IAA Risk Book

Chapter 4—Operational Risk

Peter Boller
Caroline Grégoire
Toshihiro Kawano

1. Executive Summary

Current categories for key risk factors for insurers are insurance risk (e.g., underwriting, catastrophe, and reserve risk), market risk, and credit risk. Operational risk is also an important risk for insurers and should be addressed via a multi-pillar supervisory framework.

Key messages of this chapter include:

1. The quality and maturity of the risk management process are key indicators that can impact potential losses arising from operational risk events.
2. Operational risk is closely linked to the risk culture of an insurer; as such, qualitative issues (such as strength of governance processes and oversight functions) play a large role in the management of operational risk.
3. The reliability of any operational risk modelling exercise is strictly connected with the actual quality of the overall data (internal or external data), which is generally an unknown. As a result, the appropriate model calibration in the data-poor environment of operational risk is one of the most significant and persistent challenges for insurers. Without sufficient data, models to quantify operational risk cannot be calibrated adequately.[1]
4. Typically, a capital charge or other mitigation method acts to reduce risk exposure, but adding an operational risk charge based on past losses (or the lack thereof) can be pro-cyclical.

[1] Canadian Institute of Actuaries (CIA) *Research Paper on Operational Risk*, November 2014.

This paper has been produced and approved by the Insurance Regulation Committee of the IAA on 15 September 2015 and amended on 8 March 2016. See end of chapter for explanation of amendment(s).

© 2016 International Actuarial Association / Association Actuarielle Internationale

5. Operational risk events for high-frequency/low-severity events can be captured and modelled, but tail events that are low frequency/high severity are where a qualitative scaling assessment can be most effective.

6. A credible assessment approach that is free from moral hazard is needed to evaluate the effectiveness of management in addressing operational risk exposures of both low- and high-severity events. It is true that quantitative methods for modelling operational risk for insurers are being developed and the literature supporting such methods is being published at a greater rate than in the past.[2] However, to have an effective and consistent operational risk regime, the assessment for operational risk should take into account, via a relativistic approach that is qualitative in nature, the rigor around risk management processes for such risk.

2. Introduction

In line with current regulatory interests, the focus of this chapter is on the importance of qualitative assessments to identify and estimate exposure to operational risk. It must be emphasized that of all the risks faced by insurers, operational risk is most likely the one risk that has the strongest qualitative aspects and where choosing a predominantly quantitative approach could fail to describe and assess the risk appropriately.

In international discussions on Basel II, academics and regulators have been critical of approaches to quantify operational risk capital for banking institutions that are based on expert scenarios and the probabilistic use of a tail value at risk (TVaR)-based measurement. Nevertheless, a granular focus on operational risk is increasingly evident in organizations. While some insurers are directing considerable efforts at quantifying operational risk, others are focusing primarily on the qualitative aspects of operational risk (e.g., looking into the processes that can lead to operational risk events).

Operational risk is closely linked to the risk culture of an insurer; thus, any attempt to quantify operational risk should be conducted in a very conscientious manner, making the limitations of the modelling approach transparent to the stakeholders. The focus for quantification should not be limited to the calculated results (i.e., the required capital) but also directed to:

- The processes and methodology followed to determine the required capital;
- The relevance and quality of the data used for modelling;

[2] CIA *Research Paper on Operational Risk*, November 2014.

- The frequency with which the assumptions need updating; and
- The reliability of the derived value.

In addition, a quantitative approach to measuring operational risk should take into account the specific risk management processes directed at mitigating operational risks.

A further challenge with quantifying operational risk is related to the extensive use of expert judgment. In light of the challenges related to data, many organizations incorporate the use of experts to supplement historical operational risk loss events. Where used, expert judgment should be robustly applied, well documented, and supported by data wherever possible. One of the challenges cited in the literature is the absence of methods for combining expert opinion with relevant internal and external data.[3]

Stakeholders must recognize the significantly greater uncertainty in modelled results of required capital for operational risk vs. other types of risk that have much longer histories of sufficient and reliable data (e.g., mortality risk for life insurers and catastrophe risk for general insurers). It should also be noted that, because of changes in management practices, data with respect to operational risks would potentially always be out of date.

