By Lou Felice, NAIC Health and Solvency Policy Advisor and Shanique (Nikki) Hall, CIPR Manager

**INTRODUCTION**

Recent developments in the financial services industry have underscored the importance of operational risk management (ORM). Operational risk has played a role in many of the banking industry scandals taking place over the past two decades, including Barings Bank, Long-Term Capital Management, Bear Stearns and Lehman Brothers. The recent global financial crisis brought operational risk to the forefront once again. There were a wide range of causes for failures among financial institutions that were linked to the securitization process. Some of these were rooted in poor business practices or strategies. Loose underwriting standards are a prime example. However, other risks were rooted in a failure to initiate or to adhere to proper procedures; exercise proper due diligence; and recognize external deception (e.g., mortgage fraud). These failures are the essence of operational risk.1

As the financial system has become more interconnected and complex than ever before, the challenge of understanding and mitigating operational risks has increased. Improvements in ORM have taken on greater focus and visibility within the financial services industry and in many other industries over the past decade. In recent years, the NAIC, through its Solvency Modernization Initiative (SMI), has been exploring ways to increase the regulatory focus on operational risk. In addition, in advance of the Solvency II regulations, many large European insurance companies have begun to establish formal ORM programs. This article provides an overview of operational risk and highlights some of the work financial institutions have taken to effectively measure and manage operational risk.

**OPERATIONAL RISK**

The International Association of Insurance Supervisors (IAIS) defines “operational risk” as the risk of adverse change in the value of capital resources resulting from operational events such as inadequacy or failure of internal systems, personnel, procedures or controls, as well as external events.2 It refers to risk that result from shortfalls or inadequacies in the management of otherwise quantifiable risk, and from unforeseen external events that can impact an insurer. Operational risk potentially exists in all business activities; it encompasses a wide range of events and actions or inactions, such as fraud, human error, accounting errors, legal actions and system failures. Many of these problems arise during the course of conducting day-to-day business operations and are typically managed with little or no incident.

It is important to distinguish the nature of operational risk from that of other types of financial risk such as credit risk (counterparty failure risk, e.g. a credit downgrade or default) or market risk (risk of loss due to an overall decline in the market). Financial institutions normally take on a certain amount of credit and market risk, which they typically try to manage through portfolio diversification of credit instruments and equities. Insurers also take on the risks associated with mispricing policies, misestimating liabilities and mismatching the duration of investments vs. policy obligations, which also can be managed through geographical or product diversification, reinsurance and effective hedging strategies. Operational risks, on the other hand, are inherent, as it is a necessary part of conducting business, but have the potential to override management strategies and leave the institution open to “tail risk,” thus creating the potential for large losses.

Operational risk became recognized as a major risk class in the mid-1990s following a number of large-scale insolvencies in the banking industry caused or exacerbated by events outside of market and credit risk (i.e., BCCI, 1991; Orange County, 1994; Barings Bank, 1995; and Daiwa Bank, 1995, among others) and undermined the confidence in the banking system. In these cases, significant losses were incurred due to operational risk failures. As a result, many regulators and banking executives recognized financial institutions were exposed to non-credit-related risks, which included operational risk.3

In response, the Basel Committee on Banking Supervision (BCBS) released a proposal in June 1999 to replace the 1988 Basel Capital Accord (Basel I), which applied to all banks in the U.S., with a new risk-sensitive capital accord. The initial consultative proposal introduced an operational risk category and corresponding capital requirements. According to BCBS, the change reflected the committee’s interest in making the New Basel Capital Accord (Basel II) “more risk sensitive and the realization that risks other than credit and market can be substantial.”4

The Basel II definition of operational risk is primarily linked to its origin; i.e., events related to trading activities. Pillar 1 in Basel II is focused on only three risk categories in a bank’s

---

2 IAIS Common Framework for the Supervision of Internationally Active Insurance Groups (ComFrame) definition of “operational risk.”
trading operations: credit risk, operational risk and market risk. A majority of the published literature on operational risk is written on the banking sector and based on the definition of operational risk prescribed by Basel II. However, this definition is inappropriate to adopt in insurance, as the insurance business model is much different from that of banking. Hence, the characteristics and sources of operational risk are different in these two sectors. Banks are in the borrowing and lending business, while insurers act as risk-takers and managers of insurable risks. Banking/investment banking is a transactional business, supported by short-term funding in the capital markets, whereas insurers’ business is not transactional. Insurers cover risk exposures through reinsurance.

