Operational Risk Management - The Next Frontier
The Risk Management Association (RMA)

Operational risk is not new. In fact, it is the first risk that banks must manage, even before they make their first loan or execute their first trade. What is new is the idea that operational risk management is a discipline with its own management structure, tools, and processes, much like credit or market risk.

In the 55 financial institutions surveyed, there has been a significant focus on development of risk management for market and credit risks over the past ten to 20 years. Yet, the recognition of operational risk management as a separate discipline has occurred primarily during the past three years. Although a great deal of progress has been made, many areas are yet to be explored. Consequently, we have titled this survey Operational Risk Management—The New Frontier.

The key conclusions of the research are:

- Operational risk management programs protect and enhance shareholder value.
- The creation of operational risk management programs has been driven by: (1) management commitment, (2) the need for an understanding of enterprise-wide risks, (3) a perceived increase in exposure to operational risk and risk events, and (4) regulatory interest.
- A new organizational model is emerging with a new position—a Head of Operational Risk, reporting to the Chief Risk Officer. The role is to develop and implement the operational risk framework and consult to the lines of business.
- There is consensus on the core definition of operational risk: The risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events.
- Methodologies are evolving to quantify Operational Risk Capital. While progress is being made, there is no consensus on approach, and methodologies are not yet used as a basis for decision making.
- A framework for operational risk management is emerging, consisting of a set of integrated processes, tools, and mitigation strategies.
- There are five stages of development of an operational risk management framework. Understanding these stages will aid companies to benchmark progress and identify priorities.

Operational risk management initiatives protect and enhance shareholder value. Operational risk management protects and enhances shareholder value. Senior managers surveyed most frequently cited enhanced shareholder value as a primary benefit of operational risk management. Also cited were internal awareness of operational risk, protection of reputation, and lower levels of operational losses.

Respondents are convinced that effective operational risk management can add value by improving competitive advantage and reducing the level of losses from large events that can imperil financial condition and smaller, more frequent incidents.

Operational risk management programs were created for five reasons. During the past three years, senior management has taken a more active role and demonstrated interest in operational risk. Five key reasons for this increased attention are:

1. Senior management commitment.
2. Perceived increase in operational risk.
3. Reaction to major loss events that have occurred internally or to others.
4. Focus on enterprise-wide risk management.

5. Regulatory attention.

A common definition for operational risk is emerging. The debate on how to define operational risk has at times overshadowed the debate on how to manage it.

The study found, however, perhaps not surprisingly, that many banks have an internal definition of operational risk and most banks are satisfied with that definition.

In reviewing those definitions, analyzing common classifications, and eliminating the linguistic, cultural and organizational differences, it became clear that there is a common core operational risk definition, specifically:

Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events.

Each firm can modify this definition with additions, deletions or emphases that reflect its individual circumstances. But at an industry level, this definition expresses the core operational risk factors to most firms and can facilitate exchange of information. This definition is not intended to include defaults or changes to financial markets that are otherwise covered in the scope of market and credit risks.

This definition excludes business/strategic (business) risk because there was not a consensus view on whether to include it or not. The remainder of this report does not address management of business risk.

Firms are structuring a new position: Head of Operational Risk. The business units are primarily responsible for managing operational risk on a day-to-day basis. While the trend for market risk and credit risk is towards increasing centralization, operational risk, by its nature, is decentralized. In operational risk there is no position to report, few approvals to request, or hard policy limits to measure against. The businesses have this risk whether they like it or not, and cannot transfer the responsibility for management of it.

Survey findings identify three generic organizational models for operational risk management. The culture of the organization, rather than the type of institution, determine the selection of any one of these three models. One model has a head office operational risk function, the second has a dedicated but decentralized support, and the third has Internal Audit playing a lead role in operational risk management.

The Head Office operational risk approach is the trend gaining widest acceptance. Often led by a head of operational risk who reports to the chief risk officer, the model typically includes a small Head Office staff of less than five. It is complemented by staff dedicated to supporting individual business units, as part of either the business units or the corporate function, but in either case, operating under a common framework.

Other aspects of the model and additional organizational units that play important roles are:

- The Board of Directors is taking a more active interest in reviewing operational risk policies and major issues.
- Operational Risk Committees are being established to heighten awareness and prioritize resources.
- Other Risk-Related functions (e.g., Information Technology, Legal, Compliance, Human Resources) have responsibility for specific operational risk issues.