Furthermore, an overly broad interpretation of operational risk could be problematic for events that have aspects of operational risk and are already included in the capital requirements associated with other risk types (e.g., credit, market, or insurance risk). For general insurers, an example of potential double counting of risk could arise with insurance risks that may include an element of claim fraud (detected or undetected), since fraud may be embedded in the claim ratios used to quantify underwriting risk and/or the historical claims development patterns that are used to quantify reserve risk. Operational risk solvency capital requirements generally focus on low-frequency/high-severity claim fraud events. It is important, nevertheless, to recognize that a certain amount of double counting may exist, reflecting a conservative approach to the overall quantification of capital requirements. The focus would be directed at adequate management actions to reduce the exposure to these types of boundary risk events. An important factor in quantifying a capital charge associated with operational risk is to avoid double counting with other risk categories.

[3] CIA *Research Paper on Operational Risk*, November 2014.

I. Definition

The definition of operational risk adopted by most insurance regulators is based on the definition originally set out for the regulation of international banks. Section V.A.644 of Basel II defines operational risk:

> 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.[4]

Legal risk is also defined within Basel II:

> Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.[5]

An important recent effort for insurers to expand the definition has been suggested in a white paper from the CRO Forum[6] that does not limit the definition of operational risk to losses only but also looks at other adverse consequences such as negative publicity and censure from supervisory agencies.[7] The objective is to ensure consideration of effects such as reputational risk so that appropriate operational risk management actions can be assessed.

II. Importance of Risk Culture

It is critical to recognize that a mechanical use of quantitative methods to determine required capital for operational risk should be avoided as the qualitative components that play a large role in the management of operational risks are often not fully captured by the methods. A weak risk culture has been the source of operational risk events leading to substantial financial losses within the insurance industry in the past. Examples include: poorly designed incentive systems, unclear direction from senior management (or messages that "bad news" is not welcome), and lack of accountability. Even if some elements of risk culture can be assessed

---

[4] Basel Committee on Banking Supervision, "International Convergence of Capital Measurement and Capital Standards—A Revised Approach—Comprehensive Version", Bank for International Settlements, June 2006: s.644: https://www.bis.org/publ/bcbs128.pdf.

[5] Ibid. Legal risk can be further described as "Legal risk is the risk of loss resulting from exposure to 1) non-compliance with regulatory and/or statutory responsibilities and/or 2) adverse interpretation of and/or enforceability of contractual provisions. This includes the exposure to new laws as well as changes in interpretations of existing law(s) by appropriate authorities and exceeding authority as contained in the contract." The source of this description is ORX Association, "Operational Risk Reporting Standards (ORRS)—Edition 2011", Revised 12 July 2012: s.3.1.2.

[6] CRO Forum, *Operational Risk* (*Principles of Operational Risk Management and Measurement)*, September 2014, p. 4.

[7] Ibid. p.4, A1. Definitions Practice 1 : Adopt a broad scope for the management of operational risk.

through quantitative approaches, there will always be some elements of a rather informal nature that are not assessable.

In this context, stakeholders should be cognizant of the insurer's risk culture as well as of the limitations of the selected methodology used to quantify operational risk.

3. Operational and Other Risks

I. Current Research/Findings

Key risk factors for insurers are insurance risk (i.e., underwriting, catastrophe, and reserve risk), market risk, and credit risk. Operational risk is also an important risk for insurers that should be addressed in a multi-pillar supervisory framework. In selecting a method to quantify operational risk, it is critical to carefully consider the definition of operational risk and any potential overlap with other risk categories. Many operational risks may already be considered implicitly as part of other risk types. It is essential that boundary conditions be clearly articulated so that risks are neither double counted nor overlooked. This topic is addressed in a presentation document titled "Operational Risk Management" prepared by Van den Heever and Slawski for the Actuarial Society of South Africa's 2011 Convention. They state: "A detailed taxonomy is required to obtain approximately consistent interpretations of risk event types and to ensure complete risk universe assessments."[8] They note that operational risks arising from shared services are often double counted, leading to duplication of risk management and capital. Another frequently cited example of potential double counting is the treatment of outsourcing risks.

Operational risk for insurers has been the subject of numerous papers and discussions. Two of the most recent and comprehensive papers are from the CIA and Milliman.

The CIA research paper is focused on:

- Definitions of operational risk terminology;
- Categorization of operational risk;
- Identification and description of quantification methods; and
- Details of existing regulatory requirements related to operational risk.

