Financial Services Forum
Scoring Goals in a Changing World
5-6 May 2014
Hilton Sydney

Operational risk modeling: how far have we progressed?

Prepared by Ben Cooper, Bartosz Piwcewicz and Nic Warren

Presented to the Actuaries Institute

Financial Services Forum

5 – 6 May 2014

Sydney

Institute of Actuaries of Australia
ABN 69 000 423 656
Level 2, 50 Carrington Street, Sydney NSW Australia 2000
t +61 (0) 2 9233 3466 **f** +61 (0) 2 9233 3446
e actuaries@actuaries.asn.au **w** www.actuaries.asn.au

Abstract

This paper has been written from the perspective of the general insurance industry. It discusses current approaches to the operational risk modelling for capital assessment purposes given the data and modelling techniques available.

Our review of current market practice amongst general insurers shows that there are a number of challenges related to operational risk modelling. However, it appears that various data limitations and, in particular, limited historical data are the key factors slowing down the progression of operational risk modelling in practice.

While we are of the view that it is possible to model operational risk in a robust and effective manner despite the data limitations, more research in respect of operational risk is required to advance market practice.

Key words: Capital modelling, operational risk

Table of Contents

1 Introduction

This paper discusses current market practice and key challenges in relation to operational risk modelling for capital assessment purposes in Australia. This paper approaches this topic from a general insurance industry perspective. However, we consider this discussion to be relevant for the entire financial services sector and, where insightful, we have drawn some comparisons to the banking industry.

While there has been a considerable volume of research conducted to date in respect of other risk categories, operational risk research[1], particularly amongst general insurers, is in its relative infancy. In our view, there are two main reasons for this:

- **Difficulty in measuring operational risk losses** – this arises from the nature of operational risk losses, which are often seen as low frequency/high severity. For some operational risk loss types, the cost can be quantified directly, e.g. fines paid to a regulator for various breaches. However, for many other operational risk loss types, the associated cost can often only be estimated.
- **Limited credible historical data** – most general insurers only started recording internal operational risk losses recently. Banks have been collecting this information for some time and external operational risk databases, e.g. the Operational Riskdata eXchange (ORX) database, have been created to combine operational risk loss data across multiple organisations (and, in some cases, industries). However, there are some significant challenges to using external historical data effectively.

We are of the view that there is a strong need to better understand and quantify operational risk. APRA's regulatory capital framework requires an explicit allowance for potential losses arising from this risk category. While the Standard method derives this capital allowance using a formula linked to an insurer's premium income and insurance liabilities, the Internal Model Based (**IMB**) method is expected to model operational risk in a fairly granular manner taking into account uncertainty associated with:

- frequency and severity of operational risk losses;
- dependencies between different operational risk loss types; and
- dependencies between operational risk and other risk categories.

Operational risk is a difficult topic and, in our experience, APRA's and the general insurance industry's views on what is possible in terms of modelling this risk category are not well aligned. One of the key purposes of this paper is to discuss the key challenges in relation to operational risk modelling. We hope that the issues raised contribute to the on-going dialogue between financial institutions and APRA in the operational risk space.

[1] This refers to published operational risk research focusing on quantification of operational risk.

The paper is intended for a non-technical audience. However, a basic understanding of risk based capital modelling concepts and APRA's regulatory capital framework is expected.

The paper is split into four sections:

- Section 2 – provides some context for operational risk;
- Section 3 – summarises a general approach to modelling operational risk under the IMB method and discusses the current market practice in respect of the various components of this approach;
- Section 4 – discusses the key challenges in relation to operational risk modelling; and
- Section 5 – summarises our conclusions.

2 Context

2.1 Regulatory framework

APRA's regulatory capital framework requires regulated institutions to meet a prudential capital requirement (**PCR**) that is *"intended to take account of the full range of risks to which a regulated institution is exposed"*[2]. The PCR is determined as the sum of:

- a prescribed capital amount (**PCA**) assessed using either:
  - the Standard method; or
  - the Internal Model Based method (**IMB method**); or
  - a combination of the Standard and IMB methods
- any supervisory adjustment determined by APRA.

While both the Standard and IMB methods are required to consider operational risk explicitly, the discussion in this paper is most relevant for the IMB method. This method takes a much more granular approach to assessing the operational risks to which a particular regulated institution (i.e. an insurer) is exposed to.

Apart from Allianz Australia, who was accredited by APRA to use the IMB method in June 2012[3], all other Australian insurers are required to use the Standard method. Nonetheless we understand that other general insurers have approached APRA to have their internal capital models approved for use as part of the IMB method for determining the PCA.

