Achieving *Excellence* in Operational Risk Management: A Corporate Staff Perspective

By Joseph A. Sabatini

In the past few years, many large and mid-sized financial services firms have established a new corporate staff function whose role is described generally as operational risk management. Some have undertaken this initiative simply as a response to the emerging rules under the Basel II proposal. Others directly stake claim to the noble objective of enhancing their risk management practices with the intention of improving the financial performance of their firm. Whatever the origin, it is clear the industry has embarked on an ambitious and unchartered journey of bringing a systematic and holistic perspective to the subject of operational risk.

Key to the success of a systematic and holistic approach to operational risk is the role and scope of the corporate staff function and its ability to add incrementally to a firm's risk management effort. Clearly, the role of a centralized risk function for credit and market risk has long been an industry standard and is considered fundamental to managing these risks successfully in a large financial enterprise. Does a similar approach to operational risk offer the same opportunity? And will such a function add to our understanding of this risk class?

Given the large and varied operational risk losses of the past few years, the appeal of improving this aspect of our risk management capability is more than axiomatic. Yet, the very premise of a corporate staff function called Operational Risk Management appears oxymoronic.

Is there a unit farther removed from operational risk in a large financial company? Rather than providing insight, is not the opposite more probable? Will the effort become the victim of the many unintended consequences of corporate bureaucracy? These are indeed valid concerns as we consider the role of a corporate operational risk staff function.

Before we rush off with one more lemming-like initiative for our industry, we should examine some fundamental aspects of operational risk and the role a corporate staff function may be able to play productively:

1. We should understand the unique aspects of operational risk, especially relative to credit and market risk.
2. Given the nature of operational risk, we should define the appropriate role a corporate operational risk staff function can legitimately serve.
3. Lastly, we should determine what measures exist today that can be used to monitor our progress.

The Nature of Operational Risk

At the outset, it is important to understand the nature of this risk type and the fundamental differences from its more established siblings, credit risk and market risk. The definition of operational risk alone hints that the scope of this risk class may be the first challenge. Conceived by various industry working groups and sanctioned by different regulatory statements, an industry consensus has developed around the following definition:

Operational risk is the risk of loss resulting from inadequate or failed processes or systems, human factors, or external events.

While this may be a slight improvement on the traditional view that operational risk is

© 2006 by RMA. Joseph Sabatini is a managing director and the head of the Corporate Operational Risk Team for JPMorgan Chase.

"everything but credit risk and market risk," the first observation one can easily make is that the breadth of this definition remains beyond the risk expertise of any individual or small collective team. Granted, this may also be true for credit and market risks in large, diversified financial services firms, but aspects of operational risk exist where differences are even more pronounced. Early practitioners in this space would agree that the development of operational risk management as a true risk discipline is handicapped by these characteristics:

1. No established risk language.
2. An undefined population of risk takers and risk processes.
3. Ancillary versus permissioned risk taking.

Language of risk. Unlike credit risk or market risk, there is no established language that operational risk specialists and business managers can use to describe and communicate issues and trends, or provide an overall picture of the health of a firm's control environment. We are reduced to communications revolving around specific events such as losses or near misses, audit or examination findings, and other anecdotes. Few, if any, data points provide trend information across even a small portfolio of risk issues. Simple benchmarking of one business against another by risk category is beyond our grasp, and we can only dream of a time when comparisons against peer institutions are the norm.

Today, does any business manager truly know the quality of his or her control environment relative to competitors? The absence of usable metrics and benchmarks significantly diminishes our ability to have defined performance standards. Such capabilities and measures are not only commonplace in credit and market risk, but in many respects are considered essential to the management of those risks.

Undefined population of risk takers and risk processes. A second obvious characteristic of operational risk is the absence of a defined population of risk takers. From the mailroom to the executive office, everyone in the firm incurs or generates operational risk of one nature or another in the execution of their daily responsibilities. Moreover, the usual orientation for operational risk managers is along business and organizational hierarchies. The importance of understanding operational risk as an end-to-end process has only recently become readily apparent. Adjusting our approach to a horizontal end-to-end view is a considerable challenge, especially in an environment dominated by a vertical business hierarchy that mirrors how we manage and measure business performance. Given the breadth of this risk class, it is easy to understand the challenges associated with organizing an effort to identify, monitor, manage, and improve operational risk in a disciplined, well-informed manner.