[8] R. van den Heever and J. Slawski, "Operational Risk Management", presented at the 2011 Convention of the Actuarial Society of South Africa, 8–9 November 2011. www.actuarialsociety.org.za/Portals/2/Documents/Convention-OperationalRiskManagement-RH-JS-2011.pdf.

The CIA comments that a review of the published literature on operational risk reveals a distinction between models that are used for (a) quantifying operational risk and calculating economic or regulatory capital and (b) managing operational risk. Such a differentiation can present challenges as those models used to quantify operational risk can also be used for management and vice versa. The CIA research paper focuses on models used to quantify operational risk rather than models used to manage operational risk.

Milliman's paper, "Operational Risk Modelling Framework",[9] summarizes the current quantitative approaches and compares them to processes used by industries outside the financial sector. Recently, the CRO Forum published a white paper on principles of operational risk management and measurement,[10] which takes into account both qualitative and quantitative aspects of operational risk.

II. A Point of Reference: Operational Risk in Other Sectors

Within the financial sector, the concept of operational risk has primarily emerged from the banking industry and initially was defined by exclusion—namely all risks other than market or credit. The Basel Committee on Banking Supervision (the Basel Committee) introduced a capital requirement under Basel II for operational risk for banking institutions, specifically laid out in the Revised Framework.

Under the Basel II regime, the (minimum) capital requirements of Pillar I are calculated separately for credit, market, and operational risk. It allowed the use of three different methods for the determination of operational risk capital—namely the basic indicator approach (BIA), the standardized approach (SA), and the advanced measurement approach (AMA), where increasing sophistication of the approach goes hand in hand with higher risk sensitivity. In general, the operational risk charge is a function (i.e., a proportion) of a bank's gross income; the underlying assumption is that risk corresponds to size as measured by income.

The Basel Committee recently conducted a review of the principles for sound management of operational risk that were first published in June 2011.[11] The review recommended that banks should:

[9] Milliman, *Operational Risk Modelling Framework*, February 2013.

[10] CRO Forum, *Principles of Operational Risk Management and Measurement*, September 2014.

[11] Basel Committee on Banking Supervision, *Review of the Principles for the Sound Management of Operational Risk*, 6 October 2014.

- Improve the implementation of each of the operational risk identification and assessment tools;
- Enhance the implementation of change management programs;
- Improve board and senior management oversight; and
- Strengthen the implementation of the three lines of defense, especially by refining the assignment of roles and responsibilities.

For quantification purposes, the Basel Committee has moved to two approaches: the SA and AMA.[12] Operational risk management now focuses on every process and risk within an organization and is more detailed than one overall estimate for the entire company that was previously based solely on overall revenues. The review also mentions that "methods for identifying and managing operational risk should be seen as complementary to the calculation of operational risk capital requirements, rather than as a consequence of that activity".

While different industries tend to adopt slightly revised definitions of operational risk,[13] the essence of the various definitions is quite similar—failed systems, people, processes—whether internal or external.

When comparing operational risks across different sectors of the financial industry to one another, care must be taken to pay attention to the different nature of the business. In a bank, millions of transactions can be processed each day. These are typically time-critical (e.g., money transfers and payments); and a major, persistent malfunction of such processes would have severe consequences for the bank concerned as well as other banks involved in the transactions—and possibly, through a ripple effect in a worst-case situation, for the entire financial system. Also, fraud (in particular in the form of rogue trading) has been an important phenomenon in the banking and trading industry as well as in the insurance industry, albeit of a different nature.

[12] Basel Committee on Banking Supervision, *Operational Risk—Revisions to the Simpler Approaches*, Consultative Document, October 2014.

[13] In the United States, the Federal Reserve defines operational risk as: "the potential that inadequate information systems, operational problems, breaches in internal controls, fraud or unforeseen catastrophes will result in unexpected losses" (Board of Governors of the Federal Reserve System**,** Federal Reserve Guidelines for Rating Risk Management at State Member Banks and Bank Holding Companies, SR 95-51 (SUP) 14 November 1995). And, in the Milliman paper, the following definition of operational risk is offered: "Risk of loss resulting from inadequate or failed productive inputs used in an operational activity" (Milliman (2013), p. 7).