2.2 Definition

APRA defines six main risk categories relevant to an insurer's business. These categories are required to be modelled adequately within an internal capital model (**ICM**) if this model is to be approved by APRA for use as part of the IMB method. The risk categories defined by APRA[4] are:

- **catastrophe risk** – relating to natural or man-made events that produce insurance losses from many insureds at the same time;
- **underwriting risk** – relating to the possibility that future insurance exposures (both from business in force and future business) will be loss making;
- **reserving risk** – relating to the possibility that the provisions for claims outstanding will be inadequate to meet the ultimate costs when the business is run off to extinction;
- **market risk** – relating to the risk arising from all aspects of the value of investments and currencies, including interest rate changes, market price changes, counterparty default, exchange rates and liquidity of investments;

[2] Prudential Standard GPS 110 – Capital Adequacy (**GPS 110**), paragraph 22
[3] https://www.australianbankingfinance.com/insurance/allianz-gains-apra-capital-model-approval-/
[4] GPS 113, paragraph 17

- **credit risk** – relating to the risk of loss arising from failure to collect funds from creditors, including reinsurers and intermediaries; and
- **operational risk** – the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This includes legal risk, e.g. exposures to fines, penalties or punitive damages resulting from regulatory actions, but excludes strategic or reputational risk.

Under the IMB method, insurers are required to model operational risk over a one year time horizon and "consider all of the following four elements:

a. relevant internal event data (for which the regulated institution must maintain a suitably comprehensive operational risk event recording system);
b. relevant external event data;
c. scenario analysis; and
d. the business environment and internal control systems."[5]

While APRA's definitions of risk categories are a useful reference point, our experience in capital modelling suggests that the definitions of some risk categories are different in practice. These differences arise for valid practical reasons and result in a classification of individual risks between operational risk categories that we consider to be more appropriate for an insurance business.

We discuss the implications of differences in definitions for operational risk in section 4.1. However, given the discussion included in the next two sections, it is important to highlight that these differences have a significant impact on the classification of risks, the relative size of individual risk categories and the resulting risk category attributions.

2.3 Operational risk loss types

Table 2.1 shows operational risk loss types, often used by general insurers, and examples of operational risk losses that could impact each loss type.

Table 2.1: Typical operational risk loss types for general insurers

Operational risk loss type	Examples of operational risk losses
Internal Fraud	• Misappropriation of assets • Theft of customer personal data • Tax evasion • Theft of commercially sensitive information e.g. the insurer's premium rating structure
External Fraud	• Fraud from a third party or service provider e.g. overcharging by repairers • Inability to control fraudulent insurance claims
Employment practices and workplace safety	• Discrimination • Workplace health and safety
Clients, products and business practices	• Improper distribution practices or mis-selling of insurance products

[5] GPS 113, paragraph 21

Operational risk loss type	Examples of operational risk losses
	• Inadequate policy wording results in product flaws and unexpected claim payments • Breach of accounting or regulatory standards
Damage to physical assets	• Malicious damage • Inadequate insurance cover resulting in a natural catastrophe event having a major impact on insurer's physical assets
Execution, delivery and process management	• Errors in a rating engine resulting in incorrect premiums being charged • Inadequate and reliable accounting systems with which to properly assess financial position • Process to set future budgets is overly optimistic and fails to address past failures
Business disruption and system failures	• Inadequate insurance cover resulting in a natural catastrophe event having a major impact on insurer's business operations • IT failures (software or hardware) • Cyber-terrorism • Collapse of a key corporate partnership e.g. external data provider, broker, underwriting agency etc.

We make the following key observations in respect of Table 2.1:

- The operational risk loss types shown are the same as the Basel II operational risk event types. It is current market practice to categorise operational risks using this classification.
- There are a number of losses relating to failed process, people or systems that could be included in the above table e.g. errors in the calculation of insurance liabilities or errors in the calculation of insurance premiums. However, in our view, they are already considered within reserving and underwriting risk categories and classifying them as operational risk would result in double-counting. This highlights the importance of introducing and consistent application of clear definitions of risk categories and a robust underlying risk classification process.
- Some operational risk losses are likely to impact multiple operational risk loss types (and risk categories). For example, if an insurer has an inadequate insurance cover in place a natural catastrophe event may cause damage to insurer's physical assets and disruption to its business operations and also generate an insurance loss that impacts the underwriting result. Events impacting multiple operational risk loss types and risk categories are likely to complicate the collection, processing and use of loss data, both internal and external.

