SOUTH AFRICAN ACTUARIAL JOURNAL
SAAJ **13** (2013) 39–95
http://dx.doi.org/10.4314/saaj.v13i1.3

OPERATIONAL RISK MANAGEMENT: PRACTICAL IMPLICATIONS FOR THE SOUTH AFRICAN INSURANCE INDUSTRY

By M Martin and M Hayes

Submission received 5 December 2012
Accepted for publication 12 June 2013

ABSTRACT
Like its European counterparts, the South African insurance industry is moving towards its own risk-based regulatory regime, Solvency Assessment and Management (SAM). As a result greater focus is being placed on the appreciation of risks facing firms, of which operational risk forms a significant part. This paper aims to review operational risks as they pertain to South African insurers, both in internal risk-management practices and for the purposes of regulatory compliance. It presents principles and initiatives that have the potential to assist insurers in their identification and management of operational risks. A framework for the management of operational risk is discussed, as is the use of operational-loss data in this framework. Through an industry survey, this paper assesses perceptions towards operational risk, as well as views on the SAM regulations for the calculation of operational risk capital. Furthermore, high-level feasibility of an industry-wide operational-risk consortium database is studied.

KEYWORDS
Operational risk; Risk management framework; Solvency Assessment and Management; Operational Risk Consortium; ORIC; Risk Event Database; RED

CONTACT DETAILS
Marilyn Martin, School of Statistics and Actuarial Science, University of the Witwatersrand, Johannesburg; Tel: +27(0)11 958 1182; E-mail: marilynmartin00@gmail.com
Mark Hayes, School of Statistics and Actuarial Science, University of the Witwatersrand, Johannesburg; Tel: +27(0)11 717 6271; E-mail: mark.hayes@wits.ac.za

1. INTRODUCTION

1.1 Increasingly, operational risk is becoming an important issue in the boardroom.[1] Whilst operational losses are usually of the high-frequency–low-severity type, there is the potential for extreme losses to occur and thus operational risk cannot be ignored (Embrechts, Furrer & Kaufmann, 2003). Recent times have seen a move in the insurance industry towards a greater appreciation of the risks facing individual companies and the industry as a whole (Acharyya, 2012).

1.2 There is a vast body of literature on the topic of operational risk and its management; however, most of it is centred on the banking industry. It is only recently that operational risk has been recognised as being of the same significance to insurers (Wei, unpublished). In the narrowing of the scope to the context of the South African insurance industry, a distinct lack of research on this subject is revealed.

1.3 The move in South Africa towards a risk-based regulatory regime in 2015, following the international trend, requires that firms take greater account of the risks to which they are exposed and set aside capital accordingly.[2] Operational risk carries its own explicit capital charge.[3] Additionally, regulation will demand more comprehensive management of operational risk throughout the business entity.[4]

1.4 Operational risk is difficult to identify, quantify and manage (Tripp et al., 2004). It encompasses a very broad range of risks, displaying a wide variation in potential severity to firms (Dexter et al., 2007). Of greatest concern are high-frequency–low-severity events, which have the potential to threaten the continuity of the firm (Acharyya, op. cit.). These events, in particular, are characterised by a lack of the data that is needed to gain an understanding of that threat (Selvaggi, 2009).

1.5 Management practices for operational risk that extend beyond a mere formula-based calculation or model are vital (Lam, 2003). Tripp et al. (op. cit.: 921) succinctly put it that "not having the right processes in place to manage operational risk is indeed itself an operational risk".

1.6 Like their European counterparts, insurers in South Africa face the challenges of their own new regulatory regime, Solvency Assessment and Management (SAM), which too requires account to be taken of operational risks. Whilst local insurers see benefit in

1 Guardrisk Update Newsletter, Volume 14, Issue 3, May 2008
2 Operational Risk for Insurers, Ernst & Young, 2011
3 Solvency Assessment and Management (SAM) Roadmap. Financial Services Board, 2010
4 ibid.

the formalisation of operational-risk modelling and management, it is recognised that a great deal will need to be done in order for these benefits to be realised.[5]

1.7 This paper aims to investigate operational risks in the context of the South African insurance industry in light of SAM and the preparedness of entities for the changes SAM will impose. Furthermore, the paper aims to draw together operational risk management (ORM) principles discussed in the literature and to examine the feasibility of an operational-risk database initiative that has the potential to assist insurers with the incorporation of these principles into their businesses.

1.8 This paper takes a top-down approach. Section 2 begins with a broad overview of operational risk as it pertains to insurers in general. The focus is then narrowed to the South African insurance industry through a review of the forthcoming local regulatory requirements in respect of operational risks. In further tapering the scope, an outline of a risk-management framework within an insurance entity is discussed. The literature on the usefulness of loss data as an information source to assist insurers in improving their operational-risk procedures is then considered. Sections 3 and 4 present an investigation of the South African insurance industry's perceptions towards operational risk and its management, as well as their views on the SAM regulations on the calculation of operational-risk capital. Furthermore, firms were questioned on their views of an external, industry-wide operational-risk database and their willingness to become involved with such an initiative. Section 5 draws conclusions on the maturity of operational-risk practices instituted by South African insurers, the appropriateness of operational-risk regulation as well as on the feasibility of the database, and presents the limitations of the conclusions that can be drawn.

2. LITERATURE REVIEW

2.1 OPERATIONAL RISK IN THE INSURANCE INDUSTRY

2.1.1 Operational risk forms part of one of the six risk categories in the Prudential Sourcebook (PSB) of the United Kingdom's Financial Services Authority (FSA).[6] As is common in much of the literature on the topic, the definition of operational risk adopted in this report is that of the Basel Committee:[7]

> 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.

5 Brian Metcalf (2012). Strategic and Emerging Issues in South African Insurance. 5th ed. PwC. Johannesburg

6 Integrated Prudential Sourcebook. Financial Services Authority, 2004. www.fsa.gov.uk/pubs/policy/ps04_16.pdf, 28/05/2012

7 International Convergence of Capital Measurement and Capital Standards. Bank for International Settlements, Basel Committee on Banking Supervision, 2006, page 144

Acharyya (op. cit.) does, however, state that it may be difficult to fit all operational risks that occur in an insurance business context into the above definition. For example, a decision error at top management level, i.e., a strategic risk, may give rise to an operational risk.

