Operational Risk Management: An Evolving Discipline

Operational risk is not a new concept in the banking industry. Risks associated with operational failures stemming from events such as processing errors, internal and external fraud, legal claims, and business disruptions have existed at financial institutions since the inception of banking. As this article will discuss, one of the great challenges in systematically managing these types of risks is that operational losses can be quite diverse in their nature and highly unpredictable in their overall financial impact.

Banks have traditionally relied on appropriate internal processes, audit programs, insurance protection, and other risk management tools to counteract various aspects of operational risk. These tools remain of paramount importance; however, growing complexity in the banking industry, several large and widely publicized operational losses in recent years, and a changing regulatory capital regime have prompted both banks and banking supervisors to increasingly view operational risk management (ORM) as an evolving discipline. Of particular note is the application of quantitative concepts, similar to those used to measure credit and market risks, to the measurement of operational risk.

This article provides an introduction to operational risk, outlines the current state of ORM, and describes different quantification approaches in this evolving field.

Operational Risk Defined

The definition of operational risk continues to evolve, in part owing to its scope. Before attempting to define the term, it is essential to understand that operational risk is present in all activities of an organization. As a result, some of the earliest practitioners defined operational risk as every risk source that lies outside the areas covered by market risk and credit risk. But this definition of operational risk includes several other risks (such as interest rate, liquidity, and strategic risk) that banks manage and does not lend itself to the management of operational risk per se. As part of the revised Basel framework,[1] the Basel Committee on Banking Supervision set forth the following definition:

> *Operational risk* is defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

While the Basel Committee's definition includes what the Committee considers to be crucial elements, each bank's definition for internal management purposes should recognize its unique risk characteristics, including its size and sophistication, as well as the nature and complexity of its products and activities. In cooperation with industry participants, the Basel Committee has identified the seven operational risk event types, shown in Table 1.[2]

An Evolving Banking Landscape

The operational environment for many banks has evolved dramatically in recent years. Deregulation and globalization of

[1] Basel Committee on Banking Supervision (Basel Committee), *International Convergence of Capital Measurement and Capital Standards* (the revised Basel II framework), November 2005, Paragraph 644. Available at www.bis.org/publ/bcbs118.htm.

[2] The event types and abbreviated examples presented in the table appear in the Basel Committee's *Sound Practices for the Management and Supervision of Operational Risk*, Paragraph 5. Available at www.bis.org/publ/bcbs86.pdf.

Table 1

Loss Event Types and Examples

Event Type	Examples
Internal fraud	Employee theft, intentional misreporting of positions, and insider trading on an employee's own account
External fraud	Robbery, forgery, and check kiting
Employment practices and workplace safety	Workers' compensation and discrimination claims, violation of employee health and safety rules, and general liability
Clients, products, and business practices	Fiduciary breaches, misuse of confidential customer information, money laundering, and sale of unauthorized products
Damage to physical assets	Terrorism, vandalism, earthquakes, fires, and floods
Business disruption and system failures	Hardware and software failures, telecommunication problems, and utility outages
Execution, delivery, and process management	Data entry errors, collateral management failures, incomplete legal documentation, and vendor disputes

financial services, the proliferation of new and highly complex products, large-scale acquisitions and mergers, and greater use of outsourcing arrangements have led to increased operational risk profiles for many institutions. Technological advances, including growth in e-banking transactions, automation, and other related business applications also present new and potentially heightened exposures from an operational risk standpoint.

