framework include robust internal processes, governance, controls and communication, and enhanced stakeholder relations and risk awareness. Specifically, ERM addresses stakeholder concerns and aids management because it:

- Creates a disciplined and consistent method to identify, communicate and manage risk;
- Establishes a clear link between strategic business plans and key risks;
- Aligns risk tolerance from Board through Management to Staff levels;
- Creates integrated and coordinated approaches to managing risk across all business units;
- Fulfills lender and credit rating agency requirements;
- Efficiently allocates spending capital
- Addresses higher Board and Officer risk management expectations;
- Promotes a risk awareness and management culture
- Enhances the external view and reputation of the entity; and
- Leads to better and more informed decision making.

In summary, an ERM framework improves understanding of the risks that impact the enterprise and how these may be manifested; encourages employees to integrate risk management into their normal activities; demonstrates risk management performance to stakeholders; enhances confidence that the risk profile is understood and being monitored in accordance with the enterprise's risk management plan; and focuses management attention on key risks.

ERM implementations should be highly customized at each firm such that the final framework is appropriate and reflects the complexity, size and sophistication of the company. Nevertheless, there are several key ingredients to a successful ERM framework and there are specific steps that can be taken to facilitate implementation. Virtually all ERM applications follow a typical framework as described in this section of the report. This process is illustrated in the figure E.4.

Figure E.4: Six Step Process for Enterprise Risk Management

Step 1: Identify and Quantify Risks. This step is generally a bottom -up process with information provided by each business unit. However, firms usually employ a risk management department or committee to inventory, collect, and measure, or validate the quantification of risks. Once a firm identifies the dozens of risks they face, then the risks are typically categorized and prioritized based on various quantification techniques. When statistical tools and/or data are not available to quantify risks then subjective techniques are employed.

Step 2: Establish Risk Tolerance and Policies. Top priority risks that emerge from Step 1 should be addressed by the strategic plans of the firm. Furthermore, the strategic plan should identify the risk management objectives and risk tolerance of the firm. Risk Policies are then developed to formalize and articulate the risk tolerance of the organization and to clearly identify the decision-making process and authority for individuals or committees within the firm to carry out transactions or business activities.

Step 3: Develop Business Unit Strategies and Metrics. Each business unit develops specific strategies for managing the risks for which they are responsible. In some cases, the strategy for managing certain risks may be to simply monitor since mitigation may not be possible or feasible. Scenario plans may also be developed to prepare for risks that may occur but are not conducive to address through mitigation actions. Of course, Steps 1, 2, and 3 are iterative since the business units will be responsible for identifying risk and assisting in formulating the strategic plans, risk

management objectives, and risk tolerance of the organization, but nonetheless specific strategies should not be finalized until the risk management objectives and risk tolerance of the firm are clear. In addition, the corporation must then develop a process to allocate the appropriate resources to address the risks identified as being a priority.

Step 4: Implement Controls and Procedures. Develop and implement controls and procedures to provide the assurance of proper oversight, processing, and execution of business activities. A strong control and procedural process is necessary since many risks affect numerous business units even though risks are generally assigned to a single business unit to manage.

Step 5: Execute Strategies. With an ERM process in place, strategies are executed based on a clear understanding of the risks being taken, clear oversight of activities, clear controls and procedures, and clear metrics that guide the activity and measure the level of success.

Step 6: Monitor Risk and Reporting. Each business unit is responsible for monitoring certain risks and reporting up through the risk management department in some fashion. As new risks emerge, there should be a systematic process for reporting them and determining if policies or strategies should change in response to the risk.

All utilities will face challenges regarding the gap between existing and aspirational levels of risk management sophistication, formal and informal communication networks, and risk and business culture. The challenges are listed below.

Challenge 1: Implementation Sophistication - Any successful implementation of an ERM framework must consider the utility's current level of sophistication. If the utility has some risk management infrastructure in place, then the ERM framework will serve as an enhancement, with results showing improved risk management practices and procedures. Conversely, for a utility that has adopted few risk management practices, an ERM framework implementation could produce great strides in the company's understanding of their risks and subsequent management and mitigation of these risks.

Challenge 2: Communication - Identified risks and their corresponding mitigation actions need to be communicated up and throughout the utility and to senior executives and the Board in a timely and accurate manner. To ensure consistency, accuracy and transparency, a formal reporting structure with defined frequency and standardized reports should be established and utilized. Key features of the communication network depicted include the redundancy and integration points. Corporate Risk Management, the Risk Management Committee and Board Oversight Committee are key synthesis and integration points where disparate information is brought together and analyzed. The Management Committee and Board of Directors can then use this information in making decisions. Another important aspect of this communication network is the redundancy of information flows which provides for some level of independent analysis and validation. In addition, feedback from the executives to the report providers on risk issues being addressed is also an effective tool in building an ERM process. This feedback can best be provided through the Risk Management organization. Communications and risk reporting tools should not be static but should evolve as risk exposures change and as the business adapts to meet new challenges.

Challenge 3: Culture - A risk management culture is a set of beliefs, values, attitudes, customs, and behaviors about the management of risk that are shared among people in an organization. The organization's culture sets a tone and expectations for which behaviors can expect to be either rewarded or discouraged. The corporate risk culture begins at the highest level of management, the Board of Directors and senior management. The Board and senior management should be major advocates of risk management within the organization and should be aware of, understand, and support risk management activities throughout the organization.

In conclusion, it is paramount to understand that ERM is not a product, but rather a process by which utilities can iteratively improve upon their understanding, control and management of risks. An ERM framework for utilities should ultimately strive to first identify and quantify material risks, and identify the levels of risk that are acceptable for all stakeholders. Once these have been determined, the risk governance, policies, procedures, monitoring and controls should be established in a manner that is consistent with the level of risk being controlled and the current capabilities of the firm. Once the framework is in place, a continuous review of the risks, controls and metrics is essential to establishing a lasting and improving risk management function within a utility.

To successfully implement an ERM framework, each utility must first consider where they are on the Risk Management Practices Continuum. Utilities should strive to close performance gaps (as defined in the Risk Management Practices Continuum Figure above) in developing an ERM Framework by focusing on practices that most effectively manage risks for the individual utility. The general structure of the ERM framework is complex, but the key is to consider all components of ERM, the complexity of the firm's portfolio, and available risk management resources in determining the level of sophistication to apply to each of these components.

In any risk management endeavor, there will be challenges that will be unique to the company's portfolio, resources, management and regulatory environment. Nevertheless, a key ingredient to any successful framework is constant and clear communication and a culture of risk management throughout the company, led by the tone at the top.

Acknowledgements

White papers issued by the CCRO are the product of its body of members although the views expressed in any particular paper do not necessarily represent the views of an individual member. Preparation of a paper is led by a subset of CCRO members, known as a working group, with a particular interest in the subject topic. The working group then develops, researches and prepares the paper. External parties whose functions may include providing valuable expertise, perspective and/or coordination and facilitation may also assist the working group, as necessary.

In this light, the CCRO extends special thanks to the following organizations and individuals who have dedicated considerable and valuable time, resources, expertise and/or perspective to the preparation and issuance of this paper,
Understanding Enterprise Risk Management for Utilities

Company	*Representative(s)*
Constellation Energy	**Jesus (Nano) Sierra**, Working Group Chair
	Margot C. Everett
American Electric Power	**Douglas R. Buck**
Aces Power Marketing	**John W. Sturm**

The CCRO would also like to extend a special acknowledgement and thanks to

Accenture **Mark A. Ruane**

for coordinating the activities of the working group and for his making contributions to the white paper.

Table of Contents

1. Introduction

Regulated utilities, in many cases, are continuing to apply an Enterprise Risk Management (ERM) framework. This is a process that has been taking place over the past several years since energy companies and regulated utilities with trading activities embarked on ERM implementation in the late 1990s. One key reason for this lag is that these entities had a regulatory 'cushion' whereby, as long as the company's operations were "prudent", losses could usually be recaptured through rates. In the past, utilities and stakeholders have viewed their business model as low risk. They believed that their systems, business practices and operations were sufficient to control the few risks they had and thus did not view themselves as having significant risks to manage. Changes in the utility industry, such as deregulation, have been key drivers in changing the way these companies, and the outside world, view utilities. Factors now affecting utilities include rate freezes, higher and more volatile costs of capital, and more volatile supply rates resulting from deregulated generation. Many new risks such as environmental and regulatory issues, aging workforce and infrastructure, increased competition in generation, competition for capital, volatile commodity prices, trading scandals, and the continuing focus on reliability are just a few of the drivers behind utilities changing the way in which they view themselves.

Based on these changes, there is an expanding interest in ERM as this industry continues to transform itself. The historical regulatory protections have been all but eliminated as regulators are increasingly transitioning the placement of risks from ratepayers to shareholders in the investor-owned utility business model. Significant load growth coupled with increased competition on the supply side has forced utilities to become more conscientious about their capital allocations while regulators are questioning any capital expenditures made by these entities. Finally, today utilities are participating in the expanding traded commodities markets while providing safe, reliable, and lowest cost energy to their customers along with state-of-the-art customer service. The markets in which these companies are operating are dynamic and volatile and many such entities are facing financial stresses with increased regulatory scrutiny.

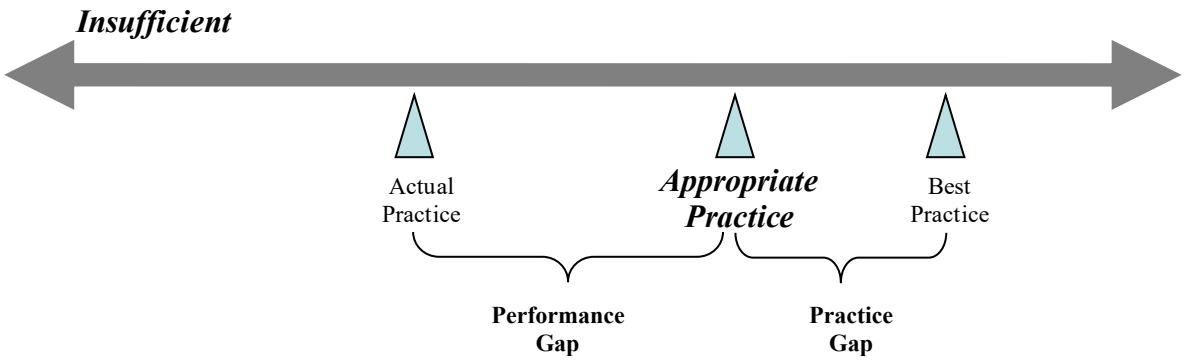
As a result of these changing tensions, utilities are expressing interest and conviction about the need for robust risk management frameworks and capabilities, which was the primary driver to the formation of the Committee of Chief Risk Officers (CCRO). The CCRO is comprised of senior risk professionals from leading energy companies participating in all sectors of the energy industry. Over the past four years, the CCRO has published a series of "white papers" that present risk management practices and disclosure standards in an attempt to raise the industry-wide awareness of these topics. One such paper published by the CCRO on the topic of ERM fully discusses the concepts of ERM and the supporting metrics. However, upon completion of that effort, it became evident that further focus on this topic was required specifically for utilities, as the scope of ERM was generally applicable for these entities, but the magnitude and focus differed greatly from deregulated energy entities. Therefore the CCRO commissioned a working group to develop a paper that would address the specifics of ERM for regulated utilities (including self-regulated/governing public power utilities).

1.1. Objective

The objective of this paper is to provide an understanding of ERM and assist executives in developing and applying an ERM framework unique to the business of a regulated utility. This paper establishes a framework for assessing the collective risk of the company, and assuring accountability for the evaluation and mitigation of risk. Within this paper, a utility is defined as an entity that has some component of regulated revenues from an obligation to provide full service to some or all users in a pre-determined service territory using a specified portfolio of assets and related infrastructure. Due to the considerable information already published on ERM, this paper only touches on basic concepts and fundamentals related to an ERM program, pointing the reader to the more in-depth discussions in other papers. As a result, this paper focuses on particular issues that apply to a utility in the context of an ERM program and the unique challenges these companies face.

The intent of this paper is to provide guidance to utilities that are implementing or improving ERM frameworks. Such frameworks are not prescriptive, one-size-fits-all endeavors. Rather an ERM framework must balance the utility's risks, business and regulatory structures and current risk management practices and governances. The guidelines published herein are intended as objectives to strive toward only to the extent that is practical and useful in managing the individual utility's risk. Further, the full implementation of an effective ERM framework may be iterative, with each iteration improving the framework. Therefore, each utility must consider where they are on the Risk Management Practices Continuum, shown in Figure 1.1.

