



Volume IV

Number 11

SPECIAL REPRINT

Operational Risk Measurement and Management...

For Energy and Commodity-Related Firms

By Carlos Blanco, Black Swan Risk Advisors, and Robert Mark, Black Diamond Inc.

Operational risk measurement and management is rapidly becoming standardized across the financial industry. We would expect in the near term that a similar trend toward standardization will take place for energy and commodity-related firms. The nature of core operational risks for firms in the energy and commodity space is tightly related to the management of physical assets such as storage facilities, transmission and distribution assets, and power plants. Therefore, those risks are considerably different than the operational risks faced by financial services firms. In this article, we present an overview of the key issues in measuring and managing operational risk

for energy and commodity-related firms in an enterprise-wide, risk-management framework.

Introduction

Traditionally, energy and commodity-related firms have managed their operational risks without the benefit of a formalized operational risk-measurement program or taking an integrated view of all risks. However, the traditional approach is no longer adequate due to the need to take into account the linkages between risk types – credit and operational risk – and to standardize and integrate various risks and business results across different asset classes – explicit or implicit commodity and currency risks. These risks can be current or implicit future risks. For example, the total sales from a power plant's output are subject to future price and volume risk.

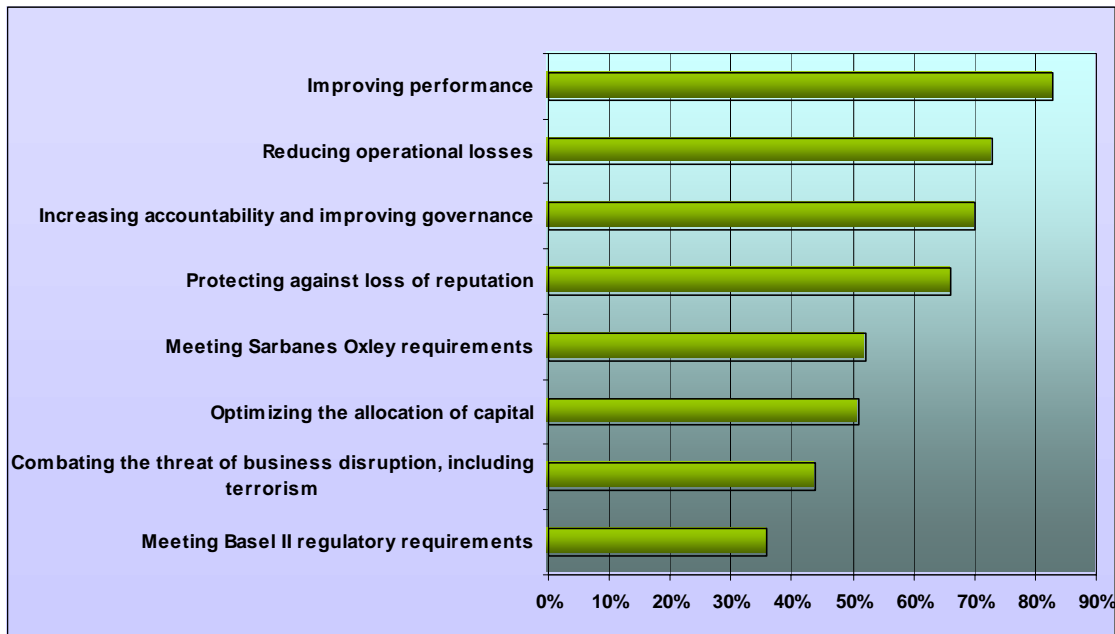
(Click to continue on page 2)

(OPERATIONAL RISK MEASUREMENT from page 1)

Oil, natural gas, electricity and multicommodity-related energy firms are implementing enterprise-wide risk management (EWRM) programs that integrate market, credit and operational risks. Management is paying more attention to these EWRM programs because they are complex and because of new regulatory and external pressures.