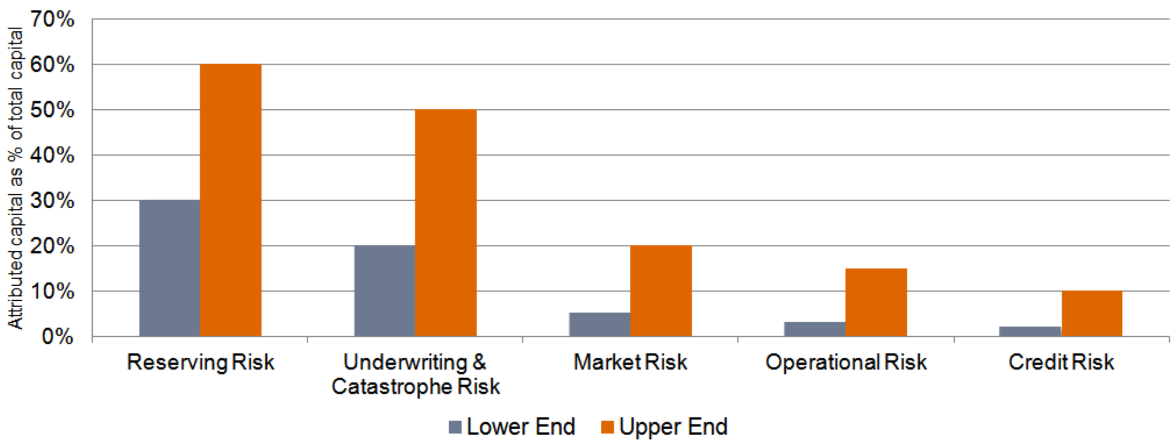
2.4 Materiality of operational risk

Understanding the risk profile and relative materiality of each risk category is crucial for any business. A risk category attribution process is often used to understand how total capital available is consumed by different risk categories, including operational risk.

The purpose of this paper is not to go into any detail regarding approaches and challenges related to capital attribution by risk category. In particular, risk category attributions adopted by insurers are likely to differ due to a number of factors e.g. business mix, investment strategy, reinsurance arrangements, capital structure, attribution method used and risk category definitions adopted etc.

Figure 2.1 below is intended to provide some context in terms of the materiality of operational risk compared to other key risk categories modelled in a general insurer's ICM. The range is derived based on our experience gained through capital modelling work for a number of insurers.

Figure 2.1: Typical risk attribution for general insurers



We make the following key observations in respect of Figure 2.1:

- The risk attribution range shown above **should not** be treated as a benchmark range for capital attribution by risk category for a particular general insurer. The purpose of Figure 2.1 is purely to provide context for the discussion included this paper.
- Insurance risk, i.e. reserving, underwriting and catastrophe risk categories combined, accounts for the majority of capital attribution. This is not surprising given that the attribution ranges have been derived in the context of general insurance business.
- Operational risk typically ranks behind insurance and market risk categories in terms of its capital contribution. The range shown above is between 3% and 15%. The mid-point in this range, i.e. 9%, is very similar to capital attributions to

operational risk, observed for largest Australian banks[6]. Having said this, one need to appreciate significantly different nature of the risk to which banks are exposed to.

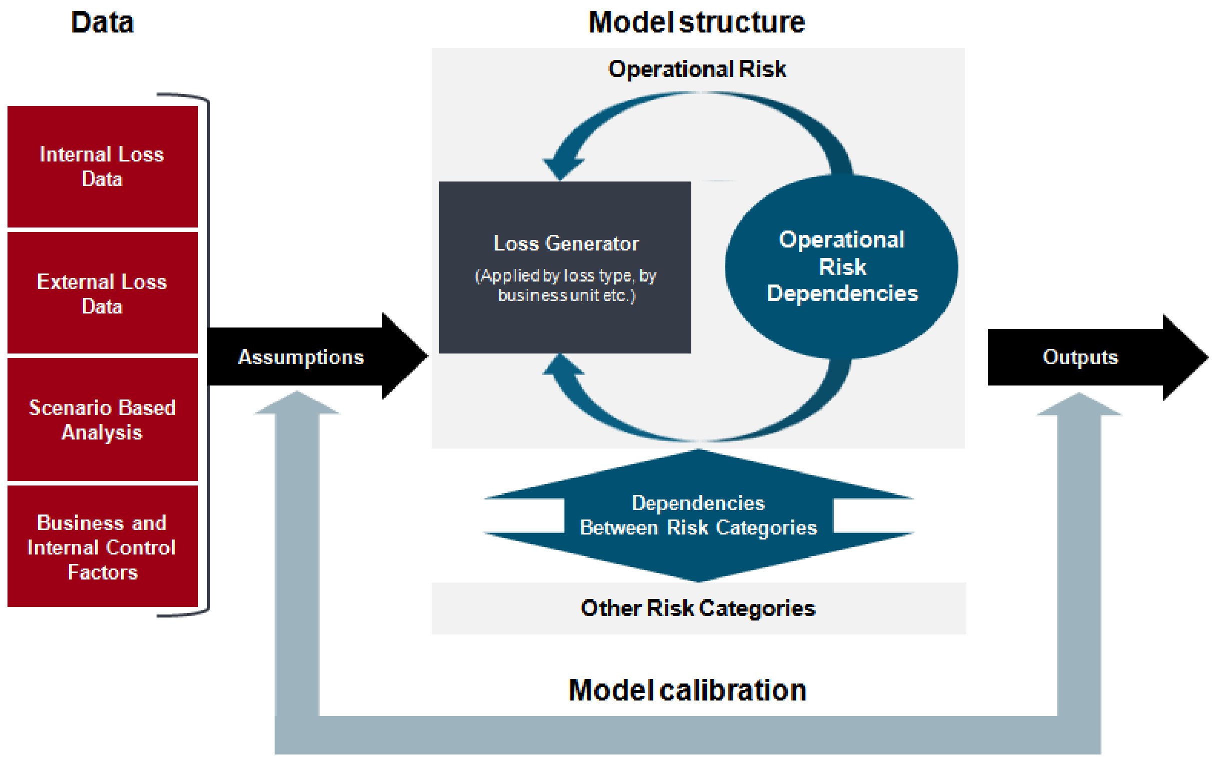
- The scale and uncertainty surrounding potential operational losses is evolving as systems increase in complexity and information flows become easier. Greater understanding of these emerging risks, together with improved data and quantification methods may shift the typical risk profile of a general insurance entity from that shown above.