Figure 1.1: Risk Management Practices Continuum



Many utilities may be tempted to strive for 'industry best practice', which is continually evolving at this point, in developing an ERM Framework, yet 'industry best practice' may not be the most effective risk management framework for an individual utility. Instead, the utility must aspire to implement those practices that best manage the risks the utility faces. Figure 1.1 demonstrates that utilities should be cognizant of the difference between their current, actual practice versus what is appropriate for their business, size, and risk portfolio. A best practice component of risk management may be marginally, if at all, improving risk management practices from the appropriate practice level.

1.2. What is ERM?

The CCRO has defined ERM as the program or process enacted to identify, assess, quantify and respond to the complete set of risks facing a firm in an integrated fashion. The CCRO emphasized that Enterprise Risk Metrics are a key component of an ERM framework and enable the assessment, quantification and reporting of identifiable risks. The utility considering the implementation of an ERM framework can view it as the aspirational destination on a Risk Management Continuum (see Figure 1.2). On all parts of the continuum, the traditional activities associated with identifying, assessing, quantifying, controlling and mitigating specific market, credit, operative or business risks will exist.[2] The main differentiator across the spectrum lies in the level of integration achieved in the firm.

Figure 1.2: RISK MANAGEMENT CONTINUUM

On the left end of the continuum lies the silo approach to risk management in which all risks are more or less treated on a stand-alone basis with little consideration given to portfolio level interactions. This fragmented approach may even translate into different approaches to measuring the same type of risk across business units or at different points in time. The next step in the continuum is to "Integrated Silos", where firms exhibit greater levels of risk management capability and there is consistency with which risks are measured within a risk or organizational silo (e.g., all supplier and customer credit risk is measure and monitored consistently across the utility). The next step of the continuum marks a clear progression toward an ERM framework, whereby risks from different silos (e.g., distribution, transmission and generation) are consistently assessed, managed and reported in an integrated manner. At the far end of the continuum is ERM which represents the highest level of sophistication currently possible for an organization. Such a framework helps a company deal effectively with uncertainty by providing a portfolio view of the risks affecting the organization across all silos, and thus enables a common understanding of risk. At this level, the business units continue to be involved in the identification, assessment, qualification and quantification, control and mitigation of risk. As such, the basic building blocks for managing the different silos continue to be useful, but ERM is layered over them and leverages the information to provide an integrated perspective and bring the risks to the attention of the appropriate and cross-organizational management level.

[2] Earlier white papers provide a comprehensive discussion of what the CCRO members consider "best practice" in several of these areas such as Analytics and Valuation, Credit Risk Management, Governance and others. Readers interested in reviewing these documents can find them at www.ccro.org.

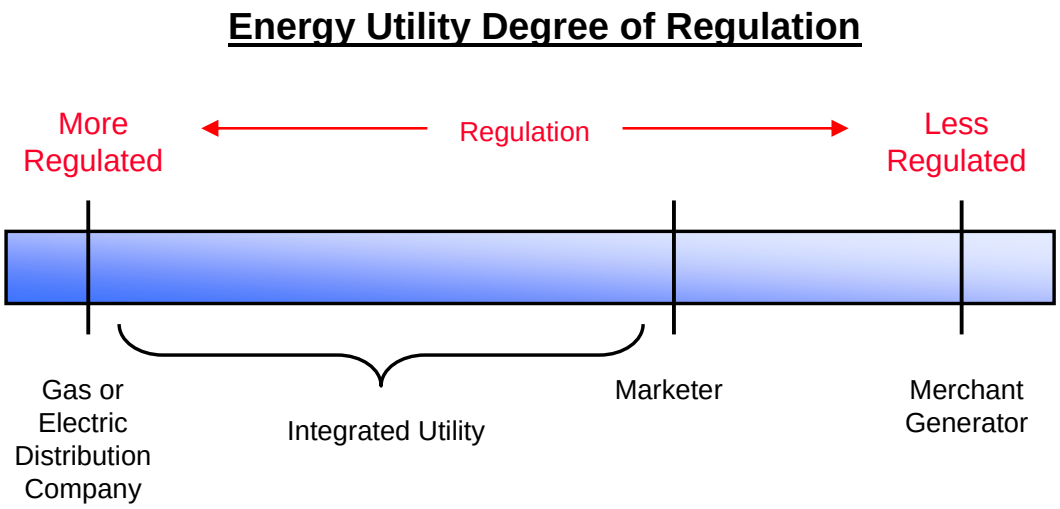
1.3. What is a Utility?

It is important to define an entity that would be considered a 'utility' to focus on the unique nature of the risks faced by such a company. For the purpose of this paper, a utility is defined as an entity that has rates that must be approved by a regulatory authority, be it local, state, regional or federal (including public power's self-regulating governance), and tends to have extensive exposure to operative risks. Further, this paper focuses only on energy-related utilities that offer products or services to the power and gas sectors. Before proceeding, the various energy-related types of utilities considered in the paper are defined below.

- **Distribution Company** – an independent owner of either gas or electricity distribution infrastructure with the responsibility of delivering the commodity on demand to the end user from the customer's commodity supplier.
- **Transmission or Transport Company** – an independent transmission or pipeline owner that sells transmission or transport capacity and related services.
- **Integrated Utility** – an entity with the obligation to provide full service to some or all end-users in a pre-determined service territory using a specified portfolio of assets and related infrastructure.
- **Provider of Last Resort** – an entity with the obligation to provide full service at a specified rate for any customer in a pre-defined service territory at the customer's discretion.

While it is true that in a sense all companies report to, or are overseen by a regulatory authority because all companies operate under various laws, this paper focuses on companies that interact with an energy-related regulatory authority. In considering risks facing these utilities, it is important to understand the degree to which these companies are regulated relative to other entities in the energy sector. Specifically, a regulated company operates in an environment in which its rates and effects of decisions are reviewed and approved by a regulatory authority, which affects the company's operations, investments, and management practices. Ultimately a regulated utility's returns and thus earnings are highly dependent upon the regulatory authority governing their rates and prudence of operations. Non-regulated companies, while still having regulatory oversight from the FERC to mitigate market power issues, rarely have their returns governed by a regulatory authority. However, regulated companies may also have a non-regulated business unit whose returns may indirectly be affected by regulation. The extent to which companies are regulated can be seen in Figure 1.2 below.

Figure 1.2: Energy Utility Degree of Regulation



1.4. Who Should Implement ERM?

The business structure and size of a company should not drive whether or not an entity employs ERM principles, but rather should determine the extent and complexity of such a framework. An ERM framework can be applied by an entire company or by a subsidiary. Even a small cooperative or distribution company can find benefit in implementing aspects of ERM, but should scale the efforts to the extent of the risks faced by the organization and risk management capabilities of the firm. An ERM framework may result in extensive governance, policies, tracking systems and processes for a company with a large, diverse portfolio, while a small company may have simple reports and policies that are more in proportion to their organization's size and complexity. For both entities, an ERM framework will improve risk management and decision making and could be critical to the financial and operational stability of the company.

2. ERM Framework for Utilities

The environment in which electric utilities operate today is very dynamic as the type, scope and frequency of risks faced by utilities have increased dramatically. Constant changes in regulations, technologies, and market structure coupled with increasing production costs, regulatory scrutiny, and commodity price volatility are just a few of the issues presenting significant risk to utilities. Although many of today's utilities participate in traded commodities markets, and thus must implement common risk management processes, increasingly conservative and standardized practices have made the risks in these areas relatively small when compared to other risks faced by the regulated utility.

The practice of ERM for these entities is unique due primarily to the additional complexities utility firms face, such as extensive and diverse physical infrastructures, regional as well as national regulatory authorities, and shareholder or stakeholder perceptions of risk appetite. Specifically, utilities must balance issues such as system reliability, public and employee safety, customer rate stability, generation costs, environmental compliance and stakeholder expectations with volatile commodity markets, regulatory retrospection, ageing infrastructure and changing market rules. More and more often this balancing act is front page news. As the industry recovers from the aftermath of the Enron debacle and increased energy prices, utilities must now also manage these risks and a public image with their regulators, communities, rating agencies, and customers.

2.1. Benefits of ERM

An ERM framework is a holistic approach to the assessment and effective management of a company's entire risk profile. Such a framework can facilitate the identification and assessment of the collective risks affecting a utility and generate company-wide risk management solutions. An ERM framework is a process, not an end result, which views an organization's cumulative risks from a broader perspective than traditional, risk-by-risk assessments and mitigation strategies. That is, a successful ERM framework adopts a portfolio approach to risk, looking at market, credit, operative and business risk issues, as well as their interaction, on a company-wide basis. The end result is a unified perspective of risk and the establishment of a risk-aware culture across the entire company. Additionally, ERM enhances the decision making and planning of a company's management as they better understand the risks of their decisions. Further, an ERM program assuages stakeholder concerns regarding the prudence of management decisions and risk management practices of the firm. Specifically, ERM addresses stakeholder concerns and aids management because it:

- Creates a disciplined and consistent method to identify, communicate and manage risk;
- Establishes a clear link between strategic business plans and key risks;
- Aligns risk tolerance from Board through Management to Staff levels;
- Creates integrated and coordinated approaches to managing risk across all business units;
- Fulfills lender and credit rating agency requirements;

- Efficiently allocates spending capital
- Addresses higher Board and Officer risk management expectations;
- Promotes a risk awareness and management culture
- Enhances the external view and reputation of the entity; and
- Leads to better and more informed decision making.

The key benefits of an ERM framework include improved internal processes, knowledge, governance, controls and communication, and enhanced stakeholder relations. ERM improvement in internal processes and infrastructure result in an integrated and cross-corporate view of risk, standardized language, metrics and tools, and enhanced transparency in reporting and controls. Improved corporate governance through consistent and well established guidelines is another outcome of a well implemented ERM framework. ERM practices lead to establishing an overall corporate risk policy that then drives the governance, policies and controls of individual businesses. With a clearly articulated risk appetite, tolerance and controls, all management has clear guidance on the parameters they must consider in making decisions. The increased clarity and resulting consistency in business decisions sends important signals, both internally and externally, about the firm's strategy and risk management approach.

For the Board of Directors, an ERM framework assures that appropriate policies are in place to identify and manage key risks and that there are processes in place to identify and communicate key risks to management. The Board must ultimately be comfortable that they are aware of the key risks facing the organization, their potential impact on performance, and the mitigating controls and contingencies. An ERM framework directly enhances the transparency, completeness and consistency in reporting to the Board and keeps the Board informed of the total levels and categories of risks being faced.

A well established and consistent message regarding risk management also allows for the utility to demonstrate how all business decisions with an impact on rates, such as O&M and capital expenditures, were prudent given the utility's risk profile. If utilities communicate expectations regarding risk appetite and tolerance, then regulators may be more inclined to agree with expenditures utilities make that are consistent with the agreed-to risk profile.

A focused and well-implemented ERM framework can also assist in both operating and capital budgeting by providing another basis for allocating resources, reducing expenditures on immaterial risks, and exploiting natural hedges and portfolio effects. Under an ERM framework, all capital expenditures are scrutinized equally to include a review of risks, an assessment of the impact on the portfolio and a comparison to alternatives.

As a result, a utility's capital expenditures and allocation are improved through the use of processes that take into account the benefit of risk reduction in all major risk categories (that is, regulatory, financial, reliability, safety, environmental, reputation, and so on) by allocating capital expenditures with consideration of the optimum risk adjusted return on investment consistent with the company's risk appetite. While the system can be complex, the result is a capital allocation process that is much more likely to lead the utility toward the optimal portfolio of capital projects.

ERM is a key tool in understanding risk exposure from a portfolio viewpoint and assessing the financial strength of the company. Financial strength is determined by the company's ability to create economic value for its stakeholders while meeting its financial liquidity demands. This concept is known as capital adequacy. From an economic value perspective capital adequacy is measured by assessing the company's equity against their risk exposure to determine the level of equity surplus or shortfall. From a financial liquidity perspective, capital adequacy is measured by the company's ability to meet demands for cash as they become due. Both economic value and financial liquidity determinations involve quantifying risk exposure where feasible. This enhanced understanding allows for an improved financial management process that focuses not only on the individual risk exposures and the ability of the company's equity structure and forecasted cash flows to cover such exposures, but also on the overall diversification effect of the portfolio of the company creating natural hedges to offset exposure. A risk-based approach to capital adequacy is becoming paramount for utilities as rating agencies are reviewing and considering a company's ERM practices in the determination of a company's credit rating. [3]

Finally, an ERM framework conveys a certain level of risk management sophistication to external parties such as rating agencies and regulators. Communication of the types and extent of risks taken on in the normal course of business provides evidence that the critical risks impacting earnings or cash flow are being addressed and can improve the reputation of the management team and the company. These internal enhancements then lead to increased stakeholder confidence as they recognize that the risk culture permeates through every decision made by the executives, and counterparties, investors and lenders understand the total risk of the portfolio, lowering costs related to credit. Specifically, ERM builds stakeholder confidence by establishing processes to stabilize earnings and costs, and demonstrating proactive risk stewardship.