2.1.2 Operational risks are apparent throughout an insurance company's operations (Dexter et al., op. cit.). Insurance companies, however, are said to lag behind the banking industry when it comes to the management of operational risk.[8] Acharyya (op. cit.) opines that insurers have not yet reached the stage of being able to appreciate adequately some of the operational risks they face, despite having extensive experience in the quantification of risk. In the sessional discussion of the work of Tripp et al. (op. cit.), a speaker argued the point that although the recognition of the importance of operational risk is in its infancy, insurers—being inherently risk quantifiers—may already be calculating operational risks without explicitly realising it.

2.1.3 Whilst much of what is proposed with regard to the quantification of operational risks is applicable across both the banking and insurance industries, it is the softer, management-type considerations that have the potential to distinguish between the two (Tripp et al., op. cit.). Acharyya (op. cit.) remarks on the significant differences between the nature of insurance companies and banks: the nature of large insurance business is largely strategic, whereas in retail banking it is transactional. Retail banks are therefore more exposed to higher-frequency–lower-severity operational risks associated with errors in these transactions than large insurers would be (Selvaggi, op. cit.). It is, however, recognised that not all lines of insurance have the same characteristics and that some classes, particularly amongst personal lines, may have significant transactional elements to them. Similarly, some investment banks may be involved in highly strategic business lines. Low-frequency–high-severity events, however, present an equally relevant challenge to both banks and insurers (Wei, op. cit.).

2.1.4 As a concluding remark in his paper, Acharyya (op. cit.: 48) makes the thought-provoking and debatable statement that insurers should not necessarily strive to reach the levels of operational-risk appreciation seen in banking institutions, believing that "unlike banking, operational risk in insurance is not a major area of concern."

2.2 REGULATORY FRAMEWORK

2.2.1 The Regulatory Environment

2.2.1.1 The regulatory environment in the global insurance industry is undergoing significant changes. SAM is intended to bring South Africa in line with Solvency II and will take greater account of risks to insurers, explicitly including operational risk.[9] A recent amendment[10] to the regulatory framework sees the inclusion of a capital charge to be held in respect of operational risk, calculated as a function of gross earned premium and gross technical liabilities.

8 Ernst & Young, 2011, supra
9 Financial Services Board, 2010, supra
10 Board Notice 169, Act 53 of 1998 as amended, Republic of South Africa

2.2.1.2 The SAM regime will take on the same three-pillar approach as Solvency II and likewise will take account of aspects of operational risk under both Pillar I, as part of the solvency capital requirements (SCR),[11] and Pillar II, as part of the own risk solvency assessment (ORSA).[12,13]

2.2.1.3 Under Pillar I, SAM will require that insurers hold an SCR that yields a 99,5% confidence interval of being able to absorb losses against all quantifiable risks incurred within a period of one year, calculated using a value at risk (VaR) approach.[14] Operational risk is to be explicitly included in the SCR calculation.

2.2.1.4 Pillar II aims to assess the efficacy of internal controls and to what extent the corporate governance structure is embedded in the running of the business.[15]

2.2.1.5 Two methods are accepted for the calculation of the operational-risk component of the SCR: the standard formula approach and the internal model approach, the latter of which can be broken into the categories of a full internal model and a partial internal model.[16,17,18]

2.2.2 The Standard Formula Approach

2.2.2.1 The standard formula is intended for insurers writing simple lines of business.[19] All insurers, including those planning to make use of the alternative approach, are, however, expected to be familiar with this approach, as reporting on this basis will be required by the Financial Services Board (FSB) during 2015 and the post-2015 transitional period.[20,21] Insurers will also be required to calculate the standard formula for a minimum period of two years after an internal model has been implemented.[22]

2.2.2.2 The standard formula for the capital requirement relating to operational risks presented by the FSB[23] forms part of the technical specifications for South Africa's first quantitative impact study (SA QIS1).[24]

---

11 Financial Services Board, 2010, supra
12 SAM Steering Committee Position Paper 34 (v 5): Own Risk and Solvency Assessment. Financial Services Board, 2012a
13 ibid.
14 Financial Services Board, 2010, supra
15 ibid.
16 ibid.
17 Financial Services Board, 2012a, supra
18 SAM Steering Committee Position Paper 35 (v 4): Use Test. Financial Services Board, 2012b
19 Financial Services Board, 2010, supra
20 ibid.
21 Solvency Assessment and Management (SAM) 2012 Update. Financial Services Board, 2012c
22 Financial Services Board, 2010, supra
23 SAM Steering Committee Discussion Document 61 (v 1) SCR Standard Formula: Operational Risk, Financial Services Board, 2011a
24 Solvency Assessment and Management: First South African Quantitative Impact Study – Technical Specifications. Financial Services Board, 2011b

2.2.2.3 Under the standard-formula approach, the capital charge for operational risk is calculated as the sum of:

(a) 25% of unit-linked expenses; and
(b) the greater of:
  – the operational-risk charges in respect of premiums earned; and
  – technical provisions held;

subject to a maximum of 30% of the basic solvency capital requirement (BSCR) relating to insurance and reinsurance operations.[25]

2.2.2.4 The operational-risk charges in respect of premiums earned and technical provisions held are both simple linear functions. The full mathematical form of this calculation can be found in Appendix A.

2.2.2.5 The appropriateness of the standard formula is questioned in both academic literature (e.g. Slawski & van den Heever, unpublished) and industry opinion given through the responses to the survey conducted for the purposes of this paper (see ¶4.2.3).

2.2.2.6 Suggested improvements to the standard formula include the incorporation of specific scenarios into the calculation and the use of different parameters to reflect the variation in operational risks associated with different classes of business.[26] Respondents to similar questions for the purposes of the fourth quantitative impact study (QIS4) performed by the Committee of European Insurance and Occupational Pension Supervisors (CEIOPS) provided the following suggestions for the improvement of the standard formula:[27]

– the operational-risk charge should be calculated as a percentage of the BSCR or the SCR;
– the operational-risk charge should be more sensitive to ORM;
– the operational-risk charge should be based on entity-specific sources of operational-risk, the quality of the ORM process and the internal control framework;
– diversification benefits and risk-mitigation techniques should be considered; and
– the formula should be more sensitive to operational-risk events that have occurred in the past and technical provisions should be replaced by the frequency of occurrence of operational-risk events or the cost of those events.