[6] See Jarratt [1]

3 General Approach

Modelling operational risk is often divided into three distinct components, i.e. data, model structure and model calibration.

Figure 3.1: General approach to modelling operational risk



Data is the key input into the model calibration. It is important that the data is categorised into appropriately granular groupings to allow analysis to be performed, e.g. loss type, business unit etc. Data can be obtained from multiple sources, internal and external to a particular institution.

Model structure relates to the mathematical approach used to model operational risk losses. The approach adopted may take either a highly granular or an aggregated view when generating operational risk losses and incorporate and approach to model dependencies between risk types and between operational risks and other risk categories.

Model calibration consists of three components:

- Calibration inputs – assumptions used as inputs including distributions and parameters in the calibration of the operational risk model.
- Calibration outputs – various outputs from the operational risk model that are used to check the reasonableness of the calibration or within the broader ICM
- Calibration process – all methods and processes used in the extraction and analysis of data, the development of model inputs and the analysis and testing of model outputs.

Model calibration is broader than just a statistical exercise to derive the parameters used within the model structure. It requires a mixture of quantitative and qualitative analysis in order to ensure that operational risk modelling is fit for capital modelling purposes.

3.1 Data

APRA requires the operational risk component of economic capital models to consider four elements[7]:

- internal loss data;
- external loss data;
- scenario based analysis; and
- the business environment and internal control factors.

The main reason for this is that internal operational risk loss data is typically sparse and insufficient for capital modelling purposes. This is due to two factors, i.e. the low frequency of occurrence of some operational risk losses and a relatively short period of time over which financial institutions have collected operational risk data.

Shevchenko [4] provided an assessment in terms of how many years of data would be required to estimate within 10% accuracy the 1 in 1000 year aggregate operational risk loss for a bank using an advanced measurement approach accredit by APRA. His estimate was 10^5 years of annual loss data.

We discuss the key challenges related to operational risk data in section 4.2.

3.1.1 Internal loss data

Internal loss data relates to an institution's own historical operational risk loss experience.

APRA does not provide any specific guidelines or requirements in relation to the collection of this data for insurers. However, within its prudential standard for authorised deposit-taking institutions (**ADIs**)[8], e.g. banks, any institution aiming to be approved to use an advanced measurement approach for quantifying operational risk must have in place policies to collect and measure internal operational risk data in a consistent, timely and comprehensive fashion. In addition this process must be transparent, verifiable and have associated review and approval processes.

An internal operational risk database must record a broad range of information including gross loss, recoveries received, nature of the loss and description, date of occurrence and date of discovery. The data used for capital calculations by ADIs must cover a minimum five year time period. However, even with this minimum five

[7] GPS 113, paragraph 21
[8] Prudential Standard APS 115 – Capital Adequacy: Advanced Measurement Approaches to Operational Risk (**APS 115**)

year data collection period, many of the operational risk categories are likely to have no or very few observations recorded.

In a general insurance context, we find that the collection of internal loss data is not as advanced as described above for ADIs. However, for some high frequency/low severity operational risk losses, internal databases may exist. For example, a legal record of fraudulent claims, a legal record of incidents of workplace discrimination or own insurance claims arising from damage to physical assets are more likely to exist.

3.1.2 External loss data

External loss data relates to information collected about operational risk losses from other institutions.

There are three key types of external loss data sources recognised by practitioners[9]:

- publicly available data – this data is compiled from operational risk losses reported in the media;
- insurance data – this data is collected by insurance brokers and originates from insurance claims made by financial institutions; and
- consortium data – this data contains non-public information provided by participating financial institutions.

All external data sources have some limitations and we discuss these in more detail in section 4.2.

In our experience, consortium data is most commonly used. The Operational Riskdata eXchange (**ORX**) database is an example of this data. Individual loss data is collected from participating institutions on a quarterly basis and made available to ORX subscribers in a de-identified format.

Banks are the key contributors to the ORX database, including all major Australian banks. However, a number of global insurers and other financial institutions have also been participating.

3.1.3 Scenario based analysis

Operational risk scenarios are used either to complement or supplement historical loss data. They are constructed by businesses and are intended to provide two key pieces of information:

- the scope and nature of a particular operational risk loss (e.g. loss of customer data due to internal fraud); and
- the underlying assumptions in terms of frequency and severity (e.g. loss of customer data due to internal fraud is expected to occur once every 10 years

[9] Wilson [2]

and, when it occurs, its most likely severity is $50 million and its worst case severity is $100 million).

Operational risk scenarios typically focus on low frequency/high severity events.

In our experience, the construction of operational risk scenarios is often a challenging process and involves a high level of subjectivity. However, there is great value in using scenario based analysis. In particular, the scenarios can consider a range of losses, i.e. losses that where near misses in the past and others which relate to new and emerging risks. By comparison, internal and external data are limited by historical information.