In summary, an ERM framework:

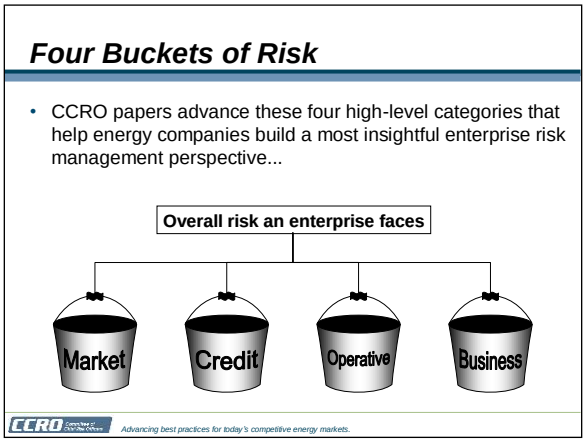
- Improves understanding of the risks that impact the enterprise and how these may be manifested;
- Encourages employees to integrate risk management into their normal activities;
- Demonstrates risk management performance to stakeholders;
- Enhances confidence that the risk profile is understood and being monitored in accordance with the enterprise's risk management plan; and
- Focuses management attention on key risks.

2.2. Appreciating the Value of Best Practice Risk Categorizations

Every Utility, Merchant, Producer – any firm for that matter - is subject to the same multitude of specific risks. However, depending on the specifics of its business, each firm is affected by each of these risks to a different degree. Thus, each firm is said to have a unique "risk profile". The firm's risk function must at some point consider how to best group or categorize this multitude

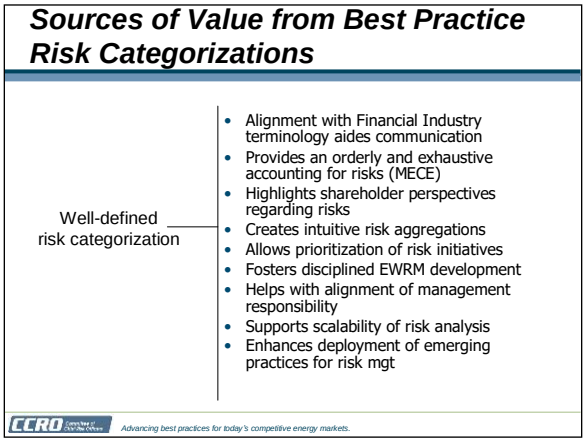
[3] For more information on capital adequacy, please see the CCRO's previously released paper Emerging Practices for Assessing Capital Adequacy, September 17, 2003 and the current release Capital Adequacy Extension, May 2007.

of risks. It must do so in order to create clear and cohesive analyses of its risk profile, and to make proposals to effectively address risks according to management needs.
Unfortunately, a utility may find itself with inconsistent categories that have simply evolved over the years. Upon close inspection, double-counting may be common, or large gaps may be left from an incomplete categorization system that leaves significant exposures overlooked. Some ways of categorizing risks may be "home grown" and suffer from little buy-in from outsiders that challenge the firm's understanding of its own risks.
In any case, the categorization system chosen by a firm as its standard, are critical to the effectiveness of its risk management program. This section highlights a wealth of past work of the CCRO and its member companies towards developing the most insightful risk categorizations which are today accepted as best practice in the energy industry. Utilities and other energy companies should be aware that adopting these categories for risk is an essential building block towards the most effective risk management function.



Though often not recognized as such a critical decision, companies should know that real value can be captured through the astute application of the four risk categories shown at right. Sometimes referred to as four "buckets" of risk, these four categories are used by the leaders in energy risk management today for good reason.
The four categories represent the highest level in a system of categorization for risks that utilities, merchants, producers & generators – for that matter – any firm faces to varying degrees.

Why have these four buckets of risk so soundly become "best practice"? Answer- because their use brings a substantial list of benefits and advantages. These benefits include those shown as sources of value in the slide at right. These advantages are now well proven by those many energy companies with risk programs in place which utilize this system of categorization. To promote the use of these risk categorizations by energy companies, this section elaborates on a number of these advantages.



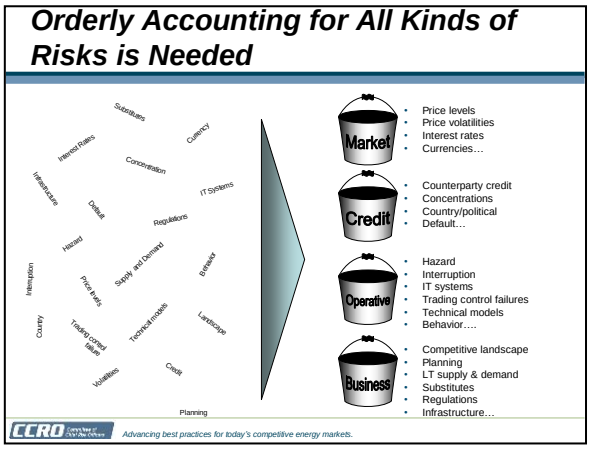
Alignment with the Financial Industry

These four categories or "buckets" are based on those originally developed in a "Corporate Metrics" paper provided as best practice to the financial industry by JP Morgan in 1999. Using that baseline from the financial industry, the CCRO has helped energy companies advance risk practices by further engineering the categories to accommodate the ways the energy industry is unlike the financial industry and its markets. The resulting combination of suitability for energy companies with familiarity for those in the financial industry smoothes the process of delivering

insights and gaining buy-in from key stakeholders outside the company. This alignment is unquestionably an advantage for the utility that is trying to communicate the insights it has gained from its risk management function. Outside stakeholders such as investment banks, regulators, or rating agencies often have built their risk management expertise from their experience in the financial industry and the use of familiar risk categorizations is a distinct advantage.

An orderly and exhaustive accounting for risks

Even in the early stages of building an enterprise risk management framework, risk managers become increasingly aware of the diversity of risks at hand. Any energy company that makes an honest attempt to tally its risks finds a daunting spectrum of exposures which seriously challenge attempts to grasp the big picture. However, with an orderly accounting of these many risks, managers can begin to see a sensible way forward. Risk categorizations are the foundation to this orderly accounting.



An effective ERM framework must be built on a risk accounting (or taxonomy) that can be called mutually exclusive and collectively exhaustive, or "MECE". The four risk categories – Market, Credit, Operative, and Business – support MECE risk accounting at least to the greatest extent practicable.

Attention to "mutual exclusivity" (the 'ME' in MECE) seeks to avoid double-counting. Inter-relationships between risks are carefully assessed, and underlying drivers of any particular risk must be understood. In this way, models and subsequent analyses are attentive to the many influences that one risk may have on another and are designed to acknowledge them.

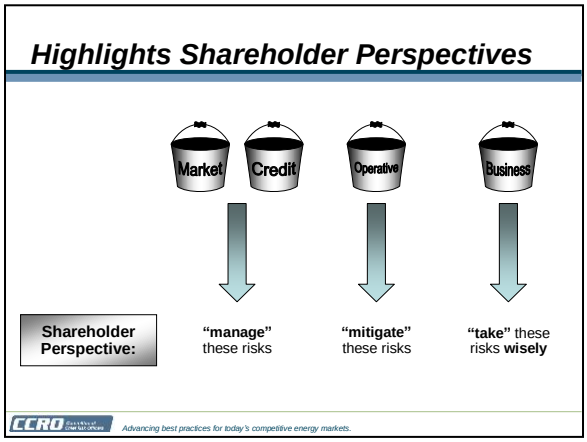
"Collectively exhaustive" (the 'CE' in MECE) means that no risks are missed. The risk taxonomy should not intentionally nor unintentionally exclude any sources of risk. Otherwise, model or assessment results are sure to provide incomplete messages which could prove to be costly errors. Furthermore, insights presented may fall apart when challenged if specific risks are excluded without robust explanation for their absence. The CCRO has available an exhaustive taxonomy, listing many detailed risks and where they fall into the four broad categories.

It is true that in reality, few occasions of pure 'MECE-ness' are found. Nevertheless, attention to the MECE rule brings light to any interrelationships that need to be understood and will help management avoid having critical gaps in its analyses.

Highlights stakeholder perspectives on risk

The four categories for risk are also helpful to the risk manager proposing actions to address the risks measured. Actions that are arguably well aligned with stakeholder perspectives on risk are

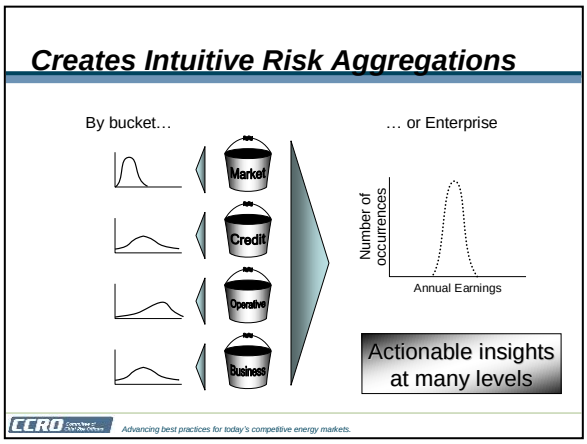
certainly preferred. In the case of an unregulated merchant, stakeholders may be shareholders. In the case of a utility, stakeholders may be ratepayers or regulators.



Typical stakeholder perspective on market & credit risks is that they are "managed". This means that they are risks to be taken to some degree to generate a financial return but they must be kept within tolerable limits. The perspective on operative risks is that they are usually to be "mitigated". This means they are targeted for removal through any number of tools ranging from policies & procedures to insurance. Perspective on business risks is that they are often necessarily "taken". This means they are inherent to the business at hand yet must be taken judiciously without ignorance, thereby avoiding what can be a rich source of bad surprises.

Clearly, using these four risk categories eases alignment of risk measurements and sensible actions to be considered to address those risks. This is very helpful for the risk manager when having a dialog about controls, hedging, capital investments, and other risk related topics with the board of directors or other senior management.

Creates Intuitive Risk Aggregations

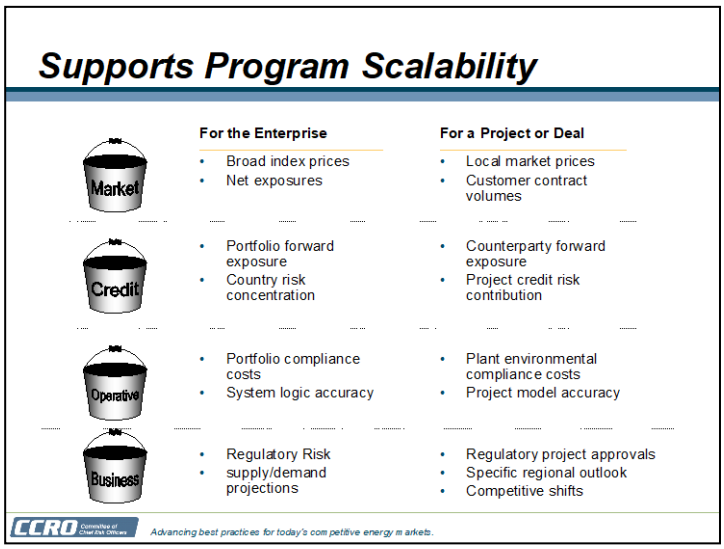


Because risk measurement and assessment approaches and associated tools have come such a long way in the last five years (and will no doubt continue to do so), it is important to be positioned to take advantage of them within your enterprise risk framework. Risk categorizations that are not in line with best practices may cause overlaps or inconsistencies across categories and prevent accurate use of these valuable emerging models. Today, market and credit risks can be measured using a wealth of software tools available that create important measures regarding each individually. Operative risk has become the focus of much work in the financial and energy industry in recent years. In this paper and others, the CCRO has been addressing operative risk for energy companies, especially as a primary component of risk for energy asset operators. The business risk category also is now under study by the CCRO, specifically in terms of how to bring assessment or possible measurements to bear. Through the astute use of the best measurement tools, each of the four buckets can bring powerful insights into the potential impact of risk on company health and performance.

However, the greatest challenge may be to create an overall picture of the enterprise and its risk. Much of the challenge comes from difficulty in robust aggregation of all risk categories. The CCRO has done much work to address this challenge in its best practice framework for capital

adequacy[4] which presents several methodologies to aggregate an enterprise view of risk. The four-categories for risk underlie this capital adequacy framework. To take advantage of this methodology then, a company needs to adopt these four best practice categories for risks.