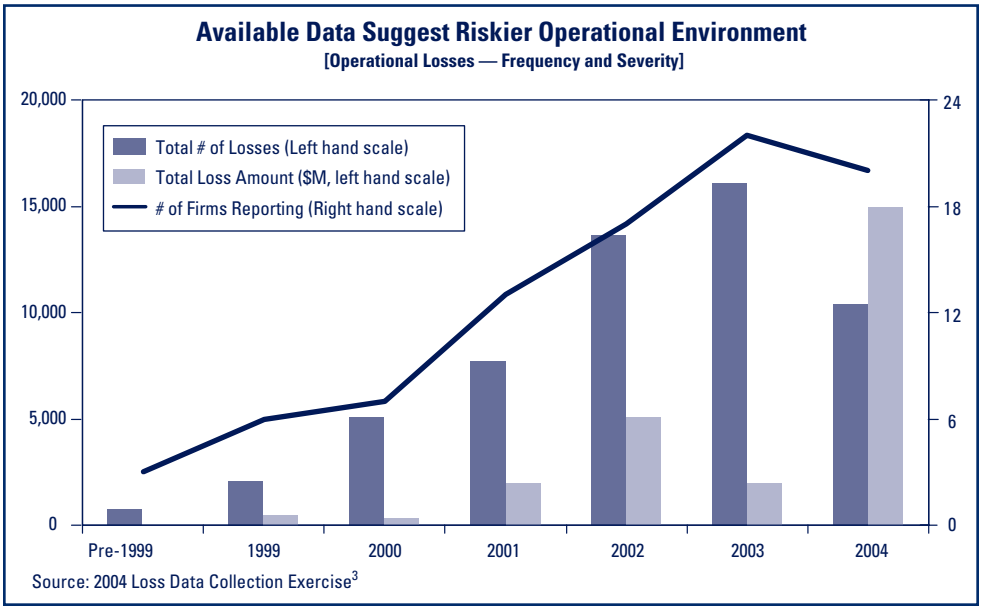
Available data support the idea that banks' operational environments are getting riskier. Chart 1 depicts data gleaned from the 2004 Loss Data Collection Exercise (LDCE)[3] conducted in preparation for the U.S. implementation of the Basel II capital framework. Despite certain inherent limitations in the data, such as differences in data availability among the reporting banks and improvements in data capture methods over the collection period, it appears that in aggregate loss amounts have increased since collection efforts began. For example, 20 participating banks reported operational losses of $15 billion in 2004, surpassing the previous high of $5 billion in losses reported by 17 institutions in 2002.

Losses associated with operational risk events can be large. Some well-known examples are the collapse of Barings Bank due to fraudulent trading and the substantial legal settlements entered into by Citigroup and JPMorgan Chase with regard to the Enron and WorldCom matters. The business disruptions and financial impacts resulting from Hurricane Katrina and the September 11 terrorist attacks also exemplify how major, unforeseen events can materially affect a bank's operations.

[3] The 2004 LDCE was a voluntary survey that asked respondents to provide data on individual operational losses through June or September 2004 to enable the banking agencies to assess the potential impact of Basel II on capital for U.S. banking organizations. The results of the survey can be found at www.bos.frb.org/bankinfo/qau/pd051205.pdf and www.bos.frb.org/bankinfo/conevent/oprisk2005/defontnouvelle.pdf. Additional information regarding the LDCE is at www.ffiec.gov/ldce.

continued from pg. 5

Chart 1



Controlling Operational Risk

Traditional ORM practices, which most banks employ today, rely on internal processes, audit programs, and insurance protection to counterbalance operational risk. They are based largely on the assumption that intelligent, educated people can, through their intuition, identify their organization's significant risks, corresponding controls, and associated metrics.[4] In such environments, business lines manage their operational risks as they see fit (using a "silo approach") with little or no formality or process transparency.

Some larger banks have gone beyond the silo approach by establishing centralized departments or groups responsible for focusing on particular segments of operational risk, such as operating processes, compliance, fraud, business continuity, or vendor management/ outsourcing. While this evolution has improved overall risk awareness, it tends to promote a natural segmentation of risk awareness, because risks are categorized along functional lines. This approach can create significant operational risks if management fails to consider end-to-end processes.[5]

More recent ORM practices are founded on the view that intuition alone is not sufficient to drive the ORM process. In this view, ORM practices must extend to quantitative measurement, including historical loss data, formal risk assessments, statistical analysis, and independent evaluation.[6]

A common framework at the largest U.S. banks combines the traditional silo approach with an enterprise-wide oversight function. The enterprise-wide (or corporate) function designs and implements the bank's ORM framework, which serves as the structure to identify, measure, monitor, and control or mitigate operational risk. The framework is defined by the risk tolerance determined by the board of directors, as well as the

[4] Ali Samad-Khan, "Fundamental Issues in OpRisk Management," *OpRisk & Compliance*, February 2006.

[5] Eric Holmquist, "Scaling Op Risk Management for SMIs: How to Avoid Boundary Disputes," *OpRisk & Compliance*, January 2006.

[6] Ali Samad-Khan, "Fundamental Issues in OpRisk Management."

formal operational risk policies outlining roles and responsibilities, data standards, risk assessment processes, reporting standards, and a quantification methodology.[7] Business line managers continue to "own the risk," but risks are identified through formal self-assessments. The risk assessments are designed to capture end-to-end processes as well as generate an understanding of the risks in individual processes and products. Table 2 compares the two approaches to ORM.