Scenario based analysis is common across many financial institutions to assess operational risks, and plays a more important role in institutions that do not have access to established operational risk loss records (e.g. insurers). The analysis is typically performed in a workshop environment with external risk management experts and business managers within the institution.

3.1.4 Business environment and internal control factors

Business environment and internal control factors (**BEICFs**) are various indicators incorporated within an institution's systems to measure the institution's operational risk profile.

Similar to operational risk scenarios, BEICFs are used either to complement or supplement historical loss data. However, unlike operational risk scenarios, BEICFs focus on high frequency/low severity events and can be determined using quantitative data or various qualitative measures that incorporate expert opinions.

Watchorn and Levy [2] provide a detailed discussion on BEICFs in the context of banks. However, in our view, the discussion is also relevant for insurers. The authors define business environment factors as those "characteristics of a bank's internal and external operating environment that bear an exposure to operational risk". They refer to them as inherent risks of the bank. Internal control factors are defined by the authors as controls embedded with the bank's internal control system that are used to mitigate the inherent risks of the bank. Any residual risk is managed by the bank on a daily/business as usual basis.

It is worth highlighting that BEICFs have some similarities with other concepts used historically such as balanced scorecards or key performance indicators.

3.2 Model structure

As highlighted in Figure 3.1, there are three components to the model structure typically specified in an operational risk model:

- a loss generator;
- operational risk dependencies; and
- dependencies between operational risk and other risk categories.

Each of these components is discussed below in more detail.

The modelling of operational risk is typically performed using Monte Carlo simulations due to their intuitive interpretation and straightforward implementation.

3.2.1 Loss generator

A loss distribution approach is the most common approach used to generate operational risk losses. This approach is easier to explain, implement and calibrate than a number of alternative approaches proposed by current literature, e.g. Generalised Linear Models, Neural Networks, Bayesian Networks and Generalised Additive Models for Location Shape and Scale. The alternative approaches are not discussed further in this paper.

As part of a loss distribution approach, the loss distribution for a particular operational risk loss type is decomposed into frequency and severity components.

The frequency distribution describes the number of losses occurring within a period, and is typically modelled using a Poisson or Negative Binomial distribution.

The severity distribution describes the distribution of each single event once it has occurred. There is a range of statistical parametric distributions available to model loss severity. However, due to the "fat-tailed" nature of operational risk losses not all of these distributions are appropriate. Some practitioners go one step further to deal with this challenge and use a blend of statistical parametric distributions, separately for the body (low severity) and tail (extreme severity) losses.

The model calibration approach (discussed below) influences the choice of distributions.

The loss distribution for a particular operational risk loss type is constructed using the convolution of the frequency and severity distributions.

3.2.2 Operational risk dependencies

Dependencies between loss types can be imposed using three different approaches:

- through aggregate losses;
- through both loss frequency and severity; and
- through loss frequency.

The method that uses both loss frequency and severity to impose dependencies is more complex to implement and calibrate than the two alternative methods. This method is also likely to require the largest number of parameters. Given data limitations discussed above, this approach is not commonly used.

Regardless of the approach taken, the implementation of dependencies requires a dependency structure (i.e. a parametric or empirical copula) and dependency parameters to define the dependency relationship between variables. A dependency structure can be thought of as a function that links the individual loss distributions between loss types to derive a combined distribution of operational risk losses. The dependency parameters signify the strength of these linkages.

Dependency structures exhibiting strong tail dependency are often preferred. The main reason for this is that the level of correlation between operational risk loss types is expected to be highest in tails of distribution, i.e. for extremely high or extremely low events. For example, a failure of insurer's claim and policy management systems is likely to have a company-wide impact.

3.2.3 Dependencies between operational risk and other risk categories

There is currently no common approach used in the Australian insurance market to implement these dependencies. The approaches range from not allowing any diversification between operational risk and other risk categories, i.e. full dependence, to allowing some diversification between these risk categories. The latter approaches are often implemented using a dependency structure that is applied between simulated combined operational risk losses and simulated underwriting result or profit before income tax that excludes operational risk losses.

For comparison, APRA does not prescribe any particular approach for the implementation of these dependencies. However, any insurer using the IMB method for regulatory capital purposes and wishing to introduce diversification benefit between operational risk and other risk categories "must demonstrate an adequate process for estimating dependencies (particularly for extreme losses) and must apply conservatism in its assumptions that is commensurate with the uncertainty of those assumptions."[10]

3.3 Model calibration

As highlighted above, there are three components underpinning model calibration, i.e. calibration inputs, calibration outputs and calibration process.

It is important to appreciate that there is a wide range of approaches used to calibrate operational risk. The points summarised below are strongly influenced by our experience gained through work in the capital modelling space.

Definitions of risk categories and the underlying risk classification process, discussed in sections 2.2 and 2.3 respectively, have a significant impact on the calibration of operational risk and other risk categories. In our experience, all three components of model calibration are affected and particular care needs to be taken to ensure that:

- there is no double-counting of risks; and
- no material risks are missed in the calibration process.