Supports a Scalable Framework for Risk



Another advantage from these risk categorizations is that the framework for risk analysis becomes entirely scalable. Scalable means that the language, metrics, assessments, and modeling approaches are much the same regardless whether studying the entire enterprise or a single project/deal. The impact of risk on a project can evaluated and explained using the same framework as the risk analyses supporting the overall corporate business plan. Similar metrics and approaches are used regardless whether the audience is the board of directors, risk committee, or business unit. Consequently, the cost-effectiveness of models and the communication of risk management insights are much improved. Obviously, scalability is a big advantage for the risk function that seeks to have impact at many levels and create value for the firm.

Helps with deployment of emerging practices for risk management

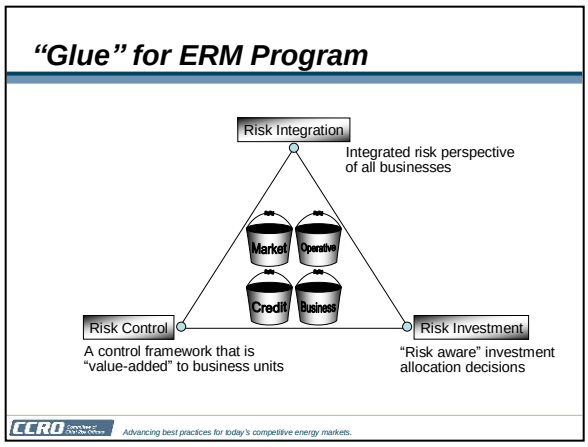
As the CCRO continues its on-going work uncovering, developing, and publishing best and emerging practices for all aspects of risk management, the four-bucket categorization system is underlying. Utilities and other firms that wish to advance their risk management capabilities are always striving to achieve best practices. Therefore, to put itself in a good position to be able to take advantage of new practices as they emerge, the utility is advised to widely adopt these best practice risk categories. Whether concerning organizational, control design, risk metric, or reporting issues, these categorizations are an important foundation supporting compliance with best practices now and in the future.

The "Glue" for an enterprise risk management program

The desirable characteristics of an enterprise risk management (ERM) program that is based on these risk categorizations has also furthered their adoption as best practice across the industry.

[4] See CCRO Papers "Emerging Practices for Capital Adequacy" and Capital Adequacy Extension.

The four categories provide consistency, MECE-ness, and fit across the spectrum of issues that an ERM program must tackle. Whether considering metric, governance, organizational, or reporting issues, all are aided by using a single set of risk categorizations and associated terminology. As if a glue were created by this categorization system, the insights presented by the ERM analysis and proposals hold-together well when challenged or studied. As diverse and complex as many projects undertaken by an ERM function in a utility may be, this risk categorization system is essential to clear and cohesive analysis.



2.3. The Utility Risk Environment

To advance all the previously mentioned benefits of best practice risk categorizations for utilities, this paper has adopted the CCRO's "four bucket" risk categorization system.

The table below lists several risks a utility should consider when addressing their risk profile, and notes the appropriate category. This list should not be considered complete and applicable to every company, but rather a general guideline of areas to be considered when evaluating the risks associated with a regulated utility. In addition, many of these areas should be subdivided into critical components in order to gain more detail in identifying areas of concern.

Figure 2.1: Risk Categories

Risk	Utility Application				Risk Category			
	Distrib. Co	Trans. Co	Integrated Utility	Provider of Last Resort	Market	Credit	Operative	Business
Asset Conditions	✓	✓	✓	✓	✓	✓	✓	✓
Audits	✓	✓	✓	✓	✓	✓	✓	✓
Business Continuity	✓	✓	✓	✓			✓	
Commercial Operations Performance			✓	✓			✓	
Compliance	✓	✓	✓	✓				✓
Construction	✓	✓	✓	✓				✓
Corporate Security, Physical	✓	✓	✓	✓			✓	✓
Corporate Security, Cyber	✓	✓	✓	✓			✓	✓
Credit	✓	✓	✓	✓		✓		
Distribution	✓		✓	✓			✓	
Environmental	✓	✓	✓	✓			✓	✓
Fuel Supply	✓		✓	✓			✓	✓
Generation Operations Performance			✓	✓	✓		✓	
Growth	✓	✓	✓	✓		✓	✓	✓
Technology	✓	✓	✓	✓			✓	
Interest	✓	✓	✓	✓		✓		✓
Liquidity	✓		✓	✓				✓
Organizational Readiness	✓	✓	✓	✓		✓	✓	✓
Production Cost Performance	✓	✓			✓	✓	✓	✓
Regulatory	✓	✓	✓	✓				✓
Reputation	✓	✓	✓	✓		✓	✓	✓
Retail Customer Exposure	✓		✓	✓		✓		✓
Safety	✓	✓	✓	✓			✓	
Staffing/Workforce Development	✓	✓	✓	✓			✓	✓
Trading		✓	✓	✓	✓	✓		
Transmission or Transport		✓	✓	✓		✓	✓	✓
Wholesale Customer Exposure		✓	✓	✓		✓		✓

2.3.1. Market Risk

All energy companies are concerned with changes in commodity prices, and utilities are no different. Utilities with retail load serving obligations typically have pre-set rates established in a regulatory forum based on expected costs of commodities over the applicable term of the rates. These load serving entities must then serve load at that fixed rate. That is, they must manage the volume variability in customer loads caused by weather, changes in customer usage patterns, and economic conditions.

In some cases, utilities have regulatory mechanisms to capture the variances in commodity costs and loads from the expected levels. Such mechanisms are designed to minimize a utility's price risks associated with fuel or the actual commodity they are delivering (electricity or natural gas). Companies with pass-through cost mechanisms are often thought to have lower market risk since there is an opportunity to recover these costs, and risk to their margins is limited to variability in revenues caused by variance in load from expectations. However, these companies may face either regulatory hindsight to recover these costs, or find that recovery mechanisms don't match the costs incurred for both the commodity and the carrying costs. For instance, depending on the timing of cost recovery mechanisms, a utility can experience cash flow lags and liquidity problems. For this reason, utilities with fuel or supply cost adjustment mechanisms must still implement sound risk management practices to maximize recovery of these costs and ensure enough liquidity to support delays in cost recovery. In addition, utilities may not be allowed to keep the benefits realized from achieving lower than expected commodity costs.

There are some utilities that do not have these fuel or cost adjustment mechanisms in place. Rates for those entities are pre-determined based on forecasts of both commodity prices and customer usage. Basically the revenue requirements for providing full service to customers incorporate these assumptions in the overall estimate of rates during rate case proceedings. These utilities must manage supply and fuel commodity prices relative to these fixed rates, presenting a conflict between regulatory recovery and hedging. That is, the revenue requirement agreed to in a rate case may only occasionally include these costs of hedges. However, variances from the forecasted fuel prices for example, may be included in the next rate case as part of a true-up mechanism.

Not only is the management of commodity prices critical, but also the hedging of volumetric risk can be paramount for entities without fuel or cost recovery mechanisms. Unfortunately, these risks can be significant as the deviations in usage are typically correlated to changes in market prices. In most cases, energy prices tend to move with energy usage, so as a customer uses more energy than expected at a fixed price, the cost to serve that load increase is generally higher as well. The market risk management practices of integrated utilities mirror those of most energy trading companies, meaning they must actively manage commodity and volumetric risks. An integrated utility, however, may benefit from higher commodity prices by making sales to off-system customers, provided the regulators allow the utility to retain all or a portion of the benefits.

In addition to the aforementioned market risks, utilities face risks related to exchange rates and interest rates, as well as commodity prices associated with operations, such as copper, steel and cement.

Historically, exchange rate risk has typically only been applicable to those utilities with service territories in different countries. This risk was fairly easily managed on its own but could become complicated by both commodity and volumetric risks, where the actual earnings to be hedged can vary significantly. However, with a growing international market for fuels, for instance uranium, or equipment, such as those relating to generating facilities or substations, many utilities are facing exchange rate risk for the first time. Exchange rate risks can become a problem for utilities when the US dollar is weak, increasing the competitive advantage of international purchasers with more buying power, as these commodities are traded in the US dollar. In effect, the price of the commodity increases as the US dollar weakens, thus the relative cost of the commodity is greater for US firms. Hedging this exchange rate risk is also very complicated because it requires forecasts of the requirements for these commodities to enable implementation of hedges, and then the recovery of these hedge costs may not be allowed.

Interest rate risk, which is the risk associated with the reduction in the value or cost of a security, good or service resulting from a rise in interest rates, can also have a major impact on utilities for two reasons. First, most utilities are required to set rates in advance of actual expenditures based on expected costs. If there is a change in costs, the company is either required to absorb the incremental cost or, at best, recover the cost at a later date, bearing short-term carrying costs of the expenditure. Second, any utility making capital investments is required to seek financing for funds used during construction and for the actual capital expenditure for an asset. In such an instance, the investor-owned utility faces the market interest rate for its credit level, but then receives an allowed rate of return on that asset. This rate of return is based on a regulatory determination of the fair and equitable value of the asset and associated risk the shareholder is taking on behalf of the ratepayer. These calculations can frequently differ, creating the risk that the investment is less cost effective relative to an industry-allowed weighted cost of capital, thereby lowering the return to the utility.

Finally, utilities that are required to maintain, improve or expand infrastructure face the costs of commodities associated with construction. The price of steel and concrete impact the construction of generation facilities as well as gas storage and pipeline infrastructure, while steel and copper costs most dramatically impact transmission assets. As these commodities become more volatile, utilities must manage these expenses because they are obligated to build or maintain their assets at a cost approved in a rate hearing, or face the regulatory burden of proof known as "prudency" to recover actual costs.

2.3.2. Credit Risk

Utilities face various credit risks in their daily operation. When a customer's credit falls into arrears, utilities do not receive the variable cost of the delivered product that stands unpaid or the recovery of fixed costs, which leads to a lower than expected rate of return on rate base. Should utility suppliers realize unexpected changes in their credit, they could also run the risk of default of financial obligations. That is, if utilities hold large positions with credit-challenged suppliers, those suppliers could in turn impact a utility's credit rating.

Further threatening a utility's financial stability is the credit health of parties in the region or industry. If poor, the availability of qualified suppliers may be limited, which could potentially lead to concentration risk, where too much of a utility's supply is dependent upon a small number

of counterparties. Also, if suppliers default, their inability or unwillingness to meet contractual obligations forces utilities to procure required energy, for example, at market rates which may be higher than those originally contracted.

Finally, a downgrade of a utility's credit rating can result in a problem that's twofold: firstly, customers will have to pay a higher premium to offset a supplier's risk of serving a customer with poor credit. Secondly, a utility with poor credit will find a limited number of suppliers willing to do business with them, exacerbating concentration risk.

There is also the threat of regulatory or legislative risk, which can be a particular problem for utilities from a credit perspective. This includes any adverse political actions that threaten an organization's resources and future cash flows and can bring a utility to the brink of bankruptcy to protect them from excessive costs they cannot recover. If a regulatory authority requires a utility to absorb costs they did not anticipate, disallows costs they thought they would recover, or defers the collection of costs to a future date, with the potential of having those costs disallowed, the costs could impact the utility's credit rating. Rating agencies are concerned utilities may not be able to collect the costs of doing business while they are required to provide ongoing service, thus becoming more stringent in their ratings of these companies.

2.3.3. Operative Risk

Operative risk includes all risks related to a utility's operations. This risk category has been further divided into Operations risk and Operational risk. Operations risk is any risk associated with the failure or constraint of a physical asset. Operational risk includes risks related to inadequate or failed internal processes, people, and systems. Both are discussed in more detail below.

Operations Risk

Operations risk is associated with a failure or constraint of a physical asset. This is a major issue for utilities, especially vertically integrated utilities with transmission infrastructure, distribution systems and a generation fleet to operate and maintain.

All utilities have some delivery requirement. The extent to which the company bears the risk of that delivery, however, varies with their regulated obligation. If a utility is only a load serving entity where all customers are required to procure their own supplies, then the utility's obligation is to maintain the delivery system such that the energy that is delivered to the appropriate interconnection or City Gate is in turn delivered to the customer.

Some electric utilities are responsible for maintaining transmission reliability because they are control area operators. Their operations risks are significant because they become the supplier of last resort. In the event suppliers do not supply adequate power to the grid, the control area operator must maintain the system reliability by either purchasing or generating the incremental energy needed. Although there are mechanisms in place to financially settle situations where a supplier could fail to perform, occasionally those mechanisms are not linked to the actual costs of these damages. Furthermore, the control area operator is responsible for security and safety

of systems so that in the event of a specific attack on the system, the transmission operator will repair and restore service as soon as possible.