Operational risks should be controlled under formalized risk measurement and management programs. These operational risks should command management attention. For example, an audit program would be wise to focus on those areas with the greatest potential risk to the organization. The benefits of a formalized operational risk program vary from firm to firm. Nevertheless, it is clear that the main objectives of an operational risk program should be outlined in advance. For example, Figure 1 presents a summary that was based on a survey of managers' main reasons to invest in operational risk measurement and management.

Figure 1. Main Reasons to Invest in Operational Risk Measurement and Management



Source: Risk Management Association (RMA). 2003.

1. Operational versus Operations Risk for Commodity and Energy Firms

The classic financial services definition of **operational risk** refers to financial loss caused by inadequate computer systems, a failure in controls, a mistake in operations, a guideline that has been circumvented or a natural disaster, etc. It includes some elements of reputation risk as well as legal and compliance-related risks. Operational risk for energy firms is considerably different than the risk for financial institutions. For example, the Committee of Chief Risk Officers (CCRO) has recommended that **operations risk** should be included as an important risk category. Operations risk is defined as the risk associated with delivering, producing or storing physical energy products.

Outages and blackouts are some of the most prominent operations risks faced by utilities. Table 1 presents a summary of the most serious outages and blackout events since 1965, indicating the megawatts (MW) lost and the millions of people affected.

Table 1. Major North American Power Outages 1965 -2003

Event	Date	MW loss	People Affected
Northeast Blackout	Nov. 9, 1965	20,000 MW	30 million
New York City Blackout	July 13, 1977	6,000 MW	9 Million
West Coast Blackout	Dec. 22, 1982	12,350 MW	5 million
West Coast Blackout	July 2-3, 1996	11,850MW	2 million
West Coast Blackout	Aug. 10, 1996	28,000MW	7.5 million
Upper Midwest Blackout	June 25, 1998:	950MW	152,000
NE and Canada Blackout	Aug. 14, 2003	61,800MW	50 million

Source: US-Canada Taskforce report (2004)

These major outages shared some common features. They are:

- ◇ conductor contact with trees;
- ◇ overestimation of dynamic reactive output of system generators;
- ◇ inability of system operators or coordinators to visualize events on the entire system;
- ◇ failure to ensure that system operation was within safe limits;
- ◇ lack of coordination on system protection;
- ◇ ineffective communication;
- ◇ lack of safety nets;
- ◇ inadequate training of operating personnel.

An analysis of these common factors can be a starting point of investigating some risks that should be monitored and managed by utilities. According to the final report by the US-Canada Power System Outage Task Force, the Aug. 14, 2003, blackout was caused by deficiencies in specific practices of the collective market participants as well as the entity-specific equipment and human decisions that afternoon. Estimates of the total costs in the United States range from \$4 billion to \$10 billion. In Canada, gross domestic product was down 0.7 percent in August. There was also a net loss of 18.9 million work hours. Further, manufacturing shipments in Ontario were down C\$2.3 billion.

Operational failures from First Energy (FE) were a direct cause for the blackouts. The main problems were related to

(Click to continue on page 3)

(OPERATIONAL RISK MEASUREMENT from page 2)

inadequate situational awareness at FE and the failure to adequately trim trees in its transmission rights-of-way. In particular, FE:

- ◇ failed to ensure the security of its transmission system after significant unforeseen contingencies because it did not use an effective contingency analysis capability on a routine basis;
- ◇ lacked procedures to ensure that operators were continually aware of the functional state of their critical monitoring tools;
- ◇ lacked procedures to test effectively the functional state of these tools after repairs were made;
- ◇ did not have additional monitoring tools for high-level visualization of the status of their transmission system to facilitate operators' understanding of transmission system conditions after the failure of their primary monitoring/alarm systems.

The CCRO recommended a categorization of operational risk according to a set of filters that allow for the aggregation, organization and analysis of these risks. Table 2 presents an example of such categorization.

Table 3. Degree of Management Attention Based on the Combination of Frequency and Severity of the Operational Events.