The primary value of such ORM techniques, as demonstrated by a growing number of institutions using them, is their application to decision making and risk management. Specifically, the use of a well-integrated ORM framework can do the following:

- Increase risk awareness and mitigation opportunities, which may minimize potential exposure
- Assist in evaluating the adequacy of capital in relation to the bank's overall risk profile
- Enhance risk management efforts by providing a common framework for managing the risk

Quantifying Operational Risk: Roots in Economic Capital

As ORM continues to evolve into a distinct discipline, efforts to quantify operational risk have gained momentum. A number of large financial institutions have been working to quantify operational risk for several years as part of their economic capital frameworks. They have developed and implemented economic capital models to allocate capital to different business segments based on a variety of risk factors (e.g., credit, market, interest rate, operational). However, within these internal capital measurement and management

Table 2

Comparison of Traditional and Modern Operational Risk Management[8]

Traditional Practice	Emerging Practice
"Silo-ed" business unit risk management	Integrated corporate risk management (CRM)
Business line managers "own the risk"	CRM supplements and reinforces business line risk ownership
Ad-hoc or no risk self-assessment	Uniform risk assessments across business units facilitated by CRM
Voluminous performance indicators	Core set of key risk and performance metrics/escalation triggers
Too much or too little information; inconsistent business unit reporting	Concise, uniform reporting to senior management and the board of directors
Reliance on qualitative processes to improve risk management	Use of quantitative information (potential operational risk exposure) and risk assessments to improve risk management

[7] The Basel Committee, *International Convergence of Capital Measurement and Capital Standards*, Paragraph 663(b).

[8] Table adapted from *Operational Risk: Regulation, Analysis, and Management* by Carol Alexander (2003), p. 15. Financial Times Prentice Hall. London.

continued from pg. 7

processes, there is great variation in methods used and levels of sophistication, ranging from largely qualitative or judgmental approaches to complex statistical modeling. With respect to operational risk, in particular, many of the measurement techniques have traditionally focused on proxies such as gross income to estimate capital allocations.

While few institutions have incorporated operational risk quantification systems into their economic capital models, ongoing work in this area is becoming increasingly important given the anticipated implementation of a new regulatory capital framework known as Basel II. This new framework, which has been under development since the late 1990s and is approaching international adoption, is intended to align capital levels more closely with underlying risks. This general intention is consistent with the broad goal of most economic capital frameworks.

Operational Risk Becomes Part of Regulatory Capital

Under the Basel II framework, institutions (both mandatory and opt-in)[9] will be required to determine an appropriate operational risk charge, along with credit and market risk charges, as part of their risk-weighted assets (RWA) calculation. Each institution's estimate of its operational risk exposure will, subject to supervisory approval, directly affect its risk-based capital (RBC) ratio.

Under the existing regulatory capital regime (Basel I), which was adopted in 1988, there is no explicit charge for operational risk. In determining RBC ratios, financial institutions calculate RWA on the basis of prescribed percentage allocations for on- and off-balance sheet credit exposures and for certain market risks. It could be argued that operational risk and other risks were implicitly accounted for in the calibration of the minimum ratio thresholds for the various Prompt Correction Action categories[10] (e.g., 4 percent Tier 1 capital to average adjusted balance sheet assets for the "Adequately Capitalized" designation), but they are not considered in determining a bank's capital ratios.

Quantifying Operational Risk

The Basel II framework outlines three quantitative approaches (shown in Table 3) for determining an operational risk capital charge: the basic indicator approach, the standardized approach, and the advanced measurement approach.

The first two approaches are simple and generate results on the basis of predetermined multipliers (percentages of gross income[11] for an entire entity or for individual business lines). The advanced

[9] As noted in the August 2003 Advanced Notice of Proposed Rulemaking (ANPR), the Basel II framework in the United States applies to large, internationally active banking organizations. Mandatory banks are defined as those with total assets of $250 billion or more or total on-balance-sheet foreign exposure of $10 billion or more. Such banks must apply advanced credit risk and operational risk approaches. Banks not subject to advanced approaches on a mandatory basis ("opt-in" banks) may voluntarily apply those approaches. The ANPR is available at www.fdic.gov/regulations/laws/publiccomments/basel/index.html.

[10] The ratio thresholds for the Prompt Corrective Action categories are included in Subpart B of Part 325 of the Federal Deposit Insurance Corporation (FDIC) Rules and Regulations. Subpart B, issued by the FDIC pursuant to section 38 of the Federal Deposit Insurance Act, establishes a framework of supervisory actions for insured depository institutions that are not adequately capitalized. This subpart is available at www.fdic.gov/regulations/laws/rules/2000-4500.html#2000part325.101.