These suggestions are, however, high-level and the authors suggest that further work with the industry is required in order to refine these and come up with a more appropriate alternative.

25 ibid.

26 Solvency Assessment and Management: Report on the results of first South African Quantitative Impact Study. Financial Services Board, 2011c

27 CEIOPS' Report on its fourth Quantitative Impact Study (QIS4) for Solvency II. Committee of European Insurance and Occupational Pension Supervisors, 2008. https://eiopa.europa.eu/fileadmin/tx_dam/files/consultations/QIS/CEIOPS-SEC-82-08%20QIS4%20Report.pdf, 26/04/2013

2.2.3 An Internal Model Approach

2.2.3.1 As an alternative to the standard formula, insurers may apply for approval of a full or partial internal model for the calculation of their SCR. The full internal model is intended to replace the standard formula in its entirety. Companies making use of a full internal model will be required to quantify operational risks using a model-based approach.[28] The partial internal model will be used as a substitute for part, or parts, of the standard formula, such as for one or more business units, or for one or more risk modules.[29] Particular mention is made by the FSB of the use of a partial internal model for the calculation of the capital requirement for operational risk.[30]

2.2.3.2 All internal models will require approval by the regulator.[31] This will be granted on the grounds that a company is able to make use of the same model to determine economic and regulatory capital in accordance with the use test, which forms part of the ORSA (see ¶2.2.4).[32,33] The FSB proposes that an internal model should be embedded in the running of the business and should be used to support and verify business decisions.[34] The stipulation that account should be taken of all relevant and reasonably foreseeable risks to the business for the internal model further emphasises the importance of proper appreciation of the operational risks to which a business is exposed.[35]

2.2.3.3 An entity employing an internal model will require a more universal appreciation of the various components it seeks to model, for example, operational risks. This implies that senior management, as well as the board of directors, of the business are required to have a thorough understanding of the internal model and thus their operational risks.[36]

2.2.3.4 The nature of a firm's operational risks has the potential to form a key component of a firm's decision whether to make use of an internal model or not.[37]

2.2.4 ORSA

2.2.4.1 Every insurance entity, whether stand-alone or part of a group, will be required to produce an ORSA that will be submitted to the regulator at least annually, or when there is a significant change in the insurer's risk profile.[38] The ORSA falls under Pillar II of the SAM regulatory regime, its minimum requirements to form

28 Measuring operational risk, Ernst & Young, 2008
29 Internal Model Approval Process (IMAP) Guide, Financial Services Board, 2011d
30 Financial Services Board, 2012c, supra
31 Financial Services Board, 2011d, supra
32 Financial Services Board, 2010, supra
33 Financial Services Board, 2012b, supra
34 SAM Steering Committee Position Paper 55 (v 2): Internal Models: Statistical Quality and Calibration. Financial Services Board, 2012d
35 ibid.
36 ibid.
37 Ernst & Young, 2008, supra
38 Financial Services Board, 2010, supra

part of secondary legislation. At this stage, however, all requirements are merely recommendations.[39]

2.2.4.2 The FSB[40] states that the ORSA is intended to be an insurer's own individual assessment of its risk-management framework and the resulting capital requirements specific to it. It is officially defined by the SAM Steering Committee[41] as follows:

> The ORSA is defined as the entirety of the processes and procedures employed to identify, assess, monitor, manage, and report the short and long term risks an insurance undertaking (and insurance group) faces or may face and to determine the own funds necessary to ensure that insurers [*sic*] (and groups [*sic*]) overall solvency needs are met at all times and are sufficient to achieve its business strategy.

2.2.4.3 It aims to address the need for the board and senior management to have an appreciation of the risks to which the insurer may be exposed by providing an assessment of all material and foreseeable risks and the resultant capital requirements.[42] These risks include, among other things, operational risks.

2.2.4.4 The FSB has recommended that an insurer have a system of identifying and collecting information about current and future risks across all organisational and operational levels. The dependencies and interrelationships between various risks should be captured in this system and reported in the ORSA. Both qualitative and quantitative risks should be captured.[43]

2.2.4.5 The ORSA requires a clear risk-appetite statement in respect of all risks, including operational risks, on which business strategies must be based. Adequacy of current and future economic capital resources given this risk appetite and tolerance level should also be considered, in particular under stressed conditions.[44] For the purposes of this assessment, the FSB recommended explicitly that scenario analysis and stress testing be used, both for individual risk categories that may be difficult to quantify, such as operational risk, as well as across risk categories in order to capture their interdependence. The results of these analyses are to be included in the ORSA.[45]

2.2.4.6 Insurers are likely to consider seriously the use of an internal model for the calculation of their economic capital in respect of operational risk, despite the calculation of SCR under Pillar I using the standard formula. This is because the standard formula is unlikely to adequately reflect the risk profile of insurers.[46] The difference in the calculation methods for the SCR under Pillar I and Pillar II will, however, need to be

39 Financial Services Board, 2012a, supra
40 ibid.
41 ibid., page 17
42 Financial Services Board, 2010, supra
43 Financial Services Board, 2012a, supra
44 ibid.
45 SAM Steering Committee Position Paper 54 (v 3): Internal Models: Governance. Financial Services Board, 2012e
46 Financial Services Board, 2012a, supra

explained and justified.[47] Although the economic-capital model for operational risk will not have to meet the same criteria as those used for the calculation of regulatory capital, the following should be considered when using an internal model under the ORSA:[48]

– risk categories should be clearly identified and documented;
– sources of data should be identified and the controls around the integrity of the data should be explained;
– methods used in identifying and analysing risks for economic-capital purposes should be justified and documented;
– economic-capital requirements should be sufficient to meet the insurer's policyholder liabilities;
– assumptions should be explained as well as the sensitivity of the results to these; and
– the model should be periodically reviewed by an independent party.

