he terrorist attacks on the U.S. immediately changed the risk profile of all institutions. The risks related to business continuity, diversification, and human resources, among others, suddenly jumped in magnitude. These are operational risks, and managing them requires a framework to identify, assess, control, monitor, and mitigate exposures.

In the past five to 10 years, operational risk management has evolved into its own discipline, with specialized staff, policies, measurement, reporting, and related technology. This was reported extensively in RMA’s study, Operational Risk: The Next Frontier. Since that study was published in January 2000, the underlying components have basically remained the same, but their content has continued to evolve and has become more widely accepted as well as more sophisticated. Implementation of a framework is also recommended by the Basel Committee in the proposed new capital accord, and will be required in order to use more advanced capital models.

As outlined in the figure on the following page, an operational risk framework can be summarized as having four components—strategy, process, infrastructure, and environment. Strategy sets the overall tone and approach for risk management. Process describes the steps and decisions for managing risk. Infrastructure identifies the tools used during the management process. Environment refers to culture. Each institution will need to define its own approach and the level of top-down versus bottom-up analysis used in the qualitative and quantitative analyses.

Defining Operational Risk

Any framework must define operational risk. The most common definition, first published in The Next Frontier and also adopted in recent operational risk documents issued by the Basel Committee, is that “Operational risk is the direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events.”1 This definition is a good overall statement, but further refinement is necessary to build an operational risk framework. The approaches used today are categories of operational risk events, complemented by a list of effects that are the types of financial consequences. The Basel documents, developed in consultation with a number of industry experts, uses event categories of internal fraud, external fraud, employment practices and workplace safety, clients/products/business practices, damage to physical assets, business interruption and systems failures, and execution/delivery/process management. It uses effect categories as a basis of quantifying legal liability, regulatory action, loss or damage to assets, restitution, loss of recourse, and write-downs. The important point about these risk categories is to use the same categories throughout all the components of the framework below in order to create a common language and facilitate the aggregation of risk and common reporting.

Strategy

Business objectives. Risk management starts with the definition of business objectives. The level of...
risk and acceptable levels of risk appetite depend on the context set by objectives. Objectives can include business strategy, such as gaining a certain percentage of market share or introducing a new product or technology. Objectives are also stated for internal units, where, for example, a finance organization might have the objective of closing the books each month within five days or identifying a certain amount of cost reductions. Objectives should also include an expression of risk appetite, such as a level of available capital or a maximum level of acceptable earnings volatility.

**Governance model.** The organization model and resulting roles and responsibilities define the approach to operational risk management. Traditionally, operational risk was part of everyone’s job; line and staff roles had to manage their respective operational risks. While the responsibility for risk still rests with line management, there is a new governance model evolving in financial institutions. This model is characterized by having a central Operational Risk Manager, who most often reports to the Chief Risk Officer. The role is one of policy setting, development of tools, coordination, integration and aggregation of the risk profile. For example, the Operational Risk Manager would set out the common definitions for operational risk; develop and facilitate the implementation of common risk management tools such as risk maps, self-assessment programs, and loss event databases; and develop measurement models, such as the economic capital model, that cross organizational boundaries and functions.

Line management remains responsible for the day-to-day risk management activities, since it is the business areas that face the customer, introduce products, manage the majority of people, operate processes and technologies, and deal with other external exposures. In addition, staff organizations like Human Resources, Information Technology, Security, Legal, and Finance develop specific policies and procedures, monitor emerging risks, and advise the organization on risk as it applies to their areas of expertise.

Operational risk units are often complemented by risk committees. The role of the risk committee is to understand the risk profile, ensure resources are properly allocated, assure risk issues are addressed, and approve policies, including capital allocation.

The definition of this governance model will need to define the roles, authority levels, and accountabilities of each involved organizational component. Any organizational model needs to be accompanied by the right people. The right skills base, combined with a training program for both operational risk staff and other affected people in the organization, becomes an important consideration for success.

**Policy.** Corporate policy sets the overall strategy for operational risk management. Organizations should have an operational risk policy statement that describes the approach for the institution. This policy statement would typically include the common definitions and categories for operational risk and a description of the operational risk framework as described in this article. The policy might also include

---

**Diagram Description:**

The diagram illustrates the operational risk management framework. It includes the following components:

- **Strategy**
  - Objectives
  - Governance Model
  - Policy

- **Process**
  - Risk Identification
  - Control Framework
  - Assessment
  - Monitoring and Measurement
  - Reporting

- **Validation/Reassessment**

- **Infrastructure**

- **Environment**

---
some core risk management principles that set the tone at the top and desired cultural characteristics. A successful operational risk management framework requires some cultural characteristics that are contrary to the way that some organizations have historically operated. One principle, for example, is openness and transparency. We have to create an environment where people can share their concerns and operational weaknesses without fear of repercussions. The same is true for pending or actual loss events. Events become opportunities to improve, rather than an opportunity to shoot the messenger.

**Process**

The following are the key steps in any risk management process. They describe the day-to-day activities required to understand and manage operational risks. The risk process applies to a transaction, to an initiative, to operations like a back office, and to a periodic, more formal process such as risk and control self-assessment.