Transmission operators, and subsequently control area operators, are regulated by both the FERC and their regional energy reliability councils. FERC is responsible for regulating market practices that include the rates that can be charged for the various control area services, which are known as ancillary services. The NERC regions are responsible for setting the guidelines by which these systems must operate, and the related fines and penalties for their failure to comply. On the operations side, if a utility does not operate their control area efficiently and economically, they will not earn an adequate rate of return, while at the same time could also face penalties for inappropriate operations.

Finally, there are operational risks associated with utilities that own and operate generation assets. For most of these utilities, the costs to run these plants are embedded in their revenue requirements. If forced outages or variable and fixed O&M costs are more than expected, the company may not earn its allowed rate of return. Some regulatory authorities incentivize utilities to operate their plants efficiently through rate mechanisms known as Incentive Rate making, where cost savings are shared between ratepayers and utilities. Unfortunately, not all utilities have this option, which places those who don't in the unenviable position of having to pass on any costs savings to the customer while at the same time absorbing cost overruns. Some regulators allow for recovery of catastrophic failure of assets, but only if the utility can prove in hindsight that all operations were executed within industry best practices and that the most effective remediation options were employed. This paradigm requires utilities to be diligent about operations while they optimize margin.

Operational Risk

Operational risks are associated with inadequate or failed internal processes, people, and systems. Ultimately a utility is responsible for hedging all risks on customers' behalf by exercising best practices for supply management, asset operation and risk mitigation to maintain a reliable and low cost supply of energy. As such, a measure of a utility's competency at anticipating these risks is an effective hedging strategy.

Without pass-through options, a utility is driven to hedge against possible extreme cases. A good operational risk strategy is regulatory recovery, whereby a partnership between a utility and their regulatory authority allows for ways to mitigate risks and options to recoup costs should they materialize. If, for example, processes and procedures are not followed, investments are poorly made, supporting information is not collected, or individuals overlook tasks assigned, the costs incurred may be disallowed. The possibility exists that a utility's costs could far exceed their expectations, leading to increased scrutiny on the part of the regulators.

Adding to this concern is a utility's need to address safety risk. Utilities operate in an environment that plays host to a critical network of generation, transmission and distribution systems, where a temporary lapse of employee attention can have catastrophic implications for the employees as well as individuals and the infrastructure within the surrounding community.

Other risks that may be disallowed include fraud risk, an intentional act that results in a material misstatement in the financial statements, information processing and technology risk, or using information technologies that could expose the organization's ability to sustain the operation of critical processes. Finally, modeling or forecasting risk is the failure to properly measure or forecast results where data is not observable. Most regulators will deem the utility the best estimator of their forecasted loads, supply costs and other revenue requirement components, and may or may not allow cost recovery because they missed their forecast.

2.3.4.Business Risk

Today, the dominant business risks for utilities are regulatory and environmental risks. Changing regulations complicate the organization's capacity to efficiently conduct business and changing environmental legislation may require significant investments to keep assets operating. In today's dynamic marketplace, it is difficult to know how the market rules will change as regulators and legislatures respond to a changing business environment and occasionally, market crises. With uncertain futures, utilities find it hard to know when and how much to invest, and lenders are leery of loaning to these entities without knowing the revenue streams guaranteed by regulation will come to fruition.

In the 1980's and 90's, many utilities faced stranded costs as legislators moved the gas market and numerous power markets to deregulation. Now many of these legislators are reviewing the merits of re-regulation, or changing back to the rules of the regulated markets. Rating agencies are eyeing these changes with caution and some utilities are facing credit downgrades. This situation highlights the need for utilities to manage regulatory risk effectively as a holistic approach to risk management.

Regulatory risk magnifies two additional business risks for utilities; capital availability and reputational risk. First, the risk of the lack of capital availability or sufficient access to capital threatens the organization's ability to execute its strategies and meet its mandated service requirements. As utilities become less vertically integrated, they become more vulnerable to market fluctuations and changing market rules. As a result, credit ratings can suffer, which will make capital more expensive. These risks can then limit the ability of a utility to maintain and improve their infrastructure. Second, risk to image or reputation could lead utilities to lose customers, investors, or suffer adverse regulatory or legislative decisions that could further cripple their ability to perform their responsibilities and meet customers, shareholder and stakeholder expectations.

Another business risk that has become a more significant issue for utilities in the last ten years is environmental risk. With concern over global warming and excessive emissions, both national and regional legislation are increasing costs for utilities, some of which may not be recoverable. For utility generators, this legislation is requiring extensive capital expenditures to retrofit existing power plants to lower emissions, or forcing them to pay the cost of emissions 'credits' to offset the physical discharge. Uncertainty about potential future legislation adds another layer of complexity to this issue. Additionally, some legislators are now requiring investment in renewable energy, which can be much more costly than conventional generation and can create operations problems. These requirements are for the longer term, forcing utilities that serve load, to either enter into long term (more than ten year) renewable contracts, or to invest in the

renewable plants themselves. These investments are increasing costs and at the same time affording legislators and regulators the ability to exercise retrospection regarding the prudence of these costly investments.

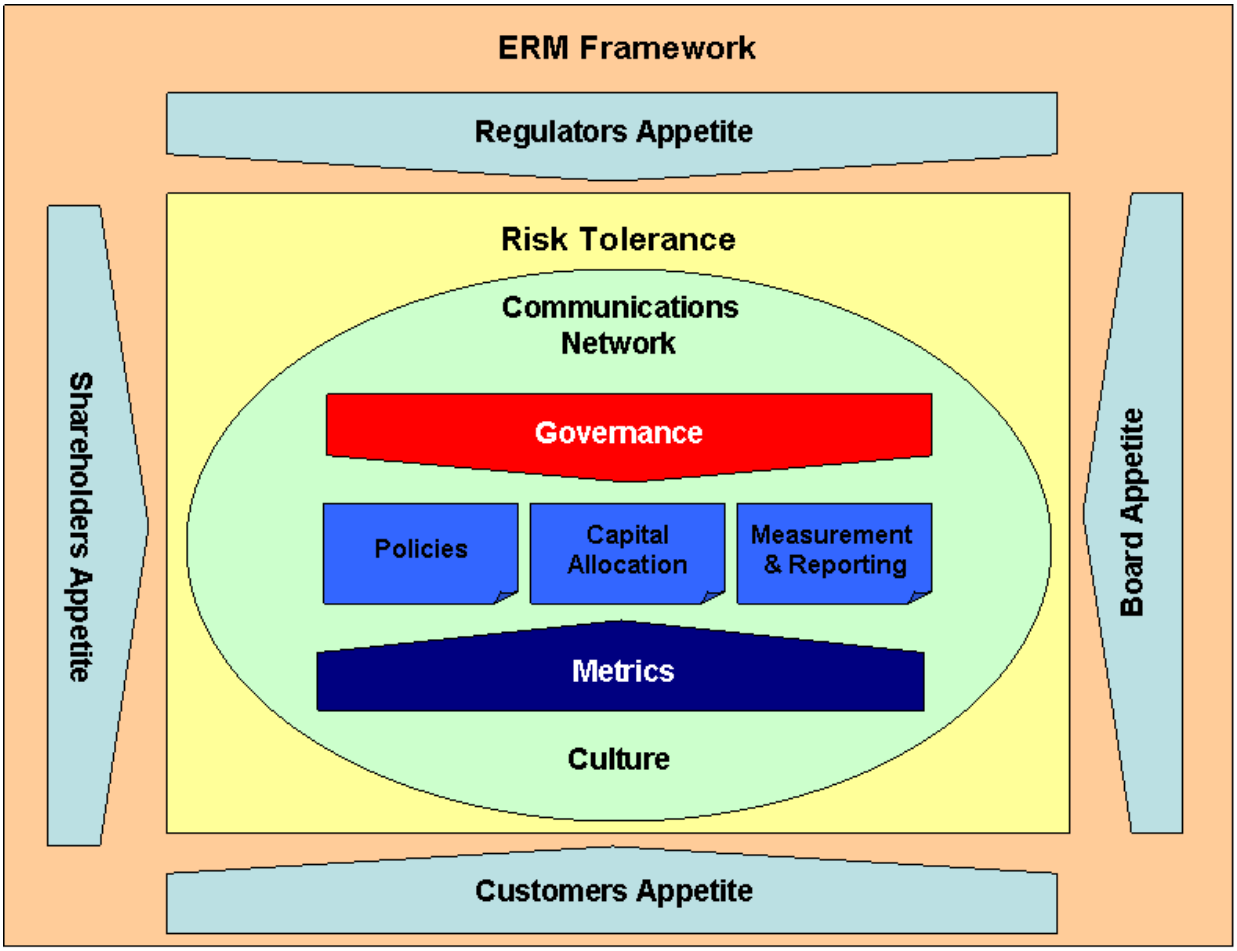
Finally, many utilities are also facing the same risks many industries are facing; an aging workforce. The knowledge and experience needed to effectively operate a gas or power system is significant, and as more of the workforce retires, the availability of skilled and experienced workers to backfill the void is a growing concern. Partly due to image and partly due to the changing complexion of the workforce, few young workers are looking to the utility industry as a career choice, be it in operations or in the corporate center. This lack of new talent, coupled with an aging workforce, threatens the success of critical business activities.

2.4. The Scope of the Framework

The general structure of the ERM framework is shown in Figure 2.2. As this diagram demonstrates, the complexity of each component is not emphasized. Rather, it establishes that, when implementing an ERM framework, it should have the components noted, but the sophistication of these components should depend on the complexity of the firm's portfolio and the available risk management resources. The key components that must be included for a successful ERM framework are:

- Identification of Risk Appetite,
- Definition of Risk Tolerance,
- Development of a Risk Awareness Culture,
- Establishment of Corporate Governance,
- Definition of Risk Metrics,
- Creation of Risk policies,
- Establishment of a Capital Allocation process, and
- Implementation of measurement and reporting consistent with the metrics, governance, and strategy.

Figure 2.2: ERM Framework



2.4.1. Risk Appetite

When a utility adopts ERM, it not only enhances its awareness of the risks inherent in its business, but also focuses the company on determining the risks that are appropriate to accept and those that are not. Determining a utility's risk appetite is a key component of setting and managing expectations of stakeholders with regard to the potential impact of risks incurred and how they will be managed. Risk appetite is defined as how much risk and which risks the stakeholders expect the utility to take. For example, losses associated with currency exchange would most likely not be acceptable to stakeholders of a US-based gas distribution company, but losses due to abnormal weather are, to an extent expected. Risk appetite sets the boundaries to a company's activities and drives the company's risk tolerance as well as governance and risk metrics.

Some utilities tend to address risk appetite informally. However, the application of an ERM framework would force entities to review their risk appetite from the perspective of all stakeholders. It is important to note that risk appetite can be applied at different levels of the firm. For utilities, these may be developed at both regulated and non-regulated units as well as at the corporate level.

2.4.2.Risk Tolerance

The determination of the appropriate risk tolerances is a hallmark of an effective ERM program. Risk tolerance is frequently synonymous with risk metrics in that limits, alerts and mitigation programs are put in place to prevent or detect a breach of a risk tolerance. That is, risk tolerance can be viewed as expectations of acceptable losses executives have defined based on stakeholders' risk appetite. Risk tolerances guide executive management and board decisions toward strategic options that are consistent with its consent to operate which is implicitly and explicitly provided by stakeholders and regulators. In effect, the establishment of risk tolerances should answer the questions regarding the board's understanding of how much a company could lose from all sources of risk in a period of time and whether external stakeholders would be surprised by such losses.

Risk tolerance should be considered separately and applied at multiple levels of the company in different settings against specific metrics. Business strategy decisions will impact the firm's outlook on overall returns, growth targets and risk – and should therefore be tied into any risk tolerance discussion.