[10] GPS 113, paragraph 20

A common approach to achieving the above is to consider each operational risk loss individually and determine whether and to what extent it is covered by other risk categories.

Treatment of the risk of under-reserving due to inadequate or failed internal processes, people and systems, or from external events is a good example to illustrate the need for care when attributing risks to a particular risk category. In particular, this risk is typically considered one of the systemic sources of uncertainty associated with the run-off of insurance liabilities within a risk margins analysis. It is common market practice to use outputs from this analysis in the calibration of reserving and underwriting risk categories and insurers need to assess whether any additional allowance for this risk needs to be made as part of operational risk modelling.

3.3.1 Calibration inputs

There are three groups of assumptions required to parameterise the model structure:

- statistical distributions and parameters for frequency and severity for each modelled loss type;
- dependency structures and the underlying assumptions required to parameterise dependencies between operational risk loss types; and
- a dependency structure and the underlying assumptions required to parameterise dependencies between operational risk and other risk categories.

3.3.2 Calibration outputs

There are a number of outputs that need to be generated by an operational risk model. In general, we would expect the following outputs to be produced:

- simulated combined operational risk losses – these are used as an input into an ICM and, depending on the modelling purpose, can be produced for a single projection year or for multiple projection years;
- implied percentiles of loss distributions – these are derived for standalone loss types, combined operational risk losses (i.e. diversified basis) and by summing standalone percentiles across all individual operational risk loss types (i.e. undiversified basis) and are used to assess the reasonableness of the implied volatilities;
- loss type attributions – these show relative contributions from individual operational risk loss types to the overall operational risk loss profile at different percentiles and are used to assess the reasonableness of the key drivers of overall operational risk losses;
- implied rank and tail correlations between loss types – these are derived using the simulated loss for each operational risk loss type and are used to assess the reasonableness of the correlations implied between operational risk loss types;
- implied diversification benefits for operational risk – these are derived using the diversified and undiversified distribution percentiles and are used to assess the

reasonableness of the overall level of diversification implied by the model for operational risk;

- implied rank and tail correlations between risk categories – these are derived using the simulated loss for each risk category and are used to assess the reasonableness of correlations implied by the ICM between operational risk and other risk categories;
- a risk category attribution by percentile – this shows relative consumption of capital by each risk category and is used to assess reasonableness of the key drivers of capital at different percentiles; and
- results of scenario and sensitivity testing – this analysis is likely to consider all key assumptions and is used to assess sensitivity of various outputs to changes in these assumptions.

3.3.3 Calibration process

While calibrating operational risk, and in particular the distribution and dependency assumptions used to model this risk category, it is important to appreciate the high level of uncertainty involved in the estimation and selection of these assumptions. This uncertainty arises for two main reasons:

- there is insufficient data for the estimation process; and
- future outcomes are likely to differ from past experience.

Given this, the calibration process is highly subjective and testing and benchmarking the reasonableness of model outputs plays a significant role in the validation of the operational risk calibration.

The calibration process can be naturally split into a process used to derive operational risk assumptions, i.e. model inputs, and a process used to assess reasonableness of model outputs. In our experience, the latter process is effectively used to test, inform and refine the former process.

The remainder of this section focuses on approaches used to derive operational risk assumptions. These approaches heavily depend on which data types are available and can be used.

If internal and external loss data are available standard parameter estimation techniques can often be applied to derive reasonable model parameters. However, any non-standard aspects of the adopted model structure may introduce unforseen complications, e.g. the use a body/tail approach for the severity distribution.

If available operational risk data is derived mainly from scenario based analysis and/or BEICFs the approach to selecting reasonable assumptions does not usually involve any statistical parameter estimation techniques. Instead the main focus is on the interpretation of information provided within the scenarios in terms of the required distribution and dependency assumptions, e.g. interpretation of the worst case scenario or interpretation of the high, medium or low correlations. This process is highly subjective and its effectiveness often depends on good communication amongst key business stakeholders involved in the process, common understanding of the scope and implications of the scenarios being proposed and a robust challenge process.

In cases where all four types of operational risk data are available for the model calibration purposes (e.g. large banks), rigorous approaches to blending parameter estimates obtained from different data sources are often required. These approaches broadly fall into two categories:

- credibility factor approaches; and
- Bayesian blending approaches.

Credibility factor approaches derive a blended parameter estimate using a weighted combination of the parameter estimates derived from different data sources. The weight applied to each data source is chosen to reflect some measure of the derived parameter's credibility (e.g. parameter standard error).

Bayesian blending approaches attempt to blend parameter estimates derived from alternative data sources using a more rigorous Bayesian probabilistic approach. Bayesian blending approaches produce an updated (posterior) estimate of parameter values given data, typically internal loss data, and some prior information about the parameter values, usually derived from external loss data and/or the scenario based analysis and BEICF data.

Bayesian blending approaches can be split into analytical and numerical.