Consequently, it has been argued operational failures in the insurance sector are much less likely to create systemic risk in the economy. However, for some large life insurers, the line between banking activities and insurance activities has been blurred. Furthermore, the existence of insurance-based large financial conglomerates has drawn the attention of national and international regulatory bodies. Examples are the systemically important financial institution (SIFI) designation process in the United States and the global Financial Stability Board/IAIS effort to identify and designate globally systemically important insurers (G-SIIs). The former includes insurance-led institutions within its scope, and the latter is focused on such groups.

**Identifying/Quantifying Operational Risk**

Historically, organizations have accepted operational risk as an unavoidable cost of doing business. However, given operational risk has become recognized as a distinct risk category, the value of effectively managing operational risk has increased considerably of late. While there is currently a huge demand for operational risk quantification, the actual management of operational risk has not evolved commensurately. This is because operational risk is difficult to identify and assess as the causes are extremely heterogeneous, thus making developing statistical models for operational risk challenging. There are many different types of operational risk and the extent of operational risk can vary based on qualitative factors including corporate governance and the quality of internal controls in place. The *Financial Times* recently noted operational risk is the most amorphous and the hardest to protect against.

A sound operational risk model extends well beyond the confines of a formula-based quantification. It encompasses a company’s business activities and is an integral part of an efficient enterprise risk-management framework. An insurer’s underlying operational risk profile should be thoroughly reviewed across its range of business activities in order to identify and estimate the model input requirements. The principal challenge is to combine two essential sources of information: empirical loss data and expert judgment.

Many companies have been leveraging the experience of the banking industry, which has been focused on operational risk for more than a decade. The BCBS framework includes seven distinct types of operational risks varying in terms of frequency and severity. For example, internal fraud is a risk considered low frequency, high severity. Frequency and severity are vital in estimating potential operational risk losses. However, historical data on the frequency and severity of losses are often not available. Thus, uniform historical data upon which operational risk capital charges could be built is lacking. Most financial institutions are still in the process of collecting data.

Organizations, such as the Operational Risk Consortium (ORIC), have begun to collect data from participating financial institutions to develop operational risk loss data consortia. The ORIC database includes loss data provided by 225 large companies, including data from 16 core insurer members of the Association of British Insurers (ABI) and is focused on European operations. The database offers benchmarks against peers for loss experience comparison purposes and comparison of overall risk-management practices. The anonymized information is divided into eight categories with four severity levels and includes the frequency and amounts of loss events.

Although there are potential drawbacks to using self-reported data, it could be beneficial in identifying trends. The information is used to generate management reports that assist companies in prioritizing resources to identify and address control weaknesses in specific areas. Although the ability to integrate the data into models for purposes of a precise capital calculation is not there yet, use of scenario analysis could improve an entities ability to avoid significant losses from operational risk failures.

(Continued on page 5)
**OPERATIONAL RISK IN INSURANCE AND CAPITAL REQUIREMENTS**

An operational risk event can cause severe losses and may lead to an insurer’s insolvency or near insolvency. Traditional risk mitigation approaches (e.g., internal controls, auditing) are not expressly designed for low frequency, high severity events. They are designed around capturing transactional errors, which tend to be of a manageable loss size, whereas operational risk in insurance entities originates mainly in other areas. It is, therefore, important to have an explicit operational risk buffer in the regulatory capital test to provide a buffer for costly operational risk events. This is being recognized by regulatory authorities around the globe, and has captured the attention of the insurance industry, as well. As noted above, databases (such as ORIC and others) are being developed and expanded to include volunteer data donors from the insurance industry.

State insurance regulators, working together through the NAIC, have been looking at whether and how best to incorporate internal and external aspects of operational risk more explicitly into the risk-based capital (RBC) formulas. In 2013, the Capital Adequacy (E) Task Force turned its attention to operational risk. The Task Force’s Solvency Modernization RBC (E) Subgroup, Chaired by Alan Seeley of New Mexico’s Office of the Superintendent of Insurance, has been charged as follows: “Evaluate options for developing an operational risk charge in each of the RBC formulas and provide a recommendation to the Capital Adequacy (E) Task Force as to treatment of operational risk in the RBC formulas.”

The Subgroup began by looking at how other jurisdictions incorporate operational risk into their regulatory capital formulas, and received presentations from the Bermuda Monetary Authority and the Office of the Superintendent of Financial Institutions Canada (OSFI). A third presentation from the European Union (EU) covered the proposed regulatory approach in Solvency II, which is not yet in effect. The Subgroup’s short-term goals include: identifying appropriate risk exposure proxies; developing a simple factor-based capital requirement within the RBC formulas as early as 2014; and starting a process for identifying how and where the current RBC formulas could address operational risk. In the long run (three to five years to implementation), the Subgroup plans to follow and provide input into further development and use of an operational risk database and other potential qualitative aspects that could lead to a more risk-sensitive RBC approach.