2.2.4.7 In discussing the quantification and management of operational risks in banks, Embrechts, Furrer & Kaufmann (op. cit.) concludes that greater emphasis should be placed on the Pillar II framework of Basel II than that placed on the quantitative aspects under Pillar I. One can infer that the same would be true for ORM in the case of insurers.

2.3 A FRAMEWORK FOR THE MANAGEMENT OF OPERATIONAL RISK

The ultimate goal in ORM is to be able to predict potential losses so that action can be taken before it is too late (Haubenstock, 2003). The first and most important element in any risk-management exercise is the determination of an holistic risk-management

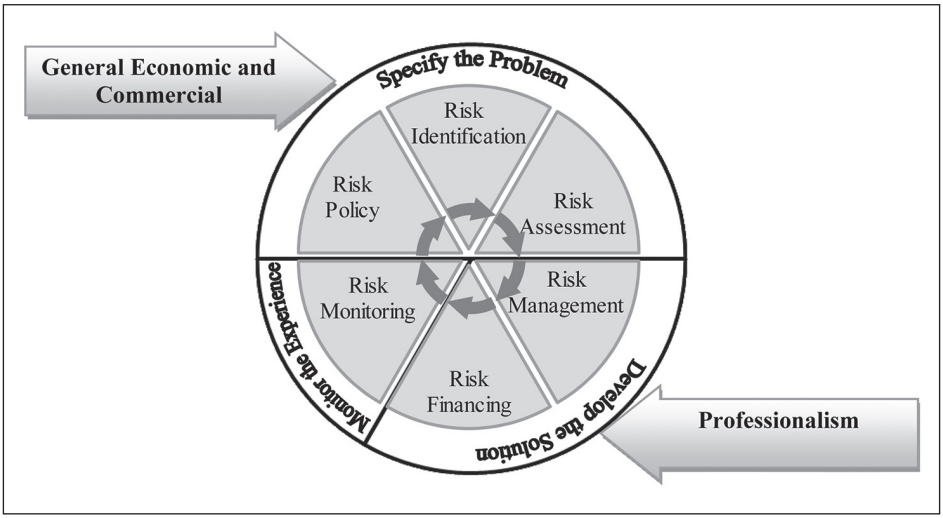

Figure 1. Actuarial control cycle: ORM framework

47 ibid.
48 ibid.

framework that works in the business (Tripp et al., op. cit.). The precise elements in an ORM framework differ slightly in the literature; however the scope of their coverage is largely the same. The framework presented below is structured according to the actuarial control cycle. It is an amalgamation of ideas presented by Lam (op. cit.), Tripp et al. (op. cit.) and Slawski & van den Heever (op. cit.).[49] In this section, each of the above stages of the risk framework is outlined.

2.3.1 Specify the Problem: Risk Policy

2.3.1.1 At the outset of the establishment of an ORM framework, a company should establish what it would like to accomplish and devise a high-level strategy of how it would like to achieve these objectives (Lam, op. cit.).

2.3.1.2 Further, it is suggested by Lam (op. cit.) that a written policy document should be produced detailing, in a manner that is understood by all parties involved in the risk management process, the following:

- principles for managing operational risk, for example, the levels at which risks are deemed to be acceptable, tolerable and intolerable and the recommended course of action for risks assigned to each of these categories;
- a definition and taxonomy of 'operational risk', including what is included and excluded in the company's definition of an 'operational risk', the categories and subcategories of operational risks and the classification system for the severity of operational risks e.g. red, amber, green;
- objectives and goals, both overarching and risk-specific;
- organisational structure, with details on the key committees, memberships and charters as well as the preferred communication lines between the board, senior management, line management, risk management and oversight groups; and
- roles and responsibilities, for example, detailing that the board is responsible for establishing policies and ensuring appropriate resources and controls are in place, and setting out the requirements for every employee to be aware of the operational risks that may arise in the area of work in which they are involved.

2.3.1.3 Risk appetite is the amount of risk an organisation is prepared to accept in pursuing its financial or other strategic objectives.[50] The articulation of an organisation's risk appetite is required under Pillar II of the SAM framework within the ORSA (see ¶2.2.4.5). This is consistent with the view of the Institute of Operational Risk[51] that regulators should take an interest in risk appetite because of its importance to governance and stability. A risk appetite should be expressed in such a way that it is measurable

49 original outline borrowed by Slawski & van den Heever (unpublished) from the 2009 Amlin Annual report

50 KPMG Issues and Insights Report, April 2012. www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/risk-appetite-operational-risk-reserves.pdf

51 Operational Risk Sound Practice Guidance – Risk Appetite. Institute of Operational Risk, 2009. www.hayderisk.com/IORRiskAppetiteSPGVersion1.pdf, 06/10/2012

and unambiguous. It should, however, always remain a matter of judgement, rather than simply a calculation.[52]

2.3.1.4 Some of the benefits in defining a risk appetite, as identified in IOR (unpublished), include:

- enabling the board to exercise appropriate oversight and corporate governance;
- promoting a risk-aware culture in the organisation;
- establishing a decision-making tool in the risk-management framework for determining which risks are to be retained, mitigated, controlled and avoided;
- improving the efficiency and appropriateness of allocation of resources, both financial and managerial; and
- encouraging more conscious and effective risk-management practices.

2.3.1.5 Industry practice suggests that, in general, it would be most appropriate that the risk policy and the company's risk appetite be determined by the chief risk officer and the company's risk committee. Using a top-down approach, a high-level risk policy and appetite should be approved by the board of the company (IOR, op. cit.). The risk appetite can then be allocated to the various business divisions through consultation with division leaders. In order to contextualise this process, it is suggested by the authors that the risk policy should also be adapted for each business division to suit its unique characteristics and should be worded in such a way that all members of the division are able to understand its objectives.

2.3.1.6 An example of a high-level operational risk-appetite statement provided by the IOR (op. cit.) is the acceptable level of economic capital that can be allocated to operational risk, based on an objective measure. For a processing-error operational risk mentioned by Dexter et al. (op. cit.), an example of a risk-appetite statement at a business-division level would be the specification of an acceptable probability of one or more claim-processing error per one thousand claims received.