2.4.3.Corporate Governance

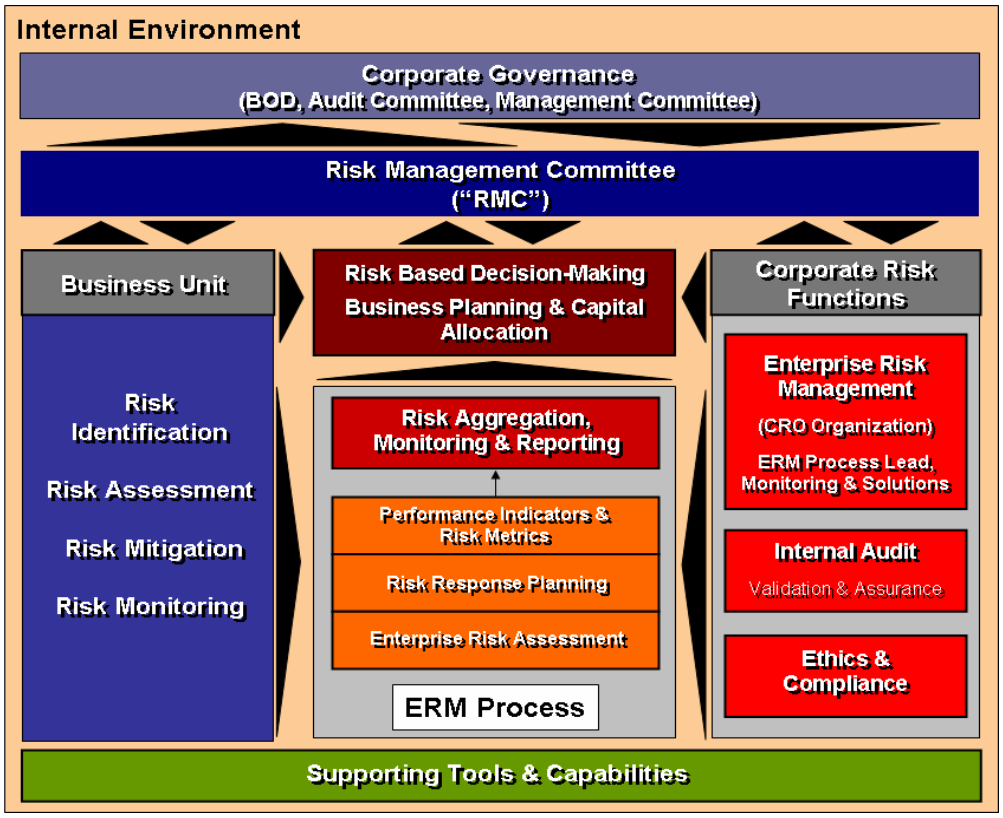
An appropriate governance structure ensures that policies, processes, limits, and enforcement systems are in place to monitor risks across an enterprise, to communicate appropriate risk information through the governance structure, to allow for prevention policies to be enacted, or to detect breaches in risk tolerance. The key to the governance structure is to develop a supportive organizational design that includes clear delegation of authority, well-defined roles and responsibilities, and enforced accountability. Figure 2.3 shows an illustrative governance structure that utilizes several governing committees and outlines key roles that must be addressed in an effective governance structure. While the concepts should be applied, the governance structure should be customized to meet the given organizational structure and needs. The roles and responsibilities must adhere to the strict rules of separations of duties such that parts of the business that are responsible for taking or mitigating risks are not the same as those charged with measuring and reporting the risks.

Additionally, the committees designated should have clear terms of reference, or charters, regarding the level and scope of authority entrusted to them by the Board of Directors or their delegates. The number, scope, composition, and authority of these committees should be highly customized to the individual utility. For example, a large, integrated utility would become overly bureaucratic with a governance structure that mandates that any transaction over $5 million be reviewed by the executive team. On the other hand, a small distribution company may need that level of review for any expenditure over $1 million.

The composition of the committee must be driven by the size and complexity of the utility's portfolio as well as the roles and responsibilities determined by the governance. That is, all review committees should be balanced with respect to the numbers of members from the business units and financial and risk management functions, and should be inclusive of all members who have a role in either managing, taking, mitigating, measuring or reporting the risks. Great care

should be taken to ensure this balance of power to prevent overly cautious or unhindered risk taking behaviors. Further, committees must work to include of all key role players while minimizing overall committee size to prevent excessive bureaucracy.

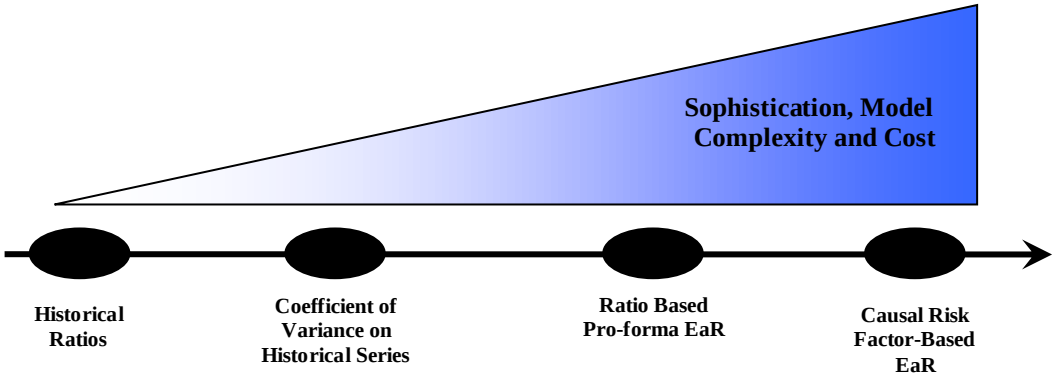
Figure 2.3: Illustrative Risk Governance Structure



2.4.4.Risk Metrics

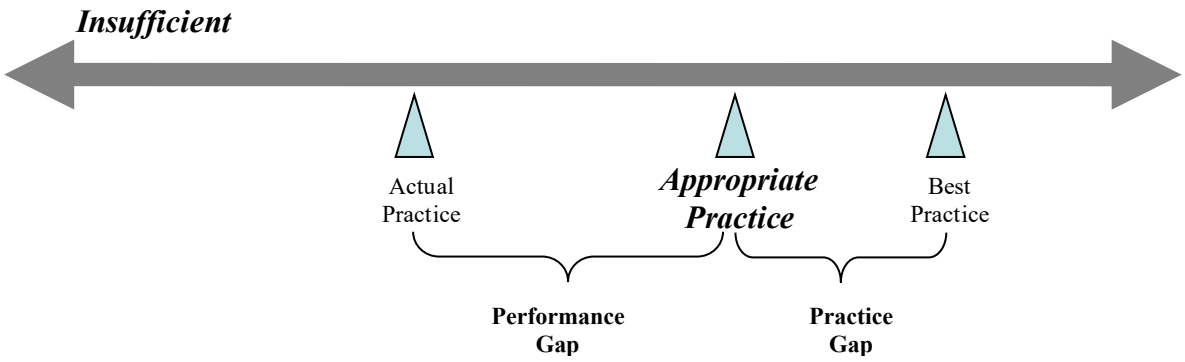
Another key component of the ERM framework is the establishment of risk metrics designed to prevent or detect breaches in the risk tolerance. These risk metrics should also be consistent with the complexity, size and composition of the portfolio. For example, a small electric distribution utility would have a portfolio that consists of primarily operational risks associated with reliable electric power. The type, scope, and number of risk metrics employed in their ERM framework would be much different than those adopted by a vertically integrated utility with gas, nuclear, and coal fueled generation, transmission assets, as well as distribution assets. Nevertheless, the overall goal of implementing any risk metrics is to demonstrate the effect of risk on earnings or costs resulting from a risk event along with the relationship between the various risks monitored. These Earnings-at-Risk (EaR), or at-risk metrics, can ultimately inform management when a risk becomes a significant threat to achieving financial targets as well as providing a baseline to executives as to the extent that any risk can impact earnings and costs. Figure 2.4 below demonstrates the continuum of risk measurement techniques that can be applied to generate an EaR metric.

Figure 2.4: The Continuum of Earnings Risk Measurement Techniques



In addition to EaR based measurements, utilities may benefit from metrics that track, for example, additional capital expenditures, significant safety ramifications, threats to business continuity, and consequences of political or regulatory activities. These metrics can be complex and sophisticated, depending on the magnitude and probability of these risks. As noted in section 1, many utilities may be tempted to strive for 'industry best practice', which is continually evolving at this time, in developing and implementing these metrics. However, aspiring to such practices may be costly and, in many cases, excessive to the situation. Figure 2.5 shows the risk management practices continuum. This figure demonstrates that utilities should be cognizant of the difference between their current, actual practice and related metrics versus what is appropriate for their business and risk portfolio. A best practice component of risk management, such as the "best practice for EaR" may be in the short run unattainable or, at best, ineffective at marginally improving risk management practices from the appropriate practice level.

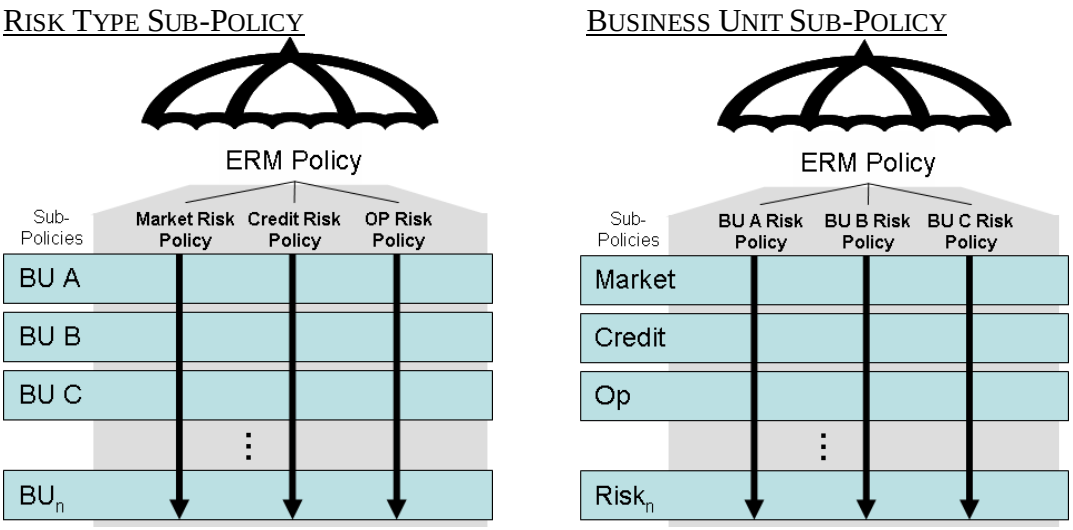
Figure 2.5: Risk Management Practices Continuum



2.4.5.Risk Policies

A firm's enterprise risk policy structure is a necessary foundation of ERM. The exact structure and presentation will vary by organization, but taken in totality, the enterprise risk policy structure includes an "umbrella" ERM policy. The "umbrella" ERM policy covers the ERM process, organization and responsibilities that provides specificity about, for example, how specific risks will be managed, which risk measures will be employed, specific authorities, and limits. The figure below illustrates two potential approaches to organizing the enterprise risk policy structure – by risk type and business unit. In practice, larger organizations with diverse business units might employ a hybrid of these "pure" approaches that includes some sub-policies by risk type (e.g. credit risk) and others by business unit. Regardless of the approach employed, key attributes of an enterprise risk policy structure include alignment between the ERM Policy and the sub-policies, and completeness in terms of risk types covered.

Figure 2.6: Illustrative Risk Policy Frameworks



The key objectives of a risk policy are to clearly articulate:

- The specific business activities that are permitted;
- The roles and responsibilities of individuals and departments in complying with the policy;
- All risk measurements that will be used to monitor each risk type; and
- Well-defined limits for each risk type.

2.4.6.Measurement and Reporting

The ERM framework encompasses a number of tools that can be used to identify, measure, and monitor risks. Many of these tools have emerged from financial markets, which were generally the first to implement extensive risk measurement and monitoring programs to manage market and credit risk. These risks have been the focus of many energy companies as they reflected the majority of risks born by energy marketers, IPPs and merchant generators. These market and credit risk tools typically focus on metrics related to minimizing losses to the value of an existing portfolio, and are statistically based. For utilities, these metrics may have only limited value for two reasons. First, these methods are based on statistics of highly liquid standardized products such as power and gas swaps. The types of products utilities offer rarely fall in this category,

with most energy utilities offering full requirements products. The risks associated with these products cannot be estimated using standard financial market tools because of the volumetric component of these markets that is highly correlated with the related markets.

Second, while most utilities face some form of market and credit risk, they also face significant operational and business risks. Risks such as reliability, regulation or legislation, reputation, and environmental, may be considerably more difficult to meaningfully quantify than market and credit related risks. Most frequently, this is a consequence of the lack of a meaningful database of outcomes that can be used to populate a distribution. In addition, some risks do not have a meaningful measure. In other cases, it should be recommended that some risks, regulatory risks for example, not be measured for discovery reasons. In other cases, historical outcomes may be available but may be too infrequent to generate predictions with any degree of confidence. As an example, a utility may have detailed historic data on reliability, but this will not necessarily predict the range of potential outages in the next peak period.

As a result of the unique risk profile of utilities, these companies should develop customized metrics and tools to measure the risks of their portfolios. This, however, is beyond the scope of this paper. While the Earnings-at-Risk measure described before will be applicable to utilities, stress-testing and scenario analysis should be employed liberally to develop a framework for understanding the unique nature of the risks a utility faces.