Felice and Hall of the National Association of Insurance Commissioners (United States) state that the definition of operational risk used for banks by the Basel Committee is inappropriate for insurers due to the differences between the business models for banking and insurance. They believe the characteristics and sources of operational risk differ:

> 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.[14]

There are countless papers on the topic of operational risk management and measurement directed at banks. These papers provide detailed theoretical presentations of various methods used to quantify operational risk. They also present the results of comprehensive case studies, some based on the historical experience of individual banks and others based on aggregated data for multiple institutions. Finding up-to-date literature specifically applicable to the quantification of operational risk for insurers, however, is a challenge. While there are papers directed at insurers, they are far fewer than those directed at banks. Furthermore, some of the papers for insurers are now dated given the continued advancements in economic capital modelling, Solvency II, and the activities of the International Association of Insurance Supervisors (IAIS).

Given the greater volume of data available for modelling operational risk events for banks, there are naturally different modelling approaches for banks compared to insurers and consequently different capital requirements.

The following table provides examples of different modelling approaches for operational risk that would be warranted in varied industries, differentiating events by frequency and severity.

[14] CIA *Research Paper on Operational Risk*, November 2014. P.15.

Examples of Operational Risk Events

	Insurance	Banking	Mining	Energy
Low severity/high frequency	Claims processing, data errors, periodic/installment premium collection	ATM failures	Transport service interruption	Meter reading errors
Medium severity/medium frequency	Fraud, regulatory compliance failure	Online security breach, fraud, regulatory compliance failure	Environmental contamination	Environmental contamination
High severity/low frequency	Mis-selling, mispricing	Rogue trader	Mine collapse	Oil spill, gas plant fire

Source: Milliman (2013), p. 13 with modifications by author

III. Common Factors and General Approach to Operational Risk—Summary of Current Research

Given that all definitions of operational risk are directed at financial losses that stem from failed people, processes, and systems, as well as from external events that adversely affect the organization, one can identify the following aspects that are common to all industries:

1. The business model drives the relative importance of people, processes, and systems and their influence on operational risk events.
2. Since tail events are often nonlinear and have interdependencies, mean and variance techniques tend to be very unstable. A useful way to address these constraints is to specify the following three major categories of inputs and outcomes:
3. Inputs
    a. Land, labor, and capital;
    b. Processes used, regulations, legal and political events/environment, and technology; and
    c. Risk culture.

4. Outcomes
    a. High frequency/low severity;
    b. Medium frequency/medium severity; and
    c. Low frequency/high severity.
5. The need to blend qualitative and quantitative assessments.
6. The need to link operational risk outcomes to the drivers that created them and to consider the related time horizon for both causation and resolution.

Thus, to address operational risk, the following items need to be considered:

Clarify how the operational risk outcomes are related to the specific people, processes, systems, and external events that produce them.

Distinguish if the primary goal is to "manage" operational risk or to "quantify" the risk with a goal to translate the quantification into a capital charge.[15] Then later evaluate which tools are necessary to manage or assess operational risk incorporating both quantitative and qualitative considerations.

Because high-severity event factors tend not to be stable over time, simple factors are often unreliable, resulting in an operational risk capital that may be insufficient or excessive in relationship to the financial impact of the operational risk event.

The management and governance of behaviours need to be a primary focus to reduce/mitigate the consequences of operational risk events.

There are evolving techniques for measurement of operational risk, but it is often a difficult task to determine an appropriate level of operational risk capital for insurers. Because insurance events are financially driven processes, operational risk may best be addressed (in some circumstances) through the tools already in place for mis-selling, pricing, or reserving. The CRO Forum stated[16] that the measurement of operational risk is not about finding the exact truth; it is about finding a reasonable numerical assessment with the aim to support the quality of (risk) management decisions.

---

[15] Historically, the quantification of a risk has been essential to being able to "trade it" in an open market. Operational risk seems to be not tradable in the open market.

[16] CRO Forum, *Principles of Operational Risk Management and Measurement*, September 2014, p. 3.

4. Prerequisites for the Quantification of Operational Risk

In "Quantifying Regulatory Capital for Operational Risk", Embrechts et al. state: "The accuracy in predicting future loss values depends on the volume and quality of the observed historical data."[17] The reliability of any operational risk modelling exercise is strictly connected with the actual quality of the overall data (internal or external data), which is generally an unknown. As a result, the appropriate model calibration in the data-poor environment of operational risk is one of the most significant and persistent challenges for insurers. Without sufficient data, models to quantify operational risk cannot be calibrated adequately.

I. Data Sources

Data sources can be internal or external to the insurer.