		Severity of loss (impact on profits)			
		Catastrophic	Critical	Marginal	Negligible
Frequency of occurrence within 1 year	Extremely Low (<0.1%)				
	Very Low (0.1-2%)				
	Low (2-5%)				
	Medium (5-10%)				
	High (10-20%)				
	Very High (>20%)				

Degree of management attention required

High Low

2. Defining and Classifying Operational Risk

The management of an institution should define what is included in operational risk. This will minimize the degree of conceptual fuzziness. To do this, a typology of operational risk must be established.

For each operational risk, a probability or likelihood and a severity or consequence rating can be assigned (see Table 3). Each combination corresponds to a particular level of risk. Each firm defines the number of probability and severity categories.

Each firm needs to perform an analysis of the major operational risks it faces.

Table 2. Sample Typology of Operational Risks for Firm XYZ.

Risk Class	Risk Type	Activity or Event	Examples	Mitigation	Frequency & Severity
People	Internal	Unauthorized Activity Lack of skilled personnel	Rogue Trading High employee turnover	Partially insured	
People	External	Fraud	Theft	Partially insured	
Systems	Internal	Model Risk	Model/Methodology error Mark-to-model error	Technical risk audit Improve quality of models/people	
Systems	External	Technology Risk	Telecommunication failure Blackouts	Contingency planning Insurance	
Processes	Internal	Transaction Risk	Execution error Settlement error Documentation/contract risk	Improve processes	
Asset damage	Internal	Physical asset risk	Pipeline Rupture Production loss Unexpected plant outage	Partially insured Contingency planning	
Asset damage	External	Physical asset risk	Uninsured or irrecoverable loss or damage to assets	Insurance	

Degree of management attention required

High Low

Disclosure of operational risks to third parties is an important component of best-practice risk management. In Panel I we can see a sample disclosure of operations risk from Pacific Corp's 10-K from March 2004.

Panel I. Risk Disclosure: Significant Operational Risks for PacifiCorp's Management.

- ◇ Generation facilities:
 - thermal and hydroelectric performance, plant maintenance and loss of generating availability;
 - managing physical fuel supply, including coal and natural gas.
- ◇ Mining operations:
 - access to sufficient coal reserves at required quality.
- ◇ Distribution and transmission system:
 - management of network reliability, including maintenance;
 - levels of network reliability in emergency conditions, including storms;

(Click to continue on page 4)

(OPERATIONAL RISK MEASUREMENT from page 3)

- system restrictions, management of transmission scheduling and capacity limits.
- ◇ Wholesale energy transactions:
 - effectiveness of energy balancing activities to serve load;
- ◇ Information technology:
 - maintaining critical information technology systems and reliance on them.
- ◇ Labor relations:
 - availability of skilled labor;
 - work stoppages due to union disputes;
 - attracting and retaining key personnel;
 - maintaining safe working conditions.
- ◇ Security:
 - effectiveness of security policies and disaster recovery plans in safeguarding assets.

Another example of operational risk disclosure is annual reliability reports that utilities operating in California must submit to the California Public Utilities Commission (CPUC.) Table 4 shows an operations risk report with the 10 largest events in 2001 prepared by PacifiCorp. for the CPUC.

Table 4: 10 Largest Outage Events in 2001 for PacifiCorp.

Description	Date	Number of Customers Affected	Customer Minutes Lost	Longest Customer Interruption (minutes)
Tree – Non-preventable	11/28/2001	380	1,300,360	3,422
Tree – Non-preventable	11/28/2001	246	1,222,878	4,993
Wind	11/28/2001	1,527	792,513	519
Snow, Sleet and Blizzard	12/1/2001	599	779,299	1,301
Tree – Non-preventable	11/29/2001	418	777,898	1,861
Snow, Sleet and Blizzard	11/28/2001	477	675,432	1,416
Vehicle Accident	11/15/2001	599	508,551	849
Major Storm or Disaster	11/19/2001	838	452,520	540
Loss of Supply	12/1/2001	380	421,040	1,108
Vehicle Accident	12/17/2001	599	392,354	672

Source. Pacific Corp. Annual reliability report. 2002

Internal dependencies should be reviewed according to a common set of factors, such as capacity, capability and availability. For example, if we examine operational risk arising from the people risk category for a particular business unit, then we could ask:

- ◇ Does the business unit have enough people (capacity) to accomplish its business plan?
- ◇ Do the people have the right skills and experience (capability)?
- ◇ Are the people going to be there when needed (availability)?