Recent NAIC initiatives have also resulted in the adoption of the Risk Management and Own Risk and Solvency Assessment Model Act (#505), as well as corporate governance standards as qualitative means for considering internal operational risk and some aspects of external risk via a group-wide assessment. An Own Risk and Solvency Assessment (ORSA) will require insurers to analyze all reasonably foreseeable and relevant material risks (i.e., underwriting, credit, market, operational, liquidity risks, etc.) that could have an impact on an insurer’s ability to meet its policyholder obligations. Resulting from the NAIC’s SMI, large- and medium-size U.S. insurance groups and/or insurers will be required to regularly conduct an ORSA starting in 2015.

Internationally, methods to quantify and model operational risks have mostly been captured using formulaic approaches (i.e., a factor applied to a base number line annual premiums revenue or defined assets or liabilities). Canadian capital requirements for operational risk are formulaic, applying factors to risk exposure proxies with a focus on retention of operational risk regardless of mitigation strategies for other types of risks (e.g., reinsurance). Bermuda’s regulatory capital formula includes a capital add-on that includes a qualitative adjustment based on responses to a corporate governance questionnaire and possibly other inspection or analysis findings.

Solvency II requirements add the element of internal operational risk models to calculating regulatory capital requirements. Solvency II includes a standard formula approach to operational risk that applies different factors to pre-established risk exposure proxies for life vs. non-life insurers. In addition, there is an option to use an internal model approach under Solvency II to establish a regulatory capital requirement for operational risk for insurance and reinsurance companies. The inputs to the models can vary based on the specificities of the institution’s business activities, which can make comparisons across companies difficult. However the models are reviewed by regulators for statistical integrity and conformity with internal capital models (the so-called “use test”).

**EU-U.S. INSURANCE REGULATORY DIALOGUE PROJECT**

In 2012, the EU and the U.S. completed a comparison of the U.S. insurance regulatory system with that of the three-pillar approach of the proposed Solvency II Directive in Europe. This project, which looked at seven elements of regulation, is referred to as the EU-U.S. Insurance Regulatory Dialogue Project (EU-U.S. Dialogue) and is described in a final report issued in December 2012. One of the elements covered solvency and capital requirements.

(Continued on page 6)
At the end of the EU-U.S. Dialogue, a number of future work streams were agreed upon to explore opportunities to further harmonize the two systems. For capital and solvency, it was agreed, along with two other risk categories, to look at operational risk. Solvency II incorporates a provision for operational risk, and is in the development stages for U.S. RBC. The two sides will interact as follows:

• The EU will share information on the methodology and data used for calibrating operational risk in Solvency II. This includes the recent delivery of a presentation to NAIC staff currently responsible for the development of operational risk in the U.S.

• The U.S. will share information on the methodology and data used for calibrating operational risk in RBC. This could include the U.S. cooperating with EU counterparts during the ongoing work toward the definition of a factor-based approach to operational risk to incorporate in the RBC.

This initial phase is tentatively scheduled to run between now and June 30, 2014. In the longer-term, the parties might work together to develop/enhance an operational risk database. The EU has not embraced the ORIC database as yet, and the U.S. is interested in use of a database for its longer-term work on operational risk. This provides an area for further discussion and possible cooperation between U.S. and EU regulators.

**SUMMARY**

Operational risk is now recognized as a major risk class across all financial institutions. In the increasingly complex and interconnected global environment, the value of effectively measuring and managing operational risk has increased significantly. State insurance regulators and the NAIC continue to discuss operational risks, its possible inclusion into the RBC formulas, as well as its role in insolvencies and its interaction with other risk categories.
The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.

The views expressed in this publication do not necessarily represent the views of NAIC, its officers or members. All information contained in this document is obtained from sources believed by the NAIC to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, such information is provided “as is” without warranty of any kind. NO WARRANTY IS MADE, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY OPINION OR INFORMATION GIVEN OR MADE IN THIS PUBLICATION.

This publication is provided solely to subscribers and then solely in connection with and in furtherance of the regulatory purposes and objectives of the NAIC and state insurance regulation. Data or information discussed or shown may be confidential and or proprietary. Further distribution of this publication by the recipient to anyone is strictly prohibited. Anyone desiring to become a subscriber should contact the Center for Insurance Policy and Research Department directly.