2.3.2 Specify the Problem: Risk Identification

2.3.2.1 A robust and comprehensive risk-identification process is fundamental to the capital assessment and overall management of operational risks (Dexter et al., op. cit.).

2.3.2.2 As part of the identification process, a firm should adopt a classification system for the operational risks to which it may potentially be exposed (Haubenstock, op. cit.). This could be likened to the creation of a common language to be understood throughout the firm (ibid.). Tripp et al. (op. cit.) propose that this will assist in placing risks within coherent groups and will provide a structure to the risk-reporting process. The Basel Committee makes use of four broad risk categories, namely process risk, people risk, system risk and event risk.[53] Dexter et al. (op. cit.) suggest that firms should

52 Ernst & Young, 2011, supra

53 Working paper on the regulatory treatment of operational risk. Bank for International Settlements, Basel Committee on Banking Supervision, 2001

then further divide these categories into levels of sub-risks which reflect their individual characteristics. The Basel Committee suggests a categorisation of loss events into seven level 1 and twenty level 2 events, as presented in Appendix B,[54] such as theft and fraud under both the internal- and external-fraud categories, and improper business or market practices under clients, products and business practices. For insurance business, it is suggested by industry participants that the classification system used by the Operational Risk Consortium (ORIC) (see ¶2.6.1.3 and Appendix B) be used.[55] Under this system, the example in ¶2.3.1.6 would fall under the category 'Execution, Delivery and Process Management', in the subcategory 'Transaction Capture, Execution and Maintenance' and could be either a customer-service failure or a transaction-system error, depending on the nature of the risk event itself.

2.3.2.3 Dexter et al. (op. cit.) recognises, however, that there are numerous alternative ways in which operational risks may be classified and that the actual method of categorisation is material; it should fit in with the business's management practices and should be sufficiently detailed so as to include all of a firm's risks. A justification of this classification should also form part of a firm's ORSA.[56] For completeness, it is suggested that a firm compare its operational-risk list to an industry-wide equivalent (Dexter et al., op. cit.).

2.3.2.4 Risk identification should be performed at a high level by business management as well as throughout the lower levels of the organisation, so as to provide a complete view of potential threats (Dexter et al., op. cit.). To facilitate the identification process further, risk personnel are often embedded within business lines (Tripp et al., op. cit.).

2.3.2.5 Dexter et al. (op. cit.) outline further techniques that can be used in the risk-identification process, including, amongst other things:

- presentations on the end-to-end ORM process to both senior management and individual business divisions, with the aim of creating company-wide appreciation for its importance;
- one-to-one meetings with key individuals within each business division to identify potentially sensitive or confidential operational risks within the division;
- brain-storming sessions involving both risk personnel and teams within business divisions to facilitate self-assessment and evaluation of potential risks; and
- scenario workshops, in which the results of the previous meetings are used to create a set of coherent risk scenarios that can be used to provide a structure for later stages of the risk-management framework.

2.3.2.6 To illustrate the possible application of the above techniques, the example outlined in ¶2.3.1.6 can be extended. Here the risk-identification exercise may begin with a presentation on operational risk to claims personnel and to the information

54 ibid.
55 CEIOPS, supra
56 Financial Services Board, 2012a, supra

technology (IT) personnel who are responsible for the claims management system. Once an understanding of operational risks has been achieved within these divisions, brain-storming sessions are held, in which all claims and relevant IT staff put forward ideas of things that could potentially go wrong within their function. Risk personnel assist managers in identifying a set of scenarios from the results of the brain-storming sessions. In this case, an example scenario could be a long-term shut down or failure of the claims-management IT system leading to a significant period in which claims cannot be processed on the system and must be delayed or done manually, potentially leading to errors.

2.3.2.7 Preliminary key risk indicators (KRIs) should also be defined as part of the identification process and updated as the framework progresses (Dexter et al., op. cit.). KRIs are quantitative measures that represent operational-risk performance for specific business units and processes and aim to provide an early indication of a potential loss so that corrective action can be taken to prevent it (Lam, op. cit.). If assigned to each risk scenario, these will allow for a more objective measure of the company's progress in their management of operational risks (Dexter et al., op. cit.). A KRI for the example in ¶2.3.1.6 could be the number of customer complaints—as the number of customer complaints increases, the probability of the existence of a systemic problem is likely to rise.[57]

2.3.2.8 Having broadly identified and categorised the operational risks to which an organisation is exposed, Dexter et al. (op. cit.) suggests that an initial frequency–severity assessment of each of these categories can assist in the prioritisation of risks and in the construction of a risk-assessment matrix to be used in later stages of the framework. In practice, this step could form part of the scenario workshops mentioned in ¶2.3.2.5.

2.3.3 Specify the Problem: Risk Assessment & Measurement

2.3.3.1 In this section a more detailed assessment of operational risks is discussed. Assessment and measurement of risks involves gaining a greater understanding of the impacts and losses that may arise from operational-risk events, as well as the frequency of their occurrence. Dexter et al. (op. cit.) suggest that this is particularly important prior to the capital assessment of a firm.

2.3.3.2 Lam (op. cit.) and Haubenstock (op. cit.) propose that a large range of qualitative and quantitative assessment tools should be used to investigate operational risks in a business. The two most common approaches discussed in the literature are the purely data-driven loss distribution approach (LDA) and the scenario approach.

2.3.3.3 The LDA approach involves the parametric estimation of a frequency and severity distribution for individual loss types as well as their aggregation, taking into account dependencies. The scenario approach makes use of statistical models to quantify risks that are calibrated by qualitative measures (Brandts, unpublished).

57 Institute of Operational Risk, https://www.ior-institute.org/sound-practice-guidance/key-risk-indicators

2.3.3.4 The models used to quantify operational risk may either be top-down models or bottom-up models (Lam, op. cit.). A top-down model centrally measures operational risk across the whole business without explicit consideration of individual business units or risks.[58] This calculated overall risk and its resulting capital requirement are then proportionally allocated across business units (Lam, op. cit.). A bottom-up model creates predicted loss expectancies for each constituent of operational risk, based on historical and other relevant data, and aggregates these to provide a total estimate of operational-risk exposure (Lam, op. cit.).