The Head Office operational risk function is responsible for development of firm-wide operational risk policies, framework and methodologies, and advising the business units. In this emerging model, the most common responsibilities are to:

- Determine operational risk policies and definition.
- Develop and deploy common tools.
- Establish indicators.
- Assess benefits of programs.
- Analyze linkages to credit and market risk.
- Consolidate cross-enterprise information.

In addition, this function focuses on cross-enterprise operational risk management initiatives such as developing economic capital methodologies and building loss databases. It also can be charged with the management of the firm's portfolio of operational risks.

Depending on the relationship with the business units, they may also consult or participate in operational risk management projects with business units.

Companies use a variety of stand-alone tools to help manage operational risk. Operational risk management is developing a comprehensive set of tools for the identification and assessment of operational risk. Individual firms use a wide variety of techniques. This study concentrated on five techniques:

1. Self- or risk assessment.
2. Risk mapping.
3. Risk indicators.
4. Escalation triggers.
5. Loss event database.

Some 71% of survey respondents use or plan to use all five tools. Currently, the most valued and most used tool is self- and risk assessment. However, the tool that most firms are looking to develop next is the internal loss event database.

Methodologies to quantify operational risk capital are improving, but firms are not satisfied with the results so far. The majority of firms that responded (31 out of 55) are trying to develop a measure of economic capital for Operational Risk. However, the gap between what most firms want to achieve and what they are able to achieve remains significant. Most report that they are not satisfied with their approach or with the behavioral incentives that they create. As a consequence, operational risk capital measures are not used to drive economic decision making.

Considerable progress is being made within the industry; however, a healthy diversity of approaches is being applied along a continuum of top-down and more risk-based, bottom-up approaches. These risk-based, bottom-up methodologies often rely on actual loss event data. They can quantify the level of exposure to each type of risk at the business line level, and react to changes in the control environment and actual operational risk results. Since no single approach is satisfactory, most firms currently use multiple methodologies to bound a result. Overall, if one trend does exist it is the movement toward risk-based and bottom-up methodologies. To go further, the industry will need to overcome three major obstacles: data, measurement, and management acceptance.

A framework for operational risk is emerging, consisting of a set of integrated processes, tools, and mitigation strategies. In the chapters of this report are the results of detailed questions and interviews about the components of operational risk management, ranging from organization to processes to reporting. In any financial firm each component is important, and

they complement one another. Upon reflection on these components as well as interview results, we can suggest an enterprise-wide operational risk framework that pulls the pieces into an integrated whole.

The framework has five key components that reflect the company's culture, including the style of decision making, the level of formal processes, and the attributes of the core business. This survey focused primarily on the first three components. However, all are outlined below for reference.

1. **Strategy.** Risk management begins with the determination of the overall strategies and objectives of the institution and the subsequent goals for individual business units, products, or managers. Once strategies and objectives are determined, the institution can identify the associated inherent risks in its strategy and objectives. Both hazards (negative events such as a major loss that would have a significant impact on earnings) and opportunities (such as new products that depend on taking operational risk) are considered. A firm is then able to set a risk appetite. Specifically, it can determine what risks the company understands, will take, and will manage versus those that should be transferred to others or eliminated. It is the basis for decision making and a reference point for the organization.
2. **Risk policies.** Operational risk management policies are a formal communication to the entire organization about the company's approach to operational risk management. Policies typically include a definition of operational risk, the organizational approach and related roles and responsibilities, key principles for management, and a high-level discussion of information and related technology.
3. **Risk management process.** This process defines the overall procedures for operational risk management, which includes:
    - *Controls*—Definition of internal controls, or selection of alternate mitigation strategy, such as insurance, for identified risks.
    - *Assessment*—Programs to ensure that controls and policies are being followed and determine the level of severity. These may include process flows, self-assessment programs, and audit programs.
    - *Measurement*—A combination of financial and nonfinancial measures, risk indicators, escalation triggers, and economic capital to determine current risk levels and progress toward goals.
    - *Reporting*—Information for management to increase awareness and prioritize resources.
4. **Risk mitigation.** These are specific controls or programs designed to reduce the exposure, frequency, or severity of an event. The controls can also eliminate or transfer an element of operational risk. Examples include business continuity planning, IT security, compliance reviews, project management, and merger integration and insurance.
5. **Operations management.** The day-to-day processes of operations management, such as front- and back-office functions, technology, performance improvement, management reporting, and people management, each has a component of operational risk management embedded in it.
6. **Culture.** There is always a balance between formal policies and culture, or the values of the people in the organization. In operational risk, cultural aspects such as communication, the "tone at the top," clear ownership of each objective, training, performance measurement, and knowledge sharing all help set the expectations for sound decision making.