External dependencies should also be analyzed in terms of the specific type of external interaction.

The main operational risk categories should not be viewed in isolation from one another. In other words, best practice calls for analyzing the interactions among the various operational categories in order to understand the full impact of operational risk. Let's assume that the firm is introducing a new inventory system. The new inventory system may generate a set of interconnected risks across people, processes and technology. In order to ana-

lyze the operational risk, the interconnections among people, processes and technology must be fully understood when the new system is implemented.

Finally, the source of each major category of operational risk should be analyzed. In Table 5 we can see that the drivers in our illustrative example fall broadly under the categories of change, complexity and complacency.

Table 5. Interconnections of Operational Risks.

Dependencies	Internal External	Connectivity of Operational Risk Measures
Operational Risk Categories	People Process Technology	
Sources	Change Complexity Complacency	Likely drivers of operational risk associated with each operational risk category

Source: Crouby, Galai, Mark (2000)

3. Management Actions to Mitigate Operational Risk

The information prepared by the operational risk group should be analyzed by management in order to decide possible corrective actions to control some of the operational risks covered by the analysis. The main categories to mitigate operational risk can be grouped into:

a. Improved internal controls

Improving the internal control environment can bring many benefits in terms of lowering certain operational risks.

Sarbanes-Oxley (SOX) requires the CEO and the CFO of publicly traded corporations to take responsibility for designing, establishing and maintaining disclosure controls and procedures. The CEO and CFO must also disclose to the audit committee and to the

company's external auditors any deficiencies and material weaknesses in internal controls, as well as any fraud (material or not) involving anyone with a significant role in internal control. The law creates a more rigorous legal environment for the board, the management committee, internal and external auditors and the chief risk officer (CRO).

The act also seeks to make sure that the board of the company includes some members who are experts in understanding financial reports and have experience with internal and accounting controls as well as an understanding of audit committee functions. In panel II, we can see a brief summary of the implications in terms of the forward curves used to value transactions and perform risk analysis.

(Click to continue on page 5)

(OPERATIONAL RISK MEASUREMENT from page 4)

nents are not meant to be sequential in nature. Each component is likely to influence another.

Panel II: Forward Curve Management and SOX

The estimation and validation of forward price curves used for valuation and risk measurement purposes are two of the building blocks of any valuation and risk management program. For example, Enron was able to inflate earnings due to the manipulation of forward curves and the lack of a unified, audited set of forward curves to be used as a reference benchmark across the firm.

Any internal or external audit of risk and pricing models should start with the analysis of the forward curves being used throughout the firm. Lack of standard forward curves may result in units within the same firm reporting different values for similar transactions. Under SOX, that would represent an error in disclosure.

If the process to generate, store and use forward curves are not documented, audited and standardized across a firm then this should be a noncompliance warning because of the potential for abuse.

The SEC also requires that each firm has “a suitable, recognized control framework.”

The framework that is emerging as the standard is the one developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), a private industry initiative organized in 1985 by five of the key finance professional organizations in the US to sponsor a national commission on fraudulent financial reporting. COSO’s emphasis on internal controls has emerged as an important element of the overall risk governance exercise, particularly with the advent of SOX.

In the COSO framework, internal controls are defined as those that assure the effectiveness and efficiency of the firm’s strategy, operations, the reliability of financial reporting, and compliance with laws and regulations. Recently, COSO produced a report that moved beyond internal controls to produce “a broadly accepted framework for enterprise risk management.” (See Figure 2)

COSO’s various reports are an important industry attempt to define the board’s relationship to management. COSO emphasized that management is accountable to the board of directors and that the board should provide the appropriate governance, guidance and oversight. COSO has also helped establish the critical oversight role of the board and the audit committee.