Analytical Bayesian approaches provide an efficient approach to deriving solutions for updated parameter estimates by utilising well known properties of statistical distributions. However analytical blending approaches face a number of restrictions on the distribution that can be used, thereby limiting the flexibility of the approach. For example, a body/tail distribution approach used for severity is unlikely to be handled well within an analytical Bayesian approach.

Numerical Bayesian approaches use algorithms to produce a series of samples from a distribution of the updated parameter estimate. Thus, a numerical approach does not produce a single point estimate for the posterior parameters. In order to produce a point estimate of the updated parameters statistics, such as the mean, must be calculated from these numerically generated samples. While this approach is more complex than analytical Bayesian approaches, numerical approaches place very few restrictions on the model being used, allowing it to be parametric or empirical, skewed or symmetric, have a large or small variance.

Ultimately there is a level of judgement required for any of the blending approaches discussed above. In the case of a credibility factor approach, the effect of any judgement overlay on the approach is directly visible in the weight applied to a particular data source. In the case of a Bayesian blending approach the subjectivity lies buried deep within in the mechanics of the approach.

This should not be viewed as a criticism of these approaches, rather a warning that the use of a sophisticated blending approach does not provide a silver bullet. Some level of subjectivity is necessary to allow the appropriate level of emphasis to be applied to scenario based analysis or BEICF data. Without this, calibration inputs would not have the ability to reflect additional information related to changes in systems and processes that are not directly quantifiable or visible in historical data.

4 Key challenges

The insurance industry's views on whether and how operational risk should be modelled within an ICM are quite diverse. They range from not modelling operational risk within an ICM at all to implementing a granular approach that considers each operational risk loss type individually. Under the former approach, an operational risk capital allowance could be derived outside the ICM using a simplified standalone approach similar to the one included in APRA's Standard method. Under the latter approach, operational risk would be modelled with an ICM and any limitations in data, etc. would be dealt with using actuarial judgement as is the case for all other risk categories.

This section summarises the key challenges related to operational risk modelling for capital purposes. Our discussion is split into several sub-sections each considering a different aspect of operational risk modelling.

4.1 Definition

APRA's definition of operational risk is broad and, in our view, substantially overlaps with definitions of underwriting and reserving risk categories. The overlap relates mainly to a risk of under-reserving of existing business and a risk of underpricing of future business, both arising due to inadequate or failed internal processes, people and systems, or from external events.

APRA's risk categorisation captures these risks within the operational risk category. However, it is common market practice, in Australia and overseas, to capture these risks within the reserving and underwriting risk categories since their impact is already reflected in the past data and considered explicitly as part of reserving or pricing analyses.

The treatment of these two risks has a material impact on the relative size of operational risk. In particular, APRA's definition of operational risk results in a higher attribution of capital to this risk category than the alternative, market adopted, approach discussed above. In our experience, this is likely to create some challenges when discussing risk attributions implied by an ICM with APRA. In light of these definitional issues we also wonder whether APRA has inadvertently double-counted certain aspects of operational risk when determining the operational risk capital charge used in the Standard method.

4.2 Data

We have summarised the key challenges relating to the data and its use for deriving operational risk assumptions by data source:

- Internal loss data – given that insurers have started collecting this data in a structured manner only recently, the volume of data and its coverage across different loss types are limited. This significantly diminishes the usefulness of this data for any quantitative analysis. For comparison, the largest Australian banks are in a better position for two reasons:

- higher volumes of transactions processed compared to insurers that would be expected to generate more operational risk losses; and
- longer collection periods for internal loss data.

However, due to the low frequency of occurrence of operational risk losses, some gaps in the bank data do exist despite the two points highlighted above.

- External loss data – while combining operational risk loss data across a number of financial institutions is desirable, there are some serious questions about the usefulness of this data for operational risk modelling purposes. In our view, the key challenges include:
  - Relevance – there is currently no external database that is specific to the insurance industry. All external loss databases available in the market consist of mostly banking data. This data is of limited (or no) use to insurers given fundamental differences between banking and insurance businesses.
  - Inherent biases – these are discussed in some detail by Wilson [2] and impact all external loss databases. The author describes three main categories of biases, i.e. reporting, control and scale biases. This list can be extended by one more category, i.e. time-related biases. All four categories can be summarised as follows:
    - Reporting biases – these arise due to differences in loss collection thresholds applied by contributing institutions.
    - Control biases – these arise due to each contributing institution being unique in terms of its operations and control structure.
    - Scale biases – these arise due to different sizes of contributing institutions.
    - Time-related biases – these arise due to changes impacting contributing institutions over the collection period (e.g. changes in size) and the collection process itself.
  - Anonymity of data – this is an obvious and common feature of any external database. However, in the context of operational risk modelling, this feature makes it difficult (or even impossible) to remove the inherent biases from the data.
- Scenario based analysis and BEICFs – these types of data can provide valuable business insights, capture potential future sources of operational risk that are not present in historical loss data and enable operational risk modelling even if no empirical data exist. However, the information provided through these sources is inherently subjective and impacted by various behavioural biases. For operational risk scenarios, an additional level of complication arises due to a need to interpret and translate a business's qualitative assessment of the likelihood and severity of scenarios into assumptions required for modelling operational risk losses. In doing so, it is crucial that both modellers and non-technical business stakeholders have common understanding of this process and its implications on modelling results.