Basel II requires banks to use a minimum of five years of internal loss data when using the AMA.[18] Internal data represent the actual operational risk losses incurred by the financial institution and can be used for the primary quantification methods used to determine required capital for operational risk. One of the reasons that internal loss data are often used as a foundation for the AMA is that internal data are considered to be the most objective risk indicator currently available reflecting the unique risk profile of the specific financial institution.[19] The challenges in securing sufficient internal data and the need to evaluate the exposure to potentially severe tail events are among the reasons why Basel II requires banks to supplement their own data with further sources (including both external data and scenario analysis) to determine their operational risk capital charge.

External data refer to operational risk losses that have occurred in other organizations. External data may be obtained from a third-party vendor or from a data consortium such as ORIC for insurers or ORX for banks. Aue and Kalkbrener explain that "external loss data can be used to supplement an internal loss data set, to modify parameters derived from the internal loss data, and to improve the quality and credibility of scenarios. External data can also be used to

[17] P. Embrechts, H. Furrer, and R. Kaufmann, "Quantifying Regulatory Capital for Operational Risk", research supported by *Credit Suisse Group*, *Swiss Re* and *UBS AG* through *RiskLab*, Switzerland, 2003: 4: www.math.ethz.ch/~embrecht/ftp/OPRiskWeb.pdf.

[18] When first moving from the BIA or SA to the AMA, a bank is allowed to use three years of internal loss data.

[19] F. Aue and M. Kalkbrener, "LDA at Work", Deutsche Bank AG, February 2007: 8: kalkbrener.at/Selected_publications_files/AueKalkbrener06.pdf.

validate the results obtained from internal data or for benchmarking."[20] However, it is not necessarily clear whether operational risk data from one company (e.g., an insurer) is relevant for the business of another company (whether another insurer or a reinsurer).

Lastly, beyond pure quantitative data (e.g., costs, frequency), the capturing and understanding of qualitative information are critical. Qualitative information describes the causal drivers of operational risk and interdependencies with other risks and circumstances. This is a particularly crucial aspect for insurers.

II. Data Quality

One of the greatest impediments to modelling operational risk is the lack of a sufficient volume of high-quality, accurate data—both internal and external data. There are numerous factors contributing to the challenges with data. First, for some insurers, historical operational risk loss data have only been recorded and aggregated for a relatively short period of time. Historically, data on losses arising from events that are categorized as operational risk loss events were not required. Furthermore, the costs of collecting such data were deemed to outweigh the benefits. In "LDA at Work", Aue and Kalkbrener discuss two inherent weaknesses of internal loss data when used as a foundation for operational risk exposure measurement:

- Loss data is a "backward-looking" measure, which means that it will not capture changes to the risk and control environment.
- Loss data is not available in sufficient quantities in any financial institution to permit a reasonable assessment of exposure, particularly in terms of assessing the risk of extreme losses.[21]

Data on operational risk need to be comprehensive. For this purpose, a framework needs to be set up and applied as data are recorded and gathered. Data standards need to be homogeneous and uniform over time and across sources of operational risk (e.g., what constitutes a loss, how a loss figure is derived), consistent over time, and complete (e.g., which loss elements are included and which are excluded).

One key aspect to be considered is the issue of potential double counting; losses should not be registered more than once.

---

[20] Ibid.: 11.

[21] F. Aue and M. Kalkbrener, "LDA at Work", Deutsche Bank AG, February 2007: 8: kalkbrener.at/Selected_publications_files/AueKalkbrener06.pdf.

III. Data Relevance

For an appropriate assessment of operational risk, the data and information used need to be relevant for the business of the insurer. As insurers differ based on domicile, size, lines of business written, organizational structure, etc., the losses arising from operational risk events at one insurer may have little relevance for another insurer. While internal data may be considered to be the most appropriate (but also likely most scarce), external data will only be valuable to the extent it is relevant for the business and the processes of the insurer concerned.

The Milliman white paper states "In general, operational risks are characterized by underlying drivers, which tend to adapt and change over time. This makes it problematic to use a classical statistical approach, as data can rapidly cease to relate to the risk."[22] Changes in processes may reduce or even eliminate the possibility that particular past losses would occur in the future, or that losses that happened in the past would recur in the future but with a significantly different severity.