COSO stresses an integrated approach toward identifying and managing risk across the firm. In particular, it explicitly defines the importance of establishing the relationship between the entity **objectives** and the **components** of the control process. Entity objectives can be viewed in the context of four categories at various levels of the organization: strategic, high-level goals supporting its mission, effective and efficient use of its resources, reliable reporting and compliance with applicable laws and regulations.

The eight components of the internal control environment within an enterprise risk-management framework are summarized in Table 6. It is important to point out that the compo-

Table 6: The Eight Essential Components of an Effective Internal Control Environment.

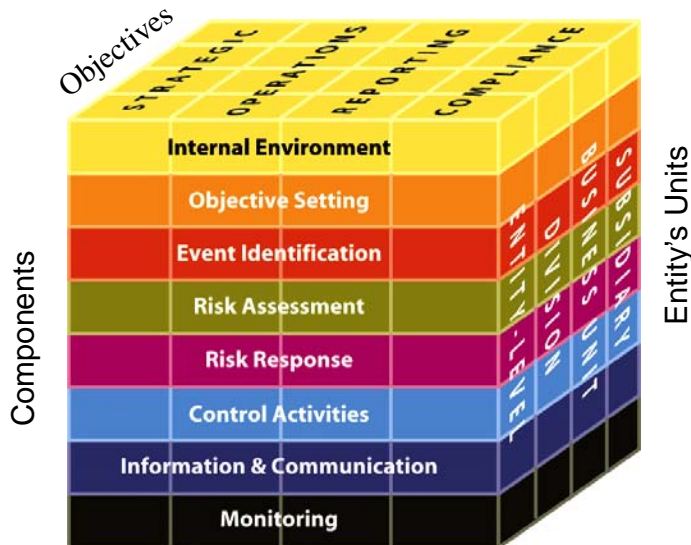
Component	Description
Internal Environment	The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity’s people, including risk-management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
Objective Setting	Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.
Event Identification	Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.
Risk Assessment	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
Risk response	Management selects risk responses – avoiding, accepting, reducing or sharing risk, developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
Control Activities	Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication	Relevant information is identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
Monitoring	The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both. Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can influence another.

(Click to continue on page 6)

(OPERATIONAL RISK MEASUREMENT from page 5)

The interrelationships among objective and components can be viewed in Figure 2. The four **objectives** categories are represented by the vertical columns and the eight **components** by horizontal rows. A third dimension that represents the **entity's units** is also analyzed. This "cube" representation allows for the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit or any subset thereof.

Figure 2: The Interrelation between objectives, components of the enterprise wide risk program and the entity's units.



Source: COSO. *Enterprise Risk Management Framework. Draft. Summer 2004.*

b. Operational Mitigation

Controls for energy and commodity-related firms should clearly extend to the operating and hedging of physical assets in order to minimize the impact of operational failures at the firm. In some cases, it may require investing in new assets or divesting those assets.

Operational mitigation solutions tend to be a medium-term and long-term measures. For example, building a power plant in order to gain additional generation capacity and either reduce dependency or gain flexibility to operate in the spot market cannot be achieved overnight. Buying and selling assets are also decisions that take considerable time until they are completed.

The firm can also enhance their management of operational risk by setting up formal partnerships among different groups involved in the process (see Panel III).

Panel III: Managing Operational Risk as a Partnership

The key to success in managing operational risk more effectively is to form a partnership between business units, internal audit and risk management. The operational risk information should travel from the operational environment, which includes infrastructure, corporate governance and business units, to the operational risk management function. In return, the operational risk-management function should provide operational risk-management analysis to all units on a timely basis. The operational risk-management function should also develop policies, generate firm-wide and regulatory risk reports as well as work closely with the audit function.

For example, the risk-management personnel cannot be expected to be experts in the actual operations of the physical assets, but they should take the lead in working with operations personnel in providing metrics and analysis to senior management and audit groups that reflect the risk of those operations.