[11] Gross income is defined in Paragraph 650 of the revised Basel framework as net income plus net noninterest income. This measure should be gross of any provisions (e.g., for unpaid interest); be gross of operating expenses, including fees paid to outsourcing service providers; exclude realized gains and losses from the sale of securities; and exclude extraordinary or irregular items, as well as income derived from insurance. The calculations for the basic indicator and standardized approaches are based on average gross income figures over a three-year period, excluding periods in which gross income is negative or zero.

Table 3

Basel II Approaches to Calculating Operational Risk Capital

Basic Indicator Approach	Standardized Approach	Advanced Measurement Approach (AMA)
Supervisor-specific parameters Bank-wide measure Exposure indicator based on gross income (15 percent multiplier)	Supervisor-specific parameters Business line measure Exposure indicator based on gross income (multipliers vary by business line and range from 12 percent to 18 percent)	Bank-defined parameters Supervisor establishes quantitative and qualitative standards Significant flexibility Examples: • Loss distribution approach • Scenario based • Extreme value theory

measurement approach (AMA) differs from the other two approaches in that it explicitly attempts to estimate a bank's operational risk exposure (aggregate operational losses faced over a one-year period) at a soundness level consistent with a 99.9 percent confidence level.[12] That is, in theory there should be only a 1-in-1,000 probability that a bank's operational losses during a year will exceed the AMA-estimated amount. Despite the statistical challenges, banks typically select a confidence level between 99.96 percent and 99.98 percent for economic capital modeling, which is generally equivalent to the expected insolvency rate for "AA" rated credit.

Banks adopting an AMA will effectively calculate operational risk capital using a value at risk (VaR) approach common in both market risk and credit risk management. The U.S. banking agencies have not mandated the use of any particular quantitative methodology; however, each institution employing an AMA must use the following four elements in arriving at its operational risk capital estimate: internal data, external data, scenario analysis, and business environment and internal control factors.

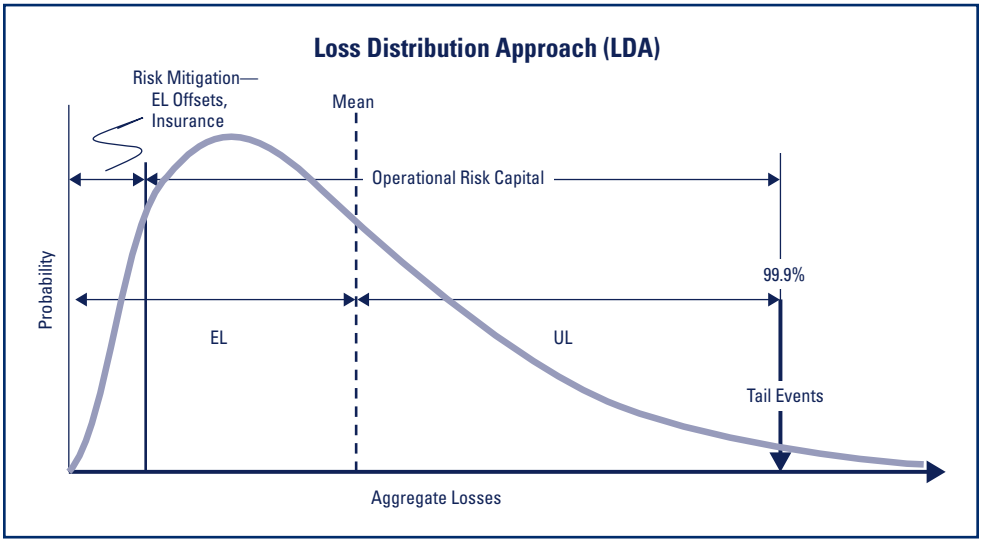
Conceptually, the operational risk capital estimate can be expressed as protection against expected and unexpected future losses at a selected confidence level, with some provisions for offsetting portions of this exposure through reserves or other permitted mitigation techniques (namely insurance). This relationship is reflected graphically in Chart 2 using the loss distribution approach (LDA), a common quantification method.