While some insurers lack a sufficient volume of operational risk loss data, others face challenges with the inconsistency in the collection of operational risk loss data. Because operational risk spreads over different activities of an insurer, any loss analysis would be exposed to the potential for inconsistencies in the identification, categorization, and reporting of losses. Inconsistencies may exist from department to department or business line to business line within an insurer as well as from one insurer to another. Inconsistencies present challenges when the internal data are aggregated within an insurer or when internal data are combined with external data. Such inconsistencies could influence the statistical analysis of operational risk losses, particularly given the limited volume of data possessed by most insurers.

The basic question remains whether the data should be used to monitor and improve the control system that limits this risk or to quantify a capital requirement. Doing the former is inconsistent with the latter, as any data uncovering a material risk generally leads to actions that make the data unusable for quantifying the future risk.

5. Assessment of Operational Risk

A comprehensive assessment of operational risk requires an amalgamation of a qualitative and a quantitative approach. While the qualitative aspect addresses primarily the "manage" part of

[22] N. Cantle, D. Clark, J. Kent, and H. Verheugen, "A Brief Overview of Current Approaches to Operational Risk under Solvency II", Milliman white paper, July 2012: 2: http://uk.milliman.com/uploadedFiles/insight/life-published/pdfs/current-approaches-operational-risk.pdf.

dealing with operational risk, the quantitative aspect addresses the financial consequences, or "measurement" part of operational risk. Depending on the characteristic of the operational risk (i.e., human, process, system, and external events), insurers may apply significantly different weights to the quantitative and qualitative approaches. Operational risk events for high-frequency/low-severity events can be captured and modelled, but those tail events that are low frequency/high severity are where a qualitative scaling assessment can be most effective.

I. Quantitative Approaches

The CIA *Research Paper on Operational Risk* includes a comprehensive description of the three primary quantitative methods that are found in the literature for both banks and insurers. The Milliman paper also describes each of these methods in detail.

A. Frequency-severity approach

The use of frequency-severity analysis is well documented in actuarial literature for general insurance. Within the context of Basel II, frequency-severity analysis is referred to as the LDA. Dutta and Babbel note that "given the similarity of operational losses to property/casualty losses, the measurement approach predominantly follows the loss distribution approach (LDA), which actuaries use for pricing property/casualty insurance".[23]

The LDA is described by Chapelle et al. as follows:

> ... a parametric technique that consists in separately estimating a frequency distribution for the occurrence of operational losses and a severity distribution for the economic impact of individual losses. In order to obtain the total distribution of operational losses, these two distributions are then combined through *n*-convolution of the severity distribution with itself, where *n* is a random variable that follows the frequency distribution.[24]

As discussed in Dutta and Perry, LDA implementation needs thorough exploratory work to be done before deciding on a model.[25]

---

[23]. K. K. Dutta and D. F. Babbel, "Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach," *Journal of Risk and Insurance*, June 2014.

[24] A. Chapelle, Y. Crama, G. Hübner, and J.-P. Peters, "Practical Methods for Measuring and Managing Operational Risk in the Financial Sector: A Clinical Study", *ScienceDirect, Journal of Banking & Finance* 32 (2008) 1049–1061, 1 October 2007: s.5: http://finance.flemingeurope.com/webdata/3118/JBF-Chapelle-etal2008.pdf.

[25] Dutta, K.K. and Perry, J., "A tale of tails: An empirical analysis of loss distribution models for estimating operational risk capital", *Working Paper Series, Federal Reserve Bank of Boston*, No. 06-13, July 2006

For banks complying with the requirements of the AMA under Basel II, the LDA would include:

- Homogeneous categories of internal observations to derive univariate distributions of operational losses for each type of loss event;
- Integration of external loss data to refine the shape of the distribution tail at its extreme; and
- Joint analysis of loss event categories to reflect possible dependence between univariate distributions.

The basic principle of a frequency-severity analysis is to generate the number of losses and the average value (i.e., severity) of each loss using separate and distinct statistical models. Model parameters are derived by fitting historical data to a variety of distributions using the input of experts or a combination of data and expert input.

B. Causal modelling and Bayesian estimation techniques (including the use of key risk indicators)

A Bayesian network (BN) is described by the Milliman paper as "a visual description (formally, a directed acyclical graph) of the relationships between causes and effects. BNs use Bayes' theorem to compute the probabilities in the model"[26]. The CIA paper explains that BNs have been used for decades in numerous applications including medical expert systems, transportation, failure diagnosis, pattern matching, chemical processing, speech recognition, infrastructure, environmental modelling, and legal and evidential reasoning. The use of BNs within financial institutions and insurance in particular, has not been as pervasive as in other industries[27].