In addition, the integration with market and credit risk in an enterprise-wide risk management framework is noted, as well as alignment with the needs of the stakeholders—for example, customers, employees, suppliers, regulators, and shareholders.

Operational risk initiatives evolve in five stages. Companies have evolved in their operational risk management practices in a variety of ways depending on the culture and the organization's operational risk event history. Although the surveyed companies had different experiences, after synthesizing the results, we suggest there are five stages in the evolution of operational risk management. Companies beginning the development of their operational risk initiatives will find these stages helpful.

Stage I—Traditional baseline: Operational risks have always existed and are managed by focusing primarily on internal controls. It is the responsibility of individual managers in the business and specialist functions, with periodic objective review by Internal Audit. Traditionally, there is not a formal operational risk management framework, like that discussed in this report.

Stage II—Awareness: Senior management must take an active role in increasing the understanding of operational risk in the organization, and they must appoint someone to be responsible for it. To gain awareness, a common understanding and assessment of operational risks must exist. This assessment begins with the formulation of an operational risk policy, a definition, and development of common tools. The tools in this stage usually include self-assessment and risk process map. In addition, early indicators of operational risk levels and collection of loss events are beginning to be developed. These provide a common framework for risk identification, definition of controls, and prioritization of issues and mitigation programs. However, the most important factor in this stage is gaining senior management commitment and the buy-in of ownership of operational risk at the business unit level.

Stage III—Monitor: After identifying all of the operational risks, it is important to understand their implications to the business. The focus then becomes tracking the current level of operational risk and the effectiveness of the management functions. Risk indicators (both quantitative and qualitative) and escalation criteria, which are goals or limits, are established to monitor performance. Measures are consolidated into an operational risk scorecard along with other relevant issues for senior management.

About this time, the businesses realize that operational risk management process is valuable and assign dedicated staff to analyze processes and monitor activity. An operational risk program may be introduced.

Stage IV—Quantify: With a better understanding of the current situation, it is time to focus on quantifying the relative risks and predict what will happen. More analytic tools, based on actual data, are required to determine the financial impact of operational risk on the organization and provide data to conduct empirical analysis on causes and mitigating factors.

The loss event database, initiated in Stage II, now has sufficient information across businesses and risk types to provide insight into causes and more predictive models. There may be a significant investment in developing capital models and establishment of a new committee to evaluate the results.

Stage V—Integrate: Recognizing the value of lessons learned by each business unit and the complementary nature of the individual tools, management focuses on integrating and implementing processes and solutions. It balances business and corporate values, qualitative versus quantitative, and different levels of management needs. Risk quantification is now fully integrated into the economic capital processes and linked to compensation. Quantification is also applied to make better cost/benefit decisions on investments and insurance programs.

However, this integration goes beyond the processes and tools. In leading companies, operational risk management is being linked to the strategic planning process and quality

initiatives. When this linkage is established, the relationship between operational risk management and shareholder value is more directly understood.

The financial services industry has made considerable progress but is still in the process of implementation. Survey participants rated themselves on the level of maturity of various aspects of their operational risk management framework, using a scale of 1-5. It is apparent from the results that although progress is being made, few think development is mature. The most mature areas are definitions, link to business strategy, and management reporting, yet progress is still needed in these areas. The least mature processes are capital and insurance. It is also recognized that there is no one company that demonstrates all aspects of leading practice. However, some companies are advanced in one or more areas.

The full report examines the roles of management structure and reporting, tools, capital allocation, and other issues in considerable depth. The research confirmed the assumption that the management approach to operational risk is still evolving and too immature for us to point with confidence to a body of best practices.

The research also shows, however, that the technology and practice of operational risk management have developed a startling and rapidly accelerating momentum in the past three years. This represents a window of opportunity for institutions—the leaders have not yet outdistanced the pack. But the very rapid growth in understanding and applying the skills we describe means that this window will not be open long.

This makes it imperative, therefore, for everyone from boards of directors to lines of business management to understand and allocate resources to operational risk, from two perspectives. The first is to protect against the downside, as acquisitions, further expansion into fee-based businesses, and transformation of other risks into operational risk accelerate. The second is to create competitive advantage through quality of process and quality of service. Because of the pervasive nature of operational risk throughout the business, meeting the challenge of this new frontier will require innovative organizational and management approaches. The opportunity is there.

Additional Information:
Charts, tables, and other illustrations available in the printed Journal may not be included in this electronic version. For a paper copy of this article, please contact *hyou@rmahq.org*.