4.3 Model calibration

As discussed above, operational risk data is the key input into the calibration process used for operational risk. Any limitations in this data need to be addressed through the calibration process to ensure that the calibration inputs are appropriate.

For many insurers, scenario based analysis and BEICFs are likely to be the only available sources of operational risk data at this stage and current market evidence certainly supports this. However, while mean and volatility assumption can be determined using this analysis, dependency assumptions pose a significantly different challenge. For this reason, special care needs to be taken when developing the scenarios and educating business stakeholders who provide input into the calibration process.

For a bank, there appear to be more data options available than for an insurer. However, this does not mean that the calibration process is significantly easier. In particular, the challenges summarised above are further complicated by the need to blend assumptions derived from the four data sources. In our experience, the choice of the most appropriate blending method is not always obvious.

4.4 Dependencies

The modelling of dependencies related to operational risk is arguably the most contentious aspect of operational risk modelling for capital assessment purposes. The main reasons for this are:

- lack of credible data that could be used to quantify these dependencies; and
- a high level of subjectivity involved in the calibration of these dependencies.

Intuitively, most operational risk losses are correlated between each other due to a number of common factors, e.g. systems, processes and culture, embedded within a particular organisation. These factors also create a level of correlation between operational risk and other risk categories, e.g. reserving and underwriting risk.

One would also expect that the level of correlation increases once a business is in a stressed scenario. This can be due to a number of causes, including the impact of a company-wide breakdown in risk management processes. The collapse of HIH is an example of a stressed scenario and shows that if things go wrong they are likely to impact the majority (if not all) risk categories.

While there are a number of approaches that could be used to incorporate dependencies into the modelling of operational risk in an ICM, the key challenge is to choose which approach is most appropriate and what dependency assumptions should be selected.

For dependencies between operational risk and other risk categories, this decision is likely to be complicated further if an insurer approaches APRA to have its ICM approved for regulatory purposes. In our experience, data limitations and high level of subjectivity involved in the calibration of these dependencies will make it really difficult to convince APRA that any diversification benefit can be allowed for between operational risk and other risk categories.

5 Summary and conclusions

The main focus of this paper has been to explore what is possible in terms of the operational risk modelling for the purposes of capital assessment by general insurers, given the data and modelling approaches available to them. This discussion is important for two reasons:

- APRA's and general insurance industry's views on this topic are not well aligned; and
- research in respect of operational risk quantification lags behind research for other risk categories.

APRA's regulatory capital framework requires an explicit allowance for operational risk. In particular, the Standard method derives this allowance using a formulaic approach, while the IMB (risk based capital) method uses a granular approach that considers the full distribution of operational risk losses, dependencies between operational risk loss types and dependencies between operational risk and other risk categories. The discussion included in this paper is most relevant for the IMB method.

Our review of current market practice amongst general insurers demonstrates that there are a number of challenges related to operational risk modelling.

The difference in definitions of operational risk between APRA and what we consider to be common market practice is an signficant challenge and has a significant impact on:

- the calibration of operation, reserving and underwriting risk categories; and
- the reconciliation of risk attributions implied by an ICM with those expected by APRA.

Various data limitations, including limited relevant historical data, are potentially the key factors slowing down the progression of operational risk modelling in practice. General insurers have only recently started collecting internal loss data and there are currently no general insurance specific external operational risk databases that could be used to supplement this data. For comparison, banks have been recording internal operational risk loss data for a number of years and have formed consortiums to share this data amongst each other through external operational risk databases.

Regardless of the data limitations, we are of the view that it is possible to model operational risk in a robust and effective manner. However, the adopted approach should be pragmatic and supported by a comprehensive calibration process. The nature of operational risk is such that judgement is likely to play a significant role in the modelling and calibration of this risk category.

We also suggest that more research is required for operational risk in the context of insurance businesses. There a number of questions that could be explored, e.g. how to develop and implement an effective framework for scenario based analysis, how to quantify operational risk dependencies, how to develop top-down benchmarks for assessing operational risk modelling results, etc.

6 Bibliography

1. Jarratt, J. (2013): "Practicalities of operational risk capital modelling". SFMW Workshop.
2. Watchorn, E. and Levy, A. (2008): "Information paper: developing business environment and internal control factors for operational risk measurement and management". APRA
3. Wilson, S. (2007): "Information paper: A review of correction techniques of inherent biases in external operational risk loss data". APRA
4. Shevchenko, P.V. and Peters, G. W. (2013): "Loss Distribution Approach for Operational Risk Capital Modelling under Basel II: Combining Different Data Sources for Risk Estimation". The Journal of Governance and Regulation 2(3), 33-57
5. GIRO 2003 Working Party: "Risk: Measurement or bust". Institute and Faculty of Actuaries
6. Peters, G. W., Shevchenko, P.V. and Wüthrich, M. V. (2009): "Dynamic operational risk: modeling dependence and combining different sources of information". The Journal of Operational Risk 4(2), pp. 69-104