Unlike the frequency-severity approach, BNs are causal networks and thus valuable for analyzing the causes that contribute to operational risk. The CIA paper states that BN's "can be particularly useful for modeling ORCs with little or no loss data (internal or external)". However, the paper also indicates that "Some European banks have experimented with using BN for operational risk capital quantification without patent success. It is unclear whether the issues encountered by the banking sector will translate to the insurance sector. As such, further

[26] Milliman, *Operational Risk Modelling Framework*, February 2013, p38.

[27] CIA *Research Paper on Operational Risk*, November 2014, p66.

research will be required by the insurance industry to determine the applicability of BN for the quantification of operational risk capital."[28]

C. Scenario analysis

According to Dr. Eric Rosengren, scenario analyses are used by banks for three primary purposes: stress testing, creating synthetic losses (when there is insufficient internal loss data), and generating severity functions for the frequency-severity approach.[29] As noted previously, historical data are not always a good predictor for future states of the world, in particular if processes surrounding operational risk events have changed significantly. Historical data may also be incomplete (especially for very low-frequency events with extreme dollar impacts). Thus, scenario analysis is a technique that is often used to describe and quantify the tail of the distribution. A scenario describes a consistent future state of the world over time, resulting from a plausible and possibly adverse set of events or sequences of events.[30] [31] Scenarios can be relatively simple and one-dimensional or very complex (e.g., a shock event triggers a series of causal, consecutive, cascading events). In addition, a scenario could be immediate with a short duration (e.g., earthquake), while other scenarios, typically complex scenarios, can develop over longer time periods (e.g., the financial crisis of 2007–2008). To better describe unobserved events for the purpose of quantitative modelling of operational risk, synthetic scenarios would typically be used. Synthetic scenarios describe hypothetical conditions that have not been observed and that can thus be more easily tailored to a specific situation of interest. These hypothetical conditions might occur but have not been observed—for instance, because of sheer good luck or because certain risks did not previously exist.

II. Qualitative Approaches

As noted repeatedly in this chapter, consideration of operational risk requires a qualitative perspective as well as a quantitative outcome.

---

[28] Ibid.: P.66 and 79.

[29] E. Rosengren, executive vice president, Federal Reserve Bank of Boston, 19 July 2006 presentation titled "Scenario Analysis and the AMA": 3: www.boj.or.jp/en/announcements/release_2006/data/fsc0608be9.pdf.

[30] For a comprehensive discussion of scenarios and scenario analysis refer to *Stress Testing and Scenario Analysis*, International Actuarial Association (IAA), July 2013: http://www.actuaries.org/CTTEES_SOLV/Documents/StressTestingPaper.pdf.

[31] For how to integrate a scenarios in estimating operational risk refer to K. K. Dutta and D. F. Babbel, "Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach," *Journal of Risk and Insurance*, June 2014.

The current data sources for operational losses are rather thin; thus, it is imperative that risk assessments for operational risks take into account the risk management processes to support this risk. The quality and maturity of an insurer's risk management processes have a material influence on the severity and frequency of potential losses arising from operational risk events. Yet, a credible measurement approach that is free from moral hazard is needed to evaluate the effectiveness of management.

The following regulatory examples illustrate some current approaches to address this challenge:

A. Commercial Insurers Solvency Self-Assessment (CISSA)

As part of the CISSA, the Bermuda Monetary Authority (BMA) relies on the Commercial Insurer Risk Assessment (CIRA[32]) for the assessment of the operational risks of an insurer. This self-assessment is split into three components: corporate governance, risk management function, and risk management process (identification, measurement, response, and monitoring/reporting) for eight operational risk categories.

The processes are checked whether they are at stage 1 ("ad hoc"), 2, 3, or 4 ("implemented, well documented, standardized and reviewed annually") as described in CIRA. They are then allocated scores (from 50 to 200) depending on their quality. The final score of the complete assessment is turned into a capital charge: the more mature the risk management system, the more points are obtained from the self-assessment, and the lower the operational risk charge becomes.

The maximum operational risk charge of CIRA corresponds to 10 percent of the required capital for the other quantifiable risks (e.g., underwriting, market, and credit). After a threshold of points has been reached in the self-assessment, the operational risk charge decreases.