Expected losses (EL) are reflected on the chart as the portion to the left of the dotted line marking the mean of the distribution. The dotted line represents the mean or expected value of the aggregate distribution of potential losses. Loss

[12] As noted in the August 2003 ANPR, the AMA will be the only permitted quantification approach for U.S.-supervised institutions (neither the basic indicator nor standardized approaches will be allowed).

continued from pg. 9

Chart 2



levels falling in the EL category are typically highly predictable and stable, and generally arise under normal operating circumstances. Banks may potentially use capital-like substitutes (such as eligible reserves per Generally Accepted Accounting Principles) or other conceptually sound methods to offset some portion of EL.

Unexpected losses (UL) on the chart are the area to the right of the dotted line. Migrating to the far right of the UL category (or the tail of the distribution) provides an increasingly high level of confidence that the estimate captures the appropriate degree of severity.

The Loss Distribution Approach

The LDA, or a hybrid thereof, has emerged as the most common statistical method to estimate a bank's operational risk exposure. Through the LDA, banks combine the four AMA elements with appropriate qualitative and quantitative adjustments to derive their operational risk exposure estimates.

Example: A global institution has five major business lines, one of which is the consumer banking group (CBG). For simplicity we will consider only one business line, which is equal to the bank's unit of measure.[13] CBG has collected 25,000 loss events over the past five years, with the majority defined as high-frequency, low-severity events. To understand its full exposure over the next year, the CBG will consider risks (both internal and external) that may not be represented in the internal data. For example, over the last year, several banks in the same business line have been sued for breaches of customer information and have settled for sums in excess of $1 billion. Additionally, the CBG has developed new product offerings and acquired several banks during the year. The business line should consider this information either by using external loss data directly or by using the information to develop scenarios. The data from these sources are combined using statistical methods to estimate operational risk exposure. The CBG should also incor-

[13] A unit of measure represents the level at which a bank's operational risk quantification system generates a separate distribution of potential operational losses. For example, a unit of measure could be represented by a business line, loss event types, or a combination of both.

porate changes into its residual risk (inherent risk less controls), as well as any risk mitigation offsets.

Quantification Challenges

Ongoing supervisory reviews and other recent industry studies indicate that progress has been made in quantifying operational risk. However, major challenges remain, particularly with respect to addressing problems resulting primarily from data paucity. The primary quantification issues are as follows:

- Properly identifying units of measure
- Collecting adequate data (regarding frequency and severity) for each unit of measure
- Calculating statistically significant parameters for each loss distribution
- Describing dependencies across units of measure if there is to be any diversification effect
- Determining how to incorporate and weigh each of the four required AMA elements within the modeling framework

ORM — Unique to Each Bank

Operational risk has emerged as a distinct discipline in response to Basel II, the increasing number of large operational losses, and the growing size, sophistication, and complexity of the banking industry. Regulators expect banks that adopt Basel II to develop and implement comprehensive ORM, data and assessment, and quantification processes that are appropriate to the nature of their activities, business environment, and internal controls.

The proposed operational risk capital rules and supporting guidance[14] establish broad regulatory expectations while enabling each bank to tailor its framework to its unique organizational structure and culture. The embedded flexibility will require regulators to exercise considerable judgment as they consider the appropriateness of the chosen ORM framework.

The vast majority of banks will continue to calculate regulatory capital under Basel I or Basel I-A (proposed)[15] guidelines, neither of which has an explicit operational risk capital component. Nevertheless, many of the risk management principles being employed by the largest U.S. banks can be used to some degree by any institution regardless of size. The fundamental goal is the same: increasing operational risk awareness and determining the means to minimize the institution's potential exposure.[16]

Alfred Seivold
Senior Examination Specialist, San Francisco

Scott Leifer
Examination Specialist, Boston

Scott Ulman
Senior Quantitative Risk Analyst, Washington, D.C.

[14] The proposed operational risk capital rules are contained in the August 2003 ANPR. In conjunction with the ANPR's issuance, the U.S banking agencies released proposed supervisory guidance to provide additional detail regarding supervisory standards for operational risk management programs that will satisfy the qualification requirements outlined in the ANPR. The proposed supervisory guidance is available at www.fdic.gov/news/news/financial/2003/fil0362.html.

[15] In October 2005, the U.S. banking agencies issued an ANPR to solicit comments regarding a new capital framework for banks that do not adopt the Basel II accord. This proposed framework, sometimes referred to as Basel I-A, is designed to modernize the risk-based capital rules and minimize potentially material differences in capital requirements between banks that adopt Basel II and banks that remain under existing rules. The ANPR is available at www.fdic.gov/news/news/press/2005/pr10105a.html.

[16] Eric Holmquist, "The Fundamentals of Operational Risk Assessments," *OpRisk & Compliance,* December 2005.