The various business units should implement the policy, manage the risks and generally run their business. At regular intervals the internal audit function should ensure that the operational risk-management process has integrity, and is indeed being implemented along with the appropriate controls. Accounting and process-oriented audits should also include addressing the more technical aspects of a firm's risk control program.

c. Insurance/Risk Transfer

Another way to reduce operational risk is to transfer the risk to a third party. Insurance can cover certain events, but it can be expensive. Energy and commodity-related firms can transfer some of their operational risks to third parties such as insurance companies or investment banks. Outage insurance is a typical example (see Panel IV). Each firm must perform cost-benefit analysis in order to evaluate whether it should purchase insurance or transfer certain risks to third parties that have expertise in managing those risks.

4. Role of Technical Risk Audits

A key audit objective is to evaluate the design and conceptual soundness of the operational risk metrics and the reliability of the reporting framework. "Technical risk audits" are needed to ensure that the risk-management processes and models are adequate to control risk. Some firms have self-assessment programs in place.

(Click to continue on page 7)

*(OPERATIONAL RISK MEASUREMENT from page 6)***Panel IV: Outage Insurance Evaluation**

Forced outage insurance can provide coverage against an unexpected outage. The protection is particularly relevant for firms that have sold power forward at fixed prices and utilities that must supply that power and may be faced with a power shortage due to an outage or a counterparty that defaults when it was expected to deliver power at fixed prices.

In order to reduce the cost of forced outage insurance, some firms have included additional triggers such as combinations of a forced outage and power prices exceeding a particular threshold before the policy pays off. Insurance firms that offer such policies include Swiss Re and XL Weather and Energy.

It is important to have the right analytics in order to evaluate the risk reduction achieved with an insurance transaction versus the cost for the firm. One must also evaluate the costs and benefits of purchasing forced outage insurance versus other risk transfer mechanisms. In the case of the evaluation of outage insurance, it is essential to have a good simulation engine that can produce accurate price and volume scenarios at the right time as well as model the availability of the plant at each point in time under each scenario.

However, their effectiveness may be limited and risk-management personnel can play a crucial role (see Panel V). In addition, the firm should conduct technical risk audits performed by independent risk specialists to examine the adequacy and effectiveness of the processes for measuring and monitoring risk documented in the risk policies and procedures documents.

Panel V: Self-Assessment vs. Risk Management Assessment

There are multiple questions about a self-assessment approach even though it may seem appealing at first sight. Many would argue that the scope and complexity involved in assessing operational risk necessitates that management of the individual business should be in charge of assessing their own risk. Nevertheless, it is highly unlikely that a business manager committing fraud would accurately self-assess the operational risk of his business unit. For example, if Barings management had asked Nick Lesson to prepare an operational risk assessment, chances are that he would have not been objective. Enron was another example where self-assessment would not have shed much light into the internal risks being taken.

A commonly mentioned argument in favor of self-assessment is that risk managers cannot possibly know as much about the business as the business manager in terms of making the tradeoff between seeking new opportunities and managing the associated operational risks of the business. This, however, confuses the respective roles and responsibilities of the business manager. The operational risk manager is trained in evaluating risk from the available information. For example, to ensure objectivity, consistency and transparency, the independent risk-management function is therefore obliged to become involved in the gathering and processing of data.

An optimal structure consists of risk managers partnering with business managers to provide an accurate view of the risk at a reasonable cost. In order to accomplish their task, risk managers must be placed "in the flow" of all relevant business management information. This can be accomplished by inviting them to sit on the various regular key business management meetings, and by ensuring that they received regular management reports.

Technical audits should also evaluate the operational risks that affect risk-management information systems that are used to assess market, credit or operational risk itself. This includes, but is not limited to, examining controls related to the accuracy and completeness of market and position data, as well as the parameter estimation process.

A technical risk audit is designed to evaluate the policies and procedures as well as models used to measure and manage risk. Risk always finds the weakest link and companies that take a reactive approach to risk management are likely to fall behind the curve. Panel VI illustrates a series of questions as part of a technical risk audit dealing with operational risk issues.