2.3.3.5 In order to inform this process, a number of authors (for example Haubenstock, op. cit.) promote the development and maintenance of an internal loss database by a business, taking note of operational losses as well as near-miss events. Near-miss events are defined by Selvaggi (op. cit.) as cases in which operational controls failed but financial losses did not materialise. External databases are discussed by Dexter et al. (op. cit.), amongst others, as an alternative or supplementary source to that collected internally. Several papers —for example Guillen et al. (2007), Baud, Frachot & Roncalli (unpublished) and Peters, Shevchenko & Wüthrich (2009)—consider statistical methods for the statistical modelling of operational risks based on a combination of these two sources.

2.3.3.6 Lam (op. cit.) and Dexter et al. (op. cit.) suggest that alternative methods of operational-risk assessment that do not rely on historical data can be of equal, and complementary, value to the process. The most notable of these is the scenario approach mentioned in ¶2.3.2.5. Although it is possible that historical data could be used to inform the scenario estimates, it is more likely that expert opinion injected into scenario workshops will provide a better view of scenario events. Participants could be asked to consider possible losses over various return periods of each scenario and to estimate the magnitude of these, i.e. consider a one-in-ten loss and a one-in-a-hundred loss for the same scenario. When participants do not come from a quantitative background, Dexter et al. (op. cit.) suggest that a categorisation of events be performed according to frequency and severity scales; for example, four frequency options could be presented that range from extremely remote to likely, and similarly for severity. After risk and actuarial adjustment and verification, the loss estimates and scenario characteristics could inform points on a statistical distribution, from which the full distribution of losses can be inferred.

2.3.3.7 A likely, or one-in-ten loss, for the scenario of a failure in the claims-IT system (see ¶2.3.2.6) may be the cost of two days' lost productivity plus the cost of some reputational damage as a result of consumer dissatisfaction with delays in claim processing. A rare, one-in-a-hundred event in the same scenario may be a power surge through all claims-IT systems and backup servers resulting in the total loss of existing claims data and the ability to process new claims. This may result in losses including, among other things, the cost of significant lost productivity and the cost of recovery and recapture of lost data, as well as the cost of any regulatory actions due to extreme customer dissatisfaction that may result.

58 http://media.wiley.com/product_data/excerpt/62/04700588/0470058862.pdf

2.3.3.8 Lam (op. cit.) identifies other sources of information for risk identification and assessment such as:

- internal audit reports;
- external assessments (external auditors and regulators);
- employee exit interviews;
- customer surveys; and
- complaints.

2.3.4 Develop the Solution: Risk Management

2.3.4.1 Lam (op. cit.) considers that the assessment and measurement of operational risk has very little value unless it is used to improve the management of operational risks. Likewise Cope et al. (2009) advocate a strong link between the process of risk management and the measurement and modelling of operational risks; this was found by Cope et al. (op. cit.) to be lacking in operational-risk regimes.

2.3.4.2 Rigorous and detailed ORM has the potential to minimise day-to-day losses and reduce the likelihood of more costly incidents (Lam, op. cit.). It allows for a greater focus on the revenue-generating activities of a firm, thus increasing its ability to achieve its business objective.

2.3.4.3 At the management stage, a firm would decide which action is most appropriate for the identified risks, based on the results of its assessment, bearing in mind its original objectives and policies, and a risk–reward profile (Haubenstock, op. cit.).

2.3.4.4 Effective risk control is seen by Slawski & van den Heever (op. cit.) as a fundamental key to risk mitigation. Haubenstock (op. cit.) focuses on the importance of optimal controls, recommending that the effectiveness and cost of each control be considered in conjunction with each other. It is noted that in cases where the costs cannot be justified, alternative, perhaps less optimal controls, may be explicitly decided upon.

2.3.4.5 Operational risk capital too plays a role in management controls; Dexter et al. (op. cit.) argue that a primary objective of operational risk capital should be to improve the effectiveness of the management controls undertaken to respond to a risk. The quantification of the costs associated with a risk translates the risk into terms that the primary decision-makers can understand. They can then consider the costs against the benefits of possible controls. In order to mitigate the risks of the example events described in ¶2.3.3.7, the company could invest in a back-up system, stored in a different location to the primary system, so that day-to-day processing can continue should the primary system temporarily fail. Additionally, all data could be backed up to an offsite server periodically so as to ensure that total data loss is virtually impossible. These solutions may, however, be expensive, and thus the company may choose to only have a small-scale back-up system or may choose to back up only the most critical data to the offsite server.

2.3.4.6 As a final stage of the management process, a risk register should be produced detailing all identified and assessed risks along with the management or control procedure applied. In most instances, risks will be recorded net of controls, however, in some instances it may be appropriate to record the risk prior to controls (Tripp et al., op.

cit.). This is particularly important in cases where the net risk and gross risk are vastly different, as this indicates a high reliance on effective controls (Dexter et al., op. cit.).

2.3.4.7 Acharyya (op. cit.) asserted that there is still much work to be done towards the improvement of the management of operational risk. Acharyya (op. cit.) argued that the management of operational risk cannot be effective until the subjectivity associated with operational risks is acknowledged and appropriately dealt with. In addition, Acharyya (op. cit.) expressed concern at his findings that the current practice of ORM remains largely separate from other risk-management functions within a firm and that, in many cases, quantification exercises for operational risk have little impact on decision-making and business management as a whole. At present, insurers appear concerned with operational risk merely from a regulatory point of view, instead of considering the profit and value creation that properly managed operational risk could lead to (Archaryya, op. cit.).

2.3.4.8 This stage of the risk-management cycle forms the basis of the ORSA assessment for SAM.

2.3.5 Develop the Solution: Risk Financing

2.3.5.1 The determination of the appropriate financing strategy for operational risk is not limited to the calculation of regulatory capital, or even the calculation of risk-based economic capital appropriate for the business. The financial implications of all aspects of the risk-management process should also be considered when determining an optimum strategy (Acharyya, op. cit.).