Operational risk is not permissioned. A natural progeny of these characteristics is the fact that taking operational risk is not a directly permissioned activity in the same manner as credit or market risk. Rarely is it a conscious "go" or "no-go" decision to incur a known amount of operational risk. The risk is a subtle by-product of our day-to-day business activities. For most businesses, operational risk is not explicitly measured and priced into a product or service. Indeed, it is presumed that the control environment is more than adequate and that upstream and downstream systems and processes will perform as expected. While some institutions are experimenting with the calculation and management of operational risk limits, the efficacy of such an approach appears dubious in today's context.

Role of the Corporate Operational Risk Function

If the above reasonably characterizes the general nature of operational risk, and some of the critical differences between this risk class and credit and market risk, there are significant implications for the role and responsibilities of a corporate staff function. Clearly, the norm in the credit or market risk functions of a large institution is a command-and-control, centralized operating model that serves to establish limits and approve certain transactions. Yet an authority-driven model that permissions operational risk taking not only is inappropriate, but would arguably be counterproductive in a large, diversified financial institution.

This is not to say that the corporate function should have no ultimate decision-making authority. The challenge is that an operational risk corporate staff function generally needs to find balance as an authority model, a partnership model, and a client service model. Achieving this balance in a manner consistent with an individual firm's overall governance and risk

culture is difficult.

Authority model. Certain aspects of a firm's operational risk agenda are appropriately within the defined authority of the corporate staff function. These would include, for example, overseeing the design and implementation of corporate policy and standards for operational risk governance, data requirements, and reporting. In addition, regulatory initiatives generally are best managed and communicated on a centralized and consistent basis within established requirements and processes clear to all businesses. This is particularly true given the ambitious nature of the new Basel II proposals and Sarbanes-Oxley Section 404 requirements. Capital measurement and allocation are a third example where centralized authority is well suited. Of course, each firm will organize its central functions differently, and there is no single blueprint for everyone. What is essential, however, is that the lines of authority are clear to all wherever they may be drawn.

Partnership model. Other aspects of the operational risk framework and initiatives are best pursued in a partnership approach between a centralized staff function and the wider business and user community. Examples of this include the selection and coordination of investments in technology or processes that can be scaled across businesses and all user groups. Decisions in these areas are often best made by actual users and in-business risk managers. By the same token, a corporate perspective is also required to ensure appropriate standardization and coordination across the firm. Consideration of regulatory requirements or industry best practices may not be readily known to business units. Partnership here is essential to ensure that decisions taken are relevant to business needs, but also avoid the needless proliferation and added costs of fully decentralized initiatives.

Client service model. A universal truth is that operational risk is best understood, owned, and managed where it is generated. As the firm-wide operational risk agenda progresses from design and implementation into an established business process, the corporate staff function needs to orient itself primarily to a client service model. If the overall objective of a corporate staff unit is to improve the management of operational risk and, by implication, the financial performance of businesses, our focus needs to be on enhancing the tools and capabilities of our business and risk managers. The blocking and tackling of our effort becomes that of providing our clients with user-friendly tools that offer meaningful and actionable data and information related to the control environment.

The equation is simple. Collecting accurate, timely, and meaningful data is the foundation. Requiring and providing transparency, as well as escalation of key issues and information, feed an effective governance program that ensures accountability for follow-up and remediation. This effort companies our collective arsenal on the operational risk front. Done properly, this work leads to cost-efficient, business-driven processes that result in continuous self-improvement in the control environment. The role of a corporate staff function is to facilitate such an environment, not to manage it.

As with any newly established unit, the role and responsibilities of a corporate operational risk function will emerge from the interactions with the broad user community as much as from being defined by corporate policy. A major challenge for us is to serve simultaneously as an authority, a partner, and a client service provider to our business colleagues—and be able to move between these roles with ease, credibility, and acceptance.

Measuring Success

An age-old question for most staff functions is how to measure success. What is an appropriate scorecard to track effectiveness? If this is a challenge for established staff groups, it is a much more daunting task for a newly formed corporate operational risk function. As indicated previously, the value of the effort at the corporate level is not immediately self-evident, and compounding the problem is the lack of historical or baseline data against which to measure future performance.