**Risk identification.** In the context of business objectives, what are the risks incurred? The definitions of operational risk provide a broad context for potential exposures. Risk identification creates a risk map detailing which of these risks applies to any one business, process, or organizational unit and to what degree. The identification process may also expand the definitions to identify more specific risks applicable to any one business that are not clearly spelled out in the definitions. For example, fiduciary risk is specifically identified in the definition above, but would be a large operational risk exposure for a private banking business.

**Control framework.** For any type of risks, what are the desired controls that apply? In other words, how do we control or mitigate each of the risks that are incurred? The definition of controls is broad. For example, typical controls include management oversight, information processing, activity monitoring, automation, process controls, segregation of duties, performance indicators, and policies and procedures. Other types of controls can include training, insurance programs, diversification, and outsourcing.

**Assessment.** Assessment processes provide the organization with an objective process to determine “How am I doing?” That is to say, what are the exposures, how well are we controlling them, what are the potential weaknesses, what should we be doing to improve, who is responsible for these actions, and what is the plan to accomplish them? Assessments, often called control self-assessment, or CSA, take on different forms. Some rely on completion of very detailed questionnaires about all the desired controls, while others provide more open-ended questions of a general nature. Another approach is to let businesses define their own set of risks and controls. Workshops are also used to brainstorm the issues and get alternate points of view. Parts of the assessment process include the accumulation of issues identified, whether through the assessment process, internal/external auditors, regulators, or other sources.

**Measurement and monitoring.** The process here is to determine how large or small the exposures are, whether controls are working properly, and whether exposures are changing and subsequently require attention.

Measurement of operational risk takes on various forms. Some of the key types are:

- **Risk drivers.** These are items that could change the overall profile of risk in the organization. They include volumes, people turnover, productivity levels, market volatility, product maturity/complexity, or any other primary factor.
- **Risk indicators.** These are the more specific ratios to monitor the effectiveness of the controls and the risk profile of any one area. Escalation criteria are set to trigger review by higher levels of management. Indicators are one tool used to keep risk profiles current and complement the more periodic nature of self-assessments. Sample indicators include the number of unreconciled accounts, aged confirmations, status of training plans, and late projects.
- **Loss history.** Leading institutions develop databases that accumulate a history of operational risk losses. They may also record the near misses and pending issues. The results yield the amount of
the operational risk costs as well as an empirical analysis of where they occur—the control point, the product, and items that repeat. A loss history provides information on the “expected losses” for operational risk involving budgeting and pricing. Analysis of this data forms one element of the value proposition for risk management and is a source for determining mitigating actions.

- Capital models. Quantifying economic capital is the expression for “unexpected losses.” There are various approaches to capital models, but as confirmed by the proposed new Basel rules, the advanced models are based on a history of loss events and developing distributions of frequency and severity of loss.

    The monitoring process helps management understand the current risk profile, how it is changing and what should be given attention. One element of monitoring is to watch the quantitative measures described above and the resulting trends. Another type of monitoring is to follow the assessment processes. Are they being performed in a timely manner? Are the right people participating and what do the results indicate? Also, are the resulting corrective action plans being executed and completed according to plan?

    We also monitor the external environment and industry trends. New risks emerge every day. Even if not new, risks may take on a new dimension. Internet security, privacy, patent risks, and discrimination are a few examples of exposures that have increased dramatically over the past few years.

    Reporting. Reporting is applicable at all levels of the organization, and the content and frequency of information must be tailored to the business area and recipients. A key objective is to communicate the overall profile of operational risk across business areas and types of risk. Reporting communicates the overall level of risk and the key trends, highlighting exceptions for particular attention. Some of the information that should be communicated includes self-assessment results with a comparison of risk levels by risk type across the organization, major operational risk events and trends of losses, key indicators and exceptions where escalation criteria have been hit, external news or events worthy of monitoring, status of major projects or initiatives that impact the risk profile, and capital levels by risk type with trends and explanation of movements.

Infrastructure

    A complement of tools is used to facilitate the entire risk management process. Two of these tools—systems and data—are particularly important. We find systems used to facilitate and aggregate self-assessment programs, databases to collect and aggregate risk indicators and loss event data, and other systems to facilitate specific control programs such as project management, insurance claims, insurance claim tracking, and security. Infrastructure may also refer to policies/procedures and specific measurement methodologies.

Environment

    Environment—the surroundings that set the tone and behavior of the organization—starts with “tone at the top.” Risk management needs the support and involvement of senior management, who can set the tone that operational risks are important and deserve attention and allocate resources accordingly. Senior management can set the values of the organization as well as communicate the goals for risk management and the organization’s risk appetite.

    Performance measures set expectations for management. The environment should not create incentives to increase unnecessary risk-taking. Rather, it should reinforce integrity and ethics.

Conclusion

    As institutions begin to implement an operational risk framework, they need to address several key challenges. They need to articulate the overall value proposition and how to justify the incremental resources. They need to find ways to make process continuous and dynamic. A they need to link a corporate framework with common definitions of business and individual risks, yet meet the needs of a consolidated risk profile.

Notes