2.3.5.2 Tripp et al. (op. cit.) recognise that the costs of implementing a risk-management framework are not limited to the costs involved in control implementation mentioned in ¶2.3.4.4. These costs would include the costs in both management time and resources. In agreement, Acharyya (op. cit.) advocates that a 'risk–reward trade-off' approach be considered when determining the detail and scope of the process of understanding operational risks in a firm, suggesting that the benefits of the ORM process are directly dependent on how well the trade-off is managed.

2.3.5.3 Under SAM, the financing of operational risks takes place through the retention of capital, the specifications of which fall under Pillar I (see ¶¶2.2.1.3, 2.2.2.3 and 2.2.3). Although firms making use of the standard formula will not have to make use of an internal model for the purpose of regulatory capital, the FSB[59] has indicated that it hopes many will do so for the calculation of their economic capital allowance.[60]

2.3.5.4 Dexter et al. (op. cit.) surmise that sufficient capital should be held for operational risks that have the potential to affect a realistic balance sheet, and that regulatory requirements may necessitate the holding of operational risk capital greater than the true economic costs of an event. Haubenstock (op. cit.) reasons that, if the standard formula results in this inflated charge, banks will be incentivised to make use of their version of an internal model, termed the 'Advanced Measurement Approach'.

59 Financial Services Board, 2010, supra
60 ibid.

Equivalently, this implies that insurers would be incentivised to use an internal model, should it lead to a lower capital charge than the standard formula. The costs of implementing an internal-model approach for the calculation of regulatory capital may, however, negate any savings in capital charges, and thus would need to be considered in relation to the company's opportunity cost of capital (Dexter et al., op. cit.).

2.3.5.5 Respondents to QIS4 reported that the reverse may also occur, i.e. certain insurers found that the standard formula resulted in a lower operational risk-capital charge than their internal models.[61] Where this is the case, an insurer would prefer to make use of the standard formula as it would reduce the physical capital it would have to hold, and therefore the cost of capital. The requirement for an insurer to produce an ORSA, however, should limit this potential for regulatory arbitrage.

2.3.5.6 Doubts are raised by Acharyya (op. cit.) as to the appropriateness of holding capital to back operational risks. Instead efforts should be focused on improving the base of operational understanding so that more effective controls can be implemented. These sentiments are similar to those mentioned in ¶2.2.4.7 and are echoed by the South African industry as shown in the responses to the industry survey performed for the purposes of this paper (see ¶4.2.2).

2.3.6 Monitor the Experience: Risk Monitoring

2.3.6.1 The monitoring of operational risks should be an ongoing process through which the insurer is able to gain feedback on the effectiveness of earlier stages in the control cycle (Lam, op. cit.; Haubenstock, op. cit.).

2.3.6.2 Dexter et al. (op. cit.) advocate embedding risk personnel within business lines in order to facilitate continual monitoring of operational risks and accurate and timely reporting of potential threats, indicating that an operational-risk manager be appointed to oversee the process. Lam (op. cit.) states that monthly committee meetings should be held to ensure that a coordinated approach to ORM is followed.

2.3.6.3 Tripp et al. (op. cit.) promote the use of a comprehensive set of KRIs (see ¶2.3.2.7). KRIs are generally specified along with corresponding escalation triggers (Tripp et al., op. cit.), which provide a minimum level of acceptable performance of the KRI. Once this level has been breached, an escalation report is immediately sent to senior management and corrective action is automatically launched (Lam, op. cit.). KRIs form an effective part of qualitative risk and risk-control assessment (Tripp et al., op. cit.). Additionally, KRIs have the potential to promote a risk-awareness culture in an organisation, as it is easy to link performance penalties and bonuses to them (Tripp et al., op. cit.). A more sophisticated KRI for the example of claims-processing error, as opposed to that mentioned in ¶2.3.2.7, may be the result of daily checks on claims-processing status and reports on IT-system status.

2.3.6.4 Reporting on operational risks falls into this aspect of the framework. Haubenstock (op. cit.) notes that whilst reporting is needed at all levels of an organisation, it should be tailored to each business area. This is done so as to afford senior management

61 CEIOPS, supra

a consolidated view and to turn their attention to areas that may have been overlooked in previous assessments of the business.

2.3.6.5 The presentation of this process as cyclical in nature highlights the need for regular amendments to each phase, based on experience in subsequent phases that are identified through this monitoring process. Risk-management standards should never be regarded as a static concept.[62]

2.3.7 General Economic and Commercial Environment

Numerous operational risks that may be faced by an organisation are systemic to the insurance industry as a whole. It is therefore recognised by Haubenstock (op. cit.) that regular monitoring of trends in the external environment and within the industry serve to better inform the risk-management process.

2.3.8 Professionalism

2.3.8.1 There is a growing appreciation for the benefits of the involvement of the actuarial profession in ORM. Whilst it is necessary for the actuary to act within the general framework of professional conduct, there is little in the way of specific professional guidance on the topic. Section 6.10 of SAP 104 of the Actuarial Society of South Africa (ASSA) makes reference to an appropriate level of capital to be held to cover operational risks, but does not offer detailed guidance. No mention of operational risk was found in guidance notes specific to general insurers. In a separate document available from ASSA,[63] suggestions are made for the allowance for operational risk under the current regulatory-capital calculations, known as 'Capital Adequacy Requirements' (CAR). That document proposes the Solvency II (or equivalently SAM) standard formula as a starting point, but where this is found to be inappropriate, a range of factors should be considered before settling on the allowance.

2.3.8.2 The guidelines by ASSA promote the establishment of a formal risk-management framework, as described above. It is noted that care should be taken not to consider risks that may be immaterial or that are fully covered elsewhere in the CAR. The same is likely to apply in guidance under SAM.

2.4 USES OF OPERATIONAL-LOSS DATA

Historical loss data have the potential to inform every step of the risk-management process; Tripp et al. (op. cit.) goes as far as to say that some form of data collection is vital for ensuring its effectiveness. In this section, the uses of loss data in relation to the aforementioned regulations and ORM framework are discussed, along with brief commentary on the limitations of loss data.