Panel VI: Technical Risk audit of operational risk procedures

1. How do you measure operational risk?
2. What is the scope of the risks categorized as operational risks?
3. Do you complement the normal operational risk analysis with stress tests?
4. Do you maintain a database with historical losses related to operational failures?
5. How do you harmonize operational risk metrics and stress test methodologies?
6. What is the interval between the actual operational risk event and the detection of a loss?
7. Do you benchmark operational losses against industry standards?
8. Is there a pattern of common causes that could be mitigated in the major operational losses?
9. Are major operational failures associated with large market and credit losses?
10. Do you incorporate operations and operational risk in stress tests?

5 . Summary and Conclusions

Operations risks have received a great deal of attention recently. Energy and commodity-related firms have realized the vital importance of developing a strong risk culture throughout the organization, as well as having an independent, strong risk-management and audit group.

In this article, we have stressed that Operational Risk should be managed as a partnership among business units, infrastructure groups, finance and corporate governance units such as internal audit and risk management.

New regulatory and governance requirements place increasing emphasis on the role of senior managers and board members to ensure that the firm establishes a risk-aware business culture and a corporate environment in which best-practice operational risk management can flourish.

The increasing complexity and degree of interaction of the risks involved in energy or commodity-related firms mean that enterprise-wide risk education and awareness should be a critical item in the agenda of senior executives and boards of directors.

The key challenge for senior management is to harmonize the behavior patterns of business units, infrastructure units, corporate governance units, internal audit and risk management. If senior management creates an environment where all sides "sink or swim" together in terms of managing operational risk,

(Click to continue on page 8)

(OPERATIONAL RISK MEASUREMENT from page 7)

the weakest links in terms of risk will be strengthened and regularly overseen by many sets of eyes.

In our next article, we will present a series of quantitative and qualitative operational risk measurement techniques in the context of energy and commodity-related operations dealing with physical and financial transactions. We will conclude by showing how operational risk can be integrated into RAROC calculations to obtain a comprehensive view of risk and return across the firm.

Bibliography

Bank of International Settlements. (2004) "International Convergence of Capital Measurement and Capital Standards: A Revised Framework." Basel Committee on Banking Supervision. June.

Risk Management Association. (2003) Progress in Operational Risk Management in the US Banking Industry. October.

Blanco, C. and Mark, R. (2004) "EWRM for Energy Trading Firms: EWRM starts with Risk Literacy." *Commodities Now*. September 2004.

Blanco, C. and Mark, R. (2004) "A Modern EWRM Framework: Liquidity Risk-Management Process for Energy and Commodity Trading Firms" *The Risk Desk*. August. Volume IV. Number VIII.

Crouhy, M., Galai, D. and Mark, R. (2000) Risk Management, McGraw-Hill. New York.

PacifiCorp. Electric System Reliability 2003 annual report. Prepared for the California Public Utilities Commission. March, 2004

US- Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. April 2004

Carlos Blanco, Ph.D. is managing director of Black Swan Risk Advisors, LLC (carlos@blackswanrisk.com), an independent advisory firm with a proprietary approach to the design, development and validation of all aspects of financial risk-management programs to global energy and commodity trading firms. He is a regional director of the Professional Risk Managers' International Association's (PRMIA)

Robert M. Mark, Ph.D. is the CEO of Black Diamond (bmark.blackdiamond@tmo.blackberry.net), which provides corporate governance, risk-management consulting and transaction services. He serves on several boards such as the Fields Institute for Research in Mathematical Sciences, and IBM's Deep Computing Institute, and is an advisory director on Entergy Koch's Audit Committee of the Board. He chairs the Professional Risk Managers' International Association's (PRMIA) Blue Ribbon Panel

The authors welcome your feedback and would like to thank Dr. Kevin Dowd, Chris Mammarella and Gabriel Thoumi from Black Swan Risk Advisors for helpful conversations and insights.