Moreover, even if this base data did exist, what portion, if any, of the change in performance in future periods should be ascribed to the corporate function versus efforts in the lines of business or external or other factors? This is a dilemma for all such corporate functions that truly desire to operate beyond the limited scope of minimum regulatory requirements. Yet incremental investments above minimum requirements need to be

justified on some measure, even a qualitative one.

While the road ahead is not clear, there are certain points of focus and early signs of success to watch for as we set out on this journey. An initial observation is to avoid "playing the regulatory card." No doubt the strong appeal of the Basel II Advanced Measurement Approach is the convergence of regulatory and risk management principles and practice. However, to label the nascent operational risk function as a regulatory requirement may doom the effort to a compliance-oriented initiative, and marginalize our ability to become an integral part of a firm's mainstream risk management disciplines. We will be much more successful over the intermediate and long term if we earn our credibility on the tougher path of enhancing risk management.

No doubt early efforts here will be given a honeymoon period. Ultimately, however, the effort will have to demonstrate value to the firm in some manner. In the absence of a definitive scorecard, we need to rely on 1) key characteristics we believe are fundamental to the understanding of operational risk, and 2) early signals from our internal user community as indications of progress.

Characteristics of a successful program. As highlighted earlier, one role of the corporate function is to design and implement a framework that will facilitate the understanding of key risk drivers. Experience has taught us that a few critical attributes to this framework are required for success.

1. We have learned that no large loss event is the result of a single point of failure. Forensic analysis has repeatedly taught us that large losses result from multiple points of failure happening simultaneously, or in sequence, across seemingly unrelated activities. Again, it is worth emphasizing that an end-to-end view and understanding of operational risk is a bedrock capability that needs to be designed into any framework.
2. Integration of various components of the framework is also valuable. The ability to assess, view, and report loss events, self-assessment issues, and audit grades on an integrated basis, readily linked with corporate reference data and internal business reporting, is a feature valued by business users and risk managers.
3. Incentives are critical. Linking risk measures to capital and economic value introduces the concept of the "cost of risk." Businesses held accountable for performance measures that include a cost of risk (or cost of capital) are properly and directly incented to manage their control environment in a disciplined and robust manner.
4. We need to ensure the effort reduces operating costs and reporting burdens for end users. The fully loaded costs associated with self-assessment, loss data collection, capital modeling, reporting, and efforts related to Sarbanes-Oxley and Basel II are substantial. Ironically, we benefit from the reality that legacy processes and systems for tracking and reporting operational risk issues are heavily manually intensive across the industry. Standardizing the methodologies where appropriate, leveraging and scaling technology, and facilitating user requirements can result in significant cost savings alone without any improvement in the management of operational risks.

Early signs of success. Two telltale signs will provide early indications of progress. The first is the "demand-pull" factor. Are businesses engaged proactively in the design and development of the operational risk framework? Are they shaping the framework based on their specific needs and requirements? Are they using the data generated as primary inputs into the risk governance process? Do they believe the data to be accurate?

If the answer to these questions is affirmative, the opportunity for success is at hand. Regulatory documents refer to the "use test" standard. The same measure applies to the efforts of the corporate operational risk function. If businesses "use" the framework, tool set, and data for primary risk management, an effective framework is in place and a winning partnership between the corporate function and business community has been forged. As a corporate risk function, "demand-pull" is a winning environment.

The second sign of real progress is the ability of the framework and process to identify control gaps before surprises occur. The bane of our industry is that losses, near misses, examinations, and audit findings often come as surprises to business and risk managers. Lowering the frequency of these surprises is the ultimate

measure of effectiveness. Credit risk managers have demanded a "no surprise" environment within their risk discipline for generations. Developing and maintaining a similar environment for operational risk need to be our most urgent objectives. Lowering the percentage of negative events that are surprises over time is an infallible measure of success.

Finally, a comment on "excellence." Risk managers like to speak in terms of excellence—sometimes real, sometimes aspirational. There is a great opportunity at hand for our industry. We are experiencing a rare convergence of need and capability, and a partnership is forming between risk managers and businesses as well as regulators and financial services firms, to develop and achieve a new vision in operational risk management. Remarkable progress has already been demonstrated. Yet much work remains before we can claim our standing as a first-class risk discipline. For corporate operational risk functions, "excellence" is aspirational, but it is certainly within our reach. ❒

Contact Joseph Sabatini by e-mail at
sabatini_joseph@jpmorgan.com