This self-assessment allows an undertaking to quantify the operational risks, which can also be validated by the other approaches mentioned above. In addition to the calculation of required capital, the self-assessment provides a direct link to the risk management process, which satisfies the so-called "use-test" of regulatory requirements. The self-assessment allows undertakings to easily identify the areas of the risk management system that need improvements, and, from there on, priorities can be set. It also provides incentives to improve the control process and reduce operational risk.

[32] Commercial Insurer Risk Assessment, BMA, Guidance Note #17, November 2008.

This approach starts with a qualitative approach that is then transformed into a quantitative figure.

B. China Risk Oriented Solvency System (C-ROSS)

In February 2015, the China Insurance Regulatory Commission introduced C-ROSS.[33] C-ROSS reflects realities of the emerging markets. C-ROSS uses qualitative regulatory tools to assess operational risk. Operational risk is categorized in Pillar II. A capital charge is included for operational risk and other Pillar II risks (strategic, reputational, and liquidity risks) via a factor applied to the "quantifiable risks" capital charge in Pillar I. This factor is assessed on a company basis and based on the regulator evaluation of "the risk management capabilities of the insurers". That evaluation results in a score between 0 and 100. For scores below 80, the factor (and the resulting Pillar II charge) is positive; for scores above 80, the factor is negative (resulting in a reduction in the overall capital requirement), with no Pillar II charge for a score of 80. As a result, C-ROSS incentivizes insurers to adopt and maintain good risk management.

C. Swiss Solvency Test (SST)

SST[34] does not include a capital charge for operational risk. It states that at the current time, no quantitative consideration of operational risks is generally required in the SST unless an insurance company were to be expressly requested by Swiss Financial Market Supervisory Authority (FINMA) to do this for serious reasons. Operational risks are to be appropriately taken into account in risk management.

III. Conclusions

To summarize, key reasons why many insurers are not yet modelling operational risk include:

The lack of credible data due to the relatively short time span for which historical operational risk loss data have been collected;

- The role of the internal control environment and its ever-changing nature, which makes historical operational risk loss data somewhat irrelevant;

[33] China Insurance Regulatory Commission, China Risk Oriented Solvency System Conceptual Framework, March 2014.

Guan Ling, China Risk Oriented Solvency System—A Practical View from Emerging Market, IAA Zurich Meeting, April 2015.

Junbo Xiang, C-ROSS: A Major Reform of China's Insurance Regulatory System, *The Geneva Association Newsletter* No. 59, June 2015.

[34] FINMA, Swiss Solvency Test, Circular 2008/44 "SST".

- The important role of infrequent but very large operational risk loss events;
- The continued state of development for insurers' internal models and the rigorous governance framework surrounding the use of such models; and
- Cost-benefit issues that result in questions about the value of internal models given their significant implementation costs.

Typically, a capital charge or other mitigation approach acts to reduce risk exposure, but adding an operational risk charge based on past losses (or the lack thereof) could have no effect on reducing future risk. A pro-cyclical process could be created whereby the absence of operational risk event losses leads to no required capital; when an event occurs, not only does the insurer need to fund the event, it must also raise funds for a possible future operational risk event even though the circumstances that generated the event have likely changed.

Dr. Peter Boller was vice-chair of the Insurance Regulation Committee, chair of the ASTIN Section, and chair of the Reinsurance Subcommittee of the IAA. He was a substantial contributor until his untimely death.

Caroline Grégoire, BSc from Université de Montréal, is an associate member of the Swedish Actuarial Association. She has worked in various positions at Hannover Re in Hannover, Germany, including reserving for property and casualty business, internal audit, operational and qualitative risk management, and risk reporting. She can be reached at *Caroline.Gregoire@hannover-re.com*.

Toshihiro Kawano, FIAJ, is chief actuary at AEGON Sony Life Insurance Company in Tokyo, Japan. He is also vice-chair of the Insurance Regulation Committee of the IAA. Toshihiro can be reached at *Toshihiro_kawano@aegonsonylife.co.jp*.

CHAPTER AMENDMENT(S):

Section 5 **Assessment of Operational Risk**, subsection I **Quantitative Approaches** of this chapter was amended on 8 March 2016. The description now uses a recent definition of the Bayesian-Network and related explanations, and some footnotes were amended to make footnotes 23 and 29 (new 31) refer to the same paper.