Stress Testing refers to creating defined scenarios in which one or more risk variables are changed in order to understand their impact on measured outcomes and understand overall firm risk sensitivities. These are frequently utilized in order to, for example, measure the impact of a large movement in commodity prices. In a utility environment, a stress test might be employed to test the impact of an increase in fuel prices or the effect of a large rate increase on demand consumption. In most cases, a number of tests are performed on a regular basis. These could include scenarios such as a large movement in the forward price curve, adverse environmental legislation, assumed regulatory decisions, or the adverse effects of workforce issues.

The results of the tests are reported and used by risk management to test the sufficiency of current hedge programs, the impact on the rate base, or to test new remediation strategies. Additional depth is obtained when the tests are performed with multiple variables. It is important to note that the stress tests themselves may not necessarily be probable or even possible outcomes. The value provided is in giving management a fuller understanding of sensitivities and relationships among different risks.

To ensure that stress tests provide their maximum benefit, a standard set of tests could be performed on a regular basis. Reporting of the results should explain the implications of changes in the results from one run to the next. At the same time, management should not be limited by the defined test set. In addition to the normal stress tests, new tests should be periodically run to ensure that new risk relationships, or unexplored correlations in the existing set of risks, are analyzed.

Scenario Planning refers to creating scenarios to better explore the risk environment and the sufficiency of risk management plans. The critical difference from stress testing is that scenarios need not be quantitative in nature. While the quantitative risks evaluated in stress tests may often

be utilized in scenario planning, scenarios typically go further in developing outcomes. For example, a typical scenario for a utility may involve a sustained service loss over an extended period. The financial impact would certainly be tested, but the analysis would go further in evaluating the sufficiency of recovery resources, the potential for reputational damage, regulatory backlash, additional reporting requirements, etc. Consequently, unlike stress tests, the results are not expected to be strictly quantitative. The results must include a narrative to explain the anticipated outcomes, the likelihood of the risk events, any other potential outcomes not explored, and the conclusions drawn from the exercise.

A complaint that is sometimes heard about scenario planning is that the scenarios tested are not "realistic." "Realism" is of course a qualitative assessment, but that said, risk managers should not feel limited to drawing up scenarios that are "realistic." Very often, the most insight into risks may come from "unrealistic" scenarios. Furthermore, many of the critical risk events that we have seen occur at various companies might well have been considered "unrealistic" by management prior to their occurrence. The critical benefit of scenario planning is to force management to think "outside the box" about the risk environment. "Unrealistic" scenarios force reviewers to realize that the greatest risks are sometimes the unknown, not the known.

Linked closely with risk metrics are monitoring and reporting, which are then linked back to risk tolerance, risk policies and ultimately governance. Effective monitoring and reporting processes are the cornerstone of an effective ERM framework. It is through these processes that controls are made effective through appropriate communication within the utility. Given the integral role that monitoring and reporting plays in ERM, it is important that firms implement a coherent reporting strategy and enabling infrastructure to ensure the free flow of necessary information to decision-makers. This integrated reporting strategy should effectively implement the monitoring requirements as set out in the ERM policy and sub-policies and comport to the culture of the organization. Reporting strategies consider not only the reports generated, but their frequency, distribution, and source.

For most organizations, this will not mean a monolithic, single platform reporting architecture, but instead a heterogeneous mix of manual and automated solutions to meet the diverse needs of different functions. For utilities, the critical consideration in designing a reporting strategy is the wall between regulated and non-regulated activities. This adds an additional layer of complexity to what is typically already a difficult process.

3. Implementation of Framework

ERM implementations should be highly customized at each firm such that the final framework is appropriate and reflects the complexity, size and sophistication of the company. Nevertheless, there are several key ingredients to a successful ERM framework and there are specific steps that can be taken to facilitate implementation.

3.1. Six Steps to Implementation

Virtually all ERM applications follow a typical framework as described in this section of the report. This process is illustrated in the following chart and each step is subsequently described. Examples of items to consider in each step are also shown.

3.1.1. Identify and Quantify Risks

The first step to an effective ERM framework is to identify and quantify the risks of the business. There are several techniques used by companies to inventory and quantify the risks. Once a firm identifies the dozens of risks they face, the risks are typically categorized and prioritized based

on various quantification techniques. When statistical tools and/or data are not available to quantify risks then subjective techniques are employed.

The risk identification and quantification step is generally a bottom -up process with information provided by each business unit. However, firms usually employ a risk management department or committee to inventory, collect, and measure or validate the quantification of risks. After risks are identified and potential impacts quantified, then risks are assigned to appropriate persons or departments in the organization to be dealt with in the following steps.

3.1.2. Establish Risk Tolerance and Policies

The second step to implementing an ERM framework is to define risk appetite and tolerance and then draft appropriate Risk Policies. Top priority risks that emerge from Step One of the process should be addressed by the strategic plans of the firm. Furthermore, the strategic plan should identify the risk management objectives and risk tolerance of the firm. These plans, objectives, and the risk tolerance should then shape the way that key risks are managed throughout the firm.

Risk Policies are developed to formalize and articulate the risk tolerance of the organization and to clearly identify the decision-making process and authority for individuals or committees within the firm to carry out transactions or business activities. The elements of the organizational design may include the following:

- A senior risk officer (often the Chief Risk Officer – "CRO") that has responsibilities for a broad spectrum of risks throughout the organization – often leads the Corporate or Enterprise Risk Management function ("CRM", "ERM")
- A Risk Management Committee ("RMC") Structure comprised of senior level decision makers representing various responsibilities within the company – may include Board and Management level committee members
- Positions within the business units that have responsibility for risk management
- Defined lines of reporting or communications to ensure an effective and comprehensive internal flow of risk information

The scope of risk issues that are the responsibility of the CRO may vary from company to company but most encompass a broad enough scope to allow for the identification and assessment of key drivers of firm performance. From an ERM perspective, the primary function of the CRO is to ensure that the elements necessary for an effective and efficient program are implemented and to oversee the ongoing process. Organizationally, the CRO role may report to one of various senior management positions, but must report at a level in the organization sufficiently high to allow the position to have some meaningful governance authority and ensure appropriate separation of duties. The CRO position should also have a reporting function to the Board of Directors much in the same way that the firm's internal auditor generally has a reporting relationship to the Audit Committee of the Board. Ultimately, the responsibility to inform the Board of significant risks rests with the CRO.

The Risk Management Committee provides oversight and governance of the company's risk management functions. Composed of senior management, the committee reviews and approves corporate and business unit risk management policies, risk roles and responsibilities, risk limits

and tolerance levels, risk positions and performance objectives. The committee should also address exceptions to risk policies, procedures and/or limits and ensure that business units are capable of measuring, managing, and monitoring their risks. In a recent survey of energy companies, over 80% had established either a board or management level risk committees. In some cases, RMC's existed at both the board and management levels.

Within the business units the responsibility for risk management is to implement risk policies and designated processes. The business unit must have individuals whose job descriptions outline their responsibilities relative to applicable risk policies and processes. In general, the business unit activities articulated in the policies and processes will be to identify, assess, and report on risks confronting their business unit as well as implement risk management actions to maintain operations within limits or at the direction of business unit or corporate management. The following table summarizes the potential roles and responsibilities of the risk management organizational elements.

Each policy will carry a different emphasis for each utility. In fact, some utilities may not need to adopt all of the policies shown above. For example, a public power utility whose primary risk management objectives and risk metrics may be focused on maintaining rate certainty and stability may put more emphasis on its hedging policy while an investor-owned utility may not require an energy hedging policy.

While the enterprise risk policy structure defines the firm's risk management philosophy and compliance requirements, the detailed procedures, process and internal control documentation provide the evidence of execution. A periodic comparison of the internal control framework with

the enterprise risk policy and sub-policies provides a basis to assess compliance on an ongoing basis. Integration of compliance with ERM can lower the redundancy of the monitoring functions of the firm through an integrated assessment process whereby companies work to rationalize the information requests and audits of the operating and support functions of the firm in order to ensure compliance with the lowest amount of intrusion and disruption. As ERM becomes an increasingly aspirational goal of energy companies, this approach is likely to become a common side effect of these efforts.

There should be a structure in place which ensures the risk management function is ultimately accountable to the Board. Any risk management committee charter or terms of reference should include:

- Authority – Mandates a level of risk management and control commensurate with best practices prior to engaging in certain commercial activities.
- Membership – Designates specific members and titles across the organization with an independent risk management officer leading each committee.
- General Duties –Includes a variety of duties including independent monitoring and reporting of risk.

These elements may be included within the risk management policy or by referencing the charter document of each risk management committee. It is helpful to include diagrams within this section of the risk management policy that help the reader visualize the committee structure within the firm.

3.1.3. Develop Business Unit Strategies and Metrics

Once the firm has a good grasp on its strategic plans, risk management objectives, and risk tolerance, then each business unit can develop specific strategies for managing the risks for which they are responsible. Of course, Steps 1, 2, and 3 are iterative since the business units will be responsible for identifying risk and assisting in formulating the strategic plans, risk management objectives, and risk tolerance of the organization, but nonetheless specific strategies should not be finalized until the risk management objectives and risk tolerance of the firm are clear.

In establishing risk tolerance through the use of metrics, management needs to determine which metrics best align with the overall risk appetite. It is quite possible that different members of the management team will be interested in different metrics – and reconciliation of these viewpoints is an important exercise that should not be avoided. Business unit strategies should be measured against specific risk tolerance or performance metrics. Several metrics are typically developed for firm-level and at the business unit level. Metrics are a critical component of risk management and serve the functions of articulating acceptable risk levels and providing valuable reporting tools to monitor the performance of the business unit relative to the risk management objectives and risk tolerance of the firm.

3.1.4. Implement Controls and Procedures

Controls and procedures for implementing strategies provide the assurance of proper oversight, processing, and execution of business activities. A strong control and procedural process is

necessary since many risks affect numerous business units even though risks are generally assigned to a single business unit to manage. For example, the trading unit trades commodities, but it must have trading contracts reviewed by legal and credit departments before transactions are executed. Controls and procedures also provide necessary safeguards against operative risks within the firm.

3.1.5. Execute Strategies

Finally, execution of strategies takes place. Many firms make the mistake of executing business unit strategies as the first step. This leads to an inconsistent approach to managing enterprise risks and often business units determine their own risk tolerance that will differ from that which the overall firm desires.

With an ERM process in place, strategies are executed based on a clear understanding of the risks being taken, clear oversight of activities, clear controls and procedures, and clear metrics that guide the activity and measure the level of success.

3.1.6. Monitor Risk and Reporting

The last step in the framework is continual monitoring and reporting of the risks of the business. Each business unit is responsible for monitoring certain risks and reporting them up through the risk management department in some fashion. As new risks emerge, there should be a systematic process for reporting them and determining if policies or strategies should change in response to the risk.

Additionally, metrics and risk reports should be systematically and consistently developed to communicate risk and results. Reports are disseminated throughout the firm based on a process agreed upon at various governance levels of the firm. A firm's reporting structure design should specify report ownership, contents, distribution, and frequency. Reports for the Board of Directors are the most general, yet they clearly articulate the risk of the organization and the performance around managing the key risks and strategies of the firm. As you move down into the organization of the firm, reports become more detailed. The risk management department either generates reports independently, or is responsible for overseeing the validity of the reports that are developed.

3.2. Key Challenges

Although many of the challenges a utility will face will be unique to the company's risk profile, there are several common challenges that all utilities will face to some degree. Specifically, all utilities will face challenges regarding the gap between existing and aspirational levels of risk management sophistication, formal and informal communication networks, and risk and business culture.

3.3. Implementation Sophistication

Throughout this paper, the concept of customizing the ERM framework to the utilities business has been emphasized. Any successful implementation of an ERM framework must consider the utility's current level of sophistication. If the utility has some risk management infrastructure in place, then the ERM framework will serve as an enhancement, with results showing improved risk management practices and procedures. Conversely, for a utility that has adopted few risk

management practices, an ERM framework implementation could produce great strides in the company's understanding of their risks and subsequent management and mitigation of these risks.

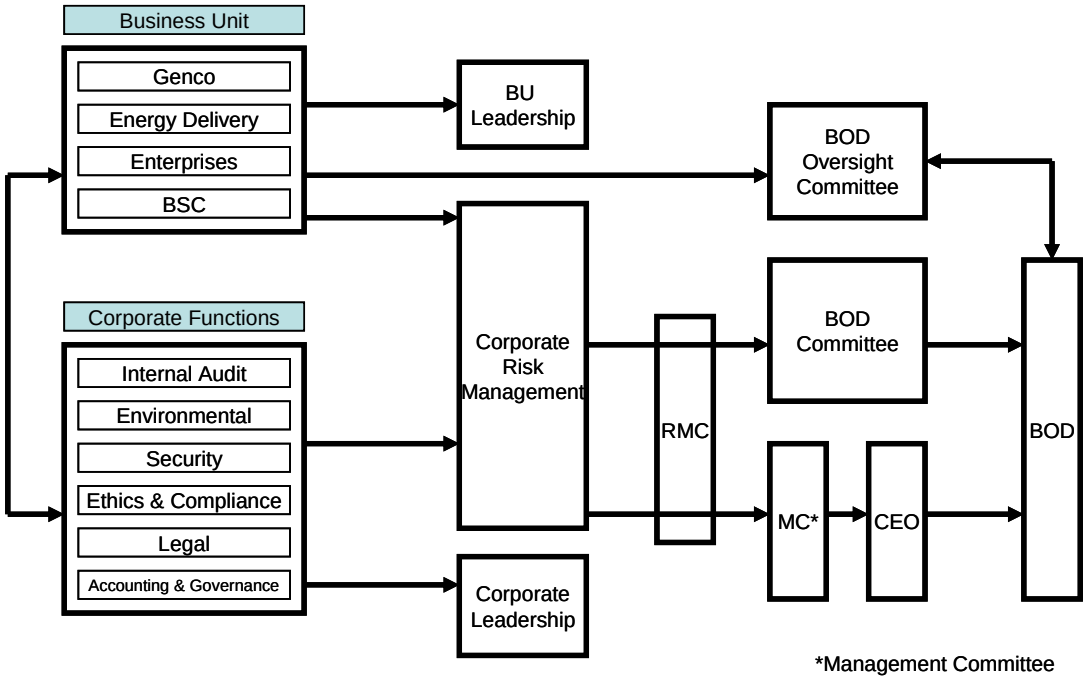
In addition to the level of sophistication present in the company is the degree of sophistication that is appropriate. As discussed above, a utility must not just ask, "Can we implement this structure?" but "Should we implement the framework?" That is, the incremental benefit of achieving greater sophistication in policies, metrics or governance may be far outweighed by the associated costs. Further, all companies implementing an ERM framework must be careful to not become too complacent once the program has been initially implemented. The temptation is to believe that an ERM framework is a 'silver bullet' that will fix risks. Instead it is a dynamic process that is constantly updated and refined with new information, changing market or business situations and level of complexity of the utility's portfolio.

3.3.1. Communication

Identified risks and their corresponding mitigation actions need to be communicated up and throughout the utility and to senior executives and the Board in a timely and accurate manner. To ensure consistency, accuracy and transparency, a formal reporting structure with defined frequency and standardized reports should be established and utilized. Figure 3.3 outlines one possible approach to the structure of a communications network. Key features of the communication network depicted include the redundancy and integration points. Corporate Risk Management, the Risk Management Committee and Board Oversight Committee are key synthesis and integration points where disparate information is bought together and analyzed. The Management Committee and Board of Directors can then use this information in making decisions. Another important aspect of this communication network is the redundancy of information flows which provides for some level of independent analysis and validation.

Once established, the communication network of a utility acts as its "central nervous system", delivering critical risk information to all interested parties. Hence, it is important to establish regular communication protocols to ensure that identified risks are regularly evaluated and the exposures communicated. More importantly, the communication network needs to be leveraged to identify emerging risks as well as a shifting of priorities among the utility's existing risks.

Figure 3.3: ILLUSTRATIVE COMMUNICATION NETWORK FOR UTILITIES



In addition to decision-making and capital allocation, management also needs to demonstrate a commitment to investigating surprises, both up-side and down-side. Most utilities have no trouble commissioning a post-mortem analysis to analyze what went wrong, but the investigation of upside surprises is much less common. A symmetrical response by management to both up-side and down-side surprises is a straightforward way to communicate the importance of risk management to the entire utility.

Most utilities provide earnings guidance to its shareholders/stakeholders in some form (EPS, EBITDA, EBIT, Net Operating Profit, and Net Income, or for public power entities, revenue requirements/cost and margin metrics). It is very important for the utility to meet its estimates or be able to explain clearly why financial targets were missed. In addition, upside surprises, while certainly more welcome than those to the downside, can still create the perception that management does not have an effective grasp of the business and lacks he necessary infrastructure to project and measure performance. Earnings risk can be estimated using techniques with varying levels of sophistication, complexity and cost. The increased complexity and cost of pursuing advanced measurement techniques is counterbalanced by the sophistication and insights potentially available.

3.3.2. Culture

A risk management culture is a set of beliefs, values, attitudes, customs, and behaviors about the management of risk that are shared among people in an organization. The organization's culture sets a tone and expectations for which behaviors will be either rewarded or discouraged. The corporate risk culture begins at the highest level of management; the Board of Directors and senior management. The Board and senior management should be major advocates of risk management within the organization and should be aware of, understand, and support risk management activities throughout the organization. The tone at the top is the key enabler to risk

management in any organization. A risk-aware culture can infuse risk management concepts and thinking into all of the decision-making, planning, and capital allocation processes of the organization. Leadership acceptance of the responsibility for risk management is evident when organizations have developed an effective risk management function that identifies the process for establishing authorities and responsibilities (governance) and rules and guidelines (protocols) that will identify, measure, monitor and manage those risks that impact the company's performance objectives. The risk management culture should embrace open dialogue in which "silo thinking" is discouraged.

The type of culture that fosters the notion of risk interdependence is one in which the risk owners are empowered to manage risks within the organization's risk appetite and risk tolerances. Open communication of risks is encouraged, as is the linking of objectives throughout the organization at all levels. The risk culture may be codified through policies such as a Risk Management Policy, Corporate Compliance Policy, and Contracting Policy. These policies should clearly tie governance and protocols to the risk appetite (the acceptable level of variation relative to achievement of the organization's objectives) defined by the Board and senior management with consideration given to appropriate practices.

Once a risk aware culture is present, risk management becomes intertwined within the normal course of business and increases the effectiveness of the organization's ability to balance the inevitable risk-reward trade-offs that arise in every day business activities. This drive for prudent risk management should be pushed down through management to the employee level. A risk-aware and compliant culture involves every member of the company. Business unit management should be expected to develop operating protocols/plans/policies that comport with ERM policy; identify, assess and report risks; propose strategies to mitigate key risks; implement a risk control structure that evidences compliance with ERM Policy; integrate risk management into operations, planning and strategy; and ensure that accurate risk related information is provided to senior management in a timely manner. Employees should be required by policy to report any material risks they have identified and should be expected to play a role in managing the various risks that a corporation is exposed to through its day-to-day activities.

Although this is a useful exercise in raising senior management awareness of risk issues, simply having a group-level statement of the desired aggregate risk profile will not in itself help the organization take the "right" risks in a well managed manner. To achieve that, risk management must become embedded throughout the organization. The "top-down" desired risk profile must be compared with the "bottom-up" reality. Aggregate reporting of the actual versus desired risk profile must be improved. The organizational model must be reviewed to ensure clear responsibilities and escalation criteria for "hard" and "soft" tolerance breaches. Finally, trigger levels, limit structures and delegated authorities must be realigned, and potential risk appetite implications must be considered in all major resource allocation decisions. This may seem a daunting and far-reaching array of tasks – but consider the ramifications if not undertaken: the firm's risk taking might be too extensive or "off strategy" or both, storing up potentially severe problems for the future.

4. Conclusions & Recommendations

The objective of this paper was to provide an understanding of ERM and assist executives in developing and applying an ERM framework unique to the business of a regulated utility. ERM is not a product, but rather a process by which utilities can iteratively improve upon their understanding, control and management of risks. An ERM framework for utilities should ultimately strive to first identify material risks and identify the level of risks that is acceptable for all stakeholders. Once these have been determined, the risk governance, policies, procedures, monitoring and controls should be established in a manner that is consistent with the level of risk being controlled and the current capabilities of the firm. Once the framework is in place, a continuous review of the risks, controls and metrics is essential to establishing a lasting and improving risk management function within a utility.

To successfully implement an ERM framework, each utility must first consider where they are on the Risk Management Practices Continuum. Utilities should avoid the temptation to strive for 'industry best practice' in developing an ERM Framework and, instead, focus on practices that most effectively manage risks for the individual utility. The general structure of the ERM framework is complex, but the key starting point is not to just consider all components of ERM with equal sophistication, but to consider the complexity of the firm's portfolio and the available risk management resources in determining the level of sophistication to apply to each of these components.

In any risk management endeavor, there will be challenges that will be unique to the company's portfolio, resources, management and regulatory environment. Nevertheless, the key ingredient to any successful framework is constant and clear communication and a culture of risk management throughout the company, lead by the tone at the top.

5. Appendix A: Risk Reporting Requirements

Illustrative High-Level Risk Reporting Requirements

Function	Overall Emphasis	Illustrative Risk Reporting Needs
Operating Units	Day to day operating decisions	• Notional and MtM analysis versus limits – commodity, location, spread etc. • Credit risk reports – authorized counterparty, exposure versus limits by counterparty, counterparty concentration report • P&L (gross margin) – realized and unrealized versus stop-loss limits • Cost-at-risk flow metric (vs. P&L) for non-profit/public power entities
Corporate / Enterprise Risk Management	Ensure that risks incurred are within constraints set-out in the risk policies of the firm	• Notional positions and risk exposures versus limits – aggregated across portfolios with drill-down capabilities • Control Self-Assessment – summary and detail • Enterprise Risk Metrics – EaR, CFaR, etc. • "Dashboard" of risks – long-term, intermediate and short-term risks; risk owners and mitigation plans • P&L (gross margin) – realized and unrealized versus stop-loss limits • Cost-at-risk flow metric (vs. P&L) for non-profit/public power entities
Risk Management Committee	Evaluate compliance with limits and policies	• Business performance report summarized to appropriate level of detail – typically presentation format aggregated from multiple sources • Compliance reports at appropriate level of detail • RMC – more detail showing trend analysis, scenarios and stress tests • BOD – "stoplight" summaries of critical risks • Unique or strategic risk assessment presentations – especially supporting investment decisions
Senior Management	Evaluate performance of the business and allocate capital	• Tone at the Top • Transform Risk Appetite to Policies and Procedures
Board of Directors	Evaluate performance of the business and meet fiduciary duties	• Tone at the Top • Develop Risk Appetite

6. Appendix B: Risk Governance Roles

ILLUSTRATIVE RISK GOVERNANCE ROLES AND RESPONSIBILITIES

Business Unit	• Develop sub-policies in conjunction with CRO/Corporate Risk that comport with ERM Policy • Identify, assess and report risks – propose strategies to mitigate key risks • Implement risk control structure that evidences compliance with ERM Policy and sub-policies • Integrate risk management into operations, planning and strategy • Ensure that accurate risk related information is provided to Corporate Risk Oversight in a timely manner for consolidation
CRO/ Corporate Risk	• Process lead in establishing and implementing ERM including the coordination of risk assessment, mitigation and monitoring activities • Develop ERM Policy and submit to RMC for approval • Work with Business Units to develop sub-policies as appropriate and submit to the RMC for approval • Facilitate the flow of risk related information across the company • Evaluate risks from a company portfolio perspective • Along with Internal Audit and Ethics and Compliance, evaluate the compliance of risk policies and procedures in the business units • Coordinate RMC meetings • Develop and implement an education program on risk management • Assess risks to the company in aggregate, by business unit, and by material business activities • Measure and report on the company's risk profile • Develop, recommend, and administer corporate risk management and/or middle-office processes and procedures • Research, develop, test, and implement risk measurement methodologies and models • Recommend to the RMC specific risk limits consistent with the company's risk management objectives, risk tolerance, and risk management policy • Report to the Board of Directors and the RMC on the company's compliance with its risk policy and risk management in accordance with the risk policy
RMC	• Approve risk management policies (ERM policy and sub-policies) • Approve key risk mitigation decisions • Approve key risk related assumptions (load growth, market prices, etc.) used in strategic and business planning processes across the organization • Monitor the management of key risks • Communicate and discuss key risk issues with senior management and the CEO
Board of Directors	• Review and approve ERM policy and other key decisions as escalated from the RMC • Via audit committee or other board oversight body, provide independent evaluation of the risk management governance and infrastructure of the company • Monitor the management of key risks via periodic reporting provided by the RMC, CRO, and/or Business units
Internal Audit	• Annual process audits and reviews

For more white papers, or if you are interested in learning how to become part of the Committee of Chief Risk Officers, please contact us:

Committee of Chief Risk Officers
9595 Six Pines Drive Ste 8340
The Woodlands, TX 77380

p: 281.825.4870
e: info@ccro.org
w: www.ccro.org