62 www.centriq.co.za

63 Suggested Guidelines for Operational Risk Allowance, v 1.2, December 2009 www.actuarialsociety.org.za

2.4.1 Regulation

2.4.1.1 Much of the innovation in the field of operational risk is a result of the move in regulation to more risk-based regimes (Selvaggi, op. cit.). As part of the ORSA process, insurers are encouraged to develop a system of capturing internal data (see ¶2.2.4.4), as well as to utilise and document any additional sources of data. Scenario analysis and stress testing are also recommended by regulators for the ORSA (see ¶2.2.4.5). In ¶2.4.4, the use of data for scenario analysis is discussed.

2.4.1.2 The FSA and the European Insurance and Occupational Pensions Authority have both identified operational-risk consortia as important sources of information, both for ensuring the statistical quality of databases for the processes of approval of internal models and for guiding general business decisions (Selvaggi, op. cit.).

2.4.2 Risk Identification

At the most basic level, historical loss data provide a reference for insurers when initially identifying risks. In particular, data from external sources may alert firms to risks that would otherwise not have been considered (Dexter et al., op. cit.). Selvaggi (op. cit.) proposes that insurers use a single, standardised classification system, such as described in ¶2.3.2.2, to classify these risks to ensure its completeness and to maintain consistency across the industry.

2.4.3 Risk Assessment: Statistical Modelling

2.4.3.1 In much of the actuarial literature around the modelling of operational risks, the frequency–severity model is discussed. Under this approach, a separate model is developed to forecast both the number of loss events that may occur, and the magnitude of the loss, the parameters of which are usually derived by fitting distributions to observed loss data. (Tripp et al., op. cit.). Dexter et al. (op. cit.) caution, however, that it is unlikely that internally observed loss data will be sufficient on their own.

2.4.3.2 The skewness and multimodality in the distribution of operational losses suggests the use of extreme-value theory for the modelling of larger losses (Tripp et al., op. cit.; Guégan, Hassani & Naud, 2011). This approach allows for a better estimate of the tails of the distribution by ignoring most of the underlying data (Tripp et al., op. cit.). A limiting factor to the application of this approach is the particular shortage of low-frequency–high-impact data, even in situations where loss data towards the central areas of the distribution may be sufficient.

2.4.3.3 Cope et al. (op. cit.) identify a few disadvantages to the use of data-based models for operational risk. Firstly, it is noted that, even in the presence of a large amount of loss data, an extreme loss can severely alter the characteristics of the distribution. Secondly, Cope et al. (op. cit.) also show that the amount of data needed to estimate a 99,9th percentile of the annual loss distribution, the level at which banks are required to hold capital under Basel II, is impracticably high without extrapolation. The level of capital that insurers are required to hold is lower than that of banks—set at the 99,5th percentile of the annual loss distribution—however, it is likely that the conclusions of Cope et al. (op. cit.) will still apply.

2.4.4 Risk Assessment: Scenario Analysis

2.4.4.1 When evaluating operational risk by means of scenario analysis, Tripp et al. (op. cit.) outline two types of events to be considered: historical events and hypothetical events. Selvaggi (op. cit.) is of the opinion that operational-loss data, both those collected internally and those obtained externally, provide an indispensable tool to inform the construction of these scenarios. These loss data allow for historical events to be included in the scenarios and provide a source of information that allows for the creation of realistic hypothetical events.

2.4.4.2 Stress testing and scenario analysis are practical and understandable methods. The attraction of scenario analysis lies in its effectiveness and practicality in dealing with problems that arise from the use of internal and external loss data.[64] It is promoted as an alternative quantification tool in instances in which a probability distribution is impossible or impractical to construct. An improved systematic use of scenarios is seen by Cope et al. (op. cit.) as a way in which the scarcity of operational-loss data may be overcome. Scenario analysis is seen as an invaluable forward-looking tool, even if an insurer has access to good loss data, as it may serve to inform hypothetical events that an insurer believes could occur in the future.

2.4.4.3 Scenario analysis may, however, require significant judgement and experience, and may need to incorporate external advice.[65] Ernst & Young[66] warns that the scenario-analysis processes should not be too complex. The same study remarks that it should be consistently applied throughout the group, taking heed of the risk appetite and strategic direction of the company along with the business environment in which it operates.

2.4.5 Risk Management

2.4.5.1 Operational-loss data, as well as the resultant models and scenarios, provide a decision-making tool for risk managers when investing in processes to reduce risks (Cope et al. (op. cit.). Even if data are not sufficient to obtain an accurate projection of the magnitude of a potential operational loss, they may assist in identifying which risks require the most immediate action.

2.4.5.2 Dexter et al. (op. cit.), along with Lam (op. cit.), suggest that every loss and incident within a company, or the industry, represents a learning opportunity which has the potential to improve risk management in the future. Regular and systematic recording of past experiences, for example in a database, will not only facilitate the sharing of this opportunity within the company, but also allows for the preservation and accumulation of lessons despite personnel turnover and the passage of time (Levitt & March, 1988).

---

64 Ernst & Young, 2011, supra

65 Selvaggi, Sound Scenarios, www.risk.net/operational-risk-and-regulation/feature/ 1603369/ sound-scenarios

66 Ernst & Young, 2011, supra

2.4.5.3 The importance of organisational learning is widely discussed in the literature (see, for example, Cyert & March,1963). Levinthal & March (1993) suggest that learning from the past increases a firm's average performance as well as its reliability. Collis (1996) views the accumulation of knowledge and learning as an intangible asset to a firm with the potential to give it an advantage over its competitors and enhance its evolution. In the context of risk management, this would mean that companies who more effectively take heed of past operational losses will be better able to manage or avoid their consequences in the future.

2.4.5.4 Although the identification of the causality of an event may be difficult, it is this that provides the greatest insight to firms on what to look out for and what actions to take to avoid adverse occurrences, or to promote positive outcomes (Levitt & March, op. cit.).

2.4.6 Risk Monitoring

The collection of internal loss data allows a firm to monitor its operational-risk experiences more objectively over time. This will allow for an assessment of control effectiveness and should serve to highlight deficiencies in the previous period's risk-management process (Dexter et al., op. cit.). By comparing internal experiences with external data over a comparable period, a firm will be able to better isolate firm-specific losses from those that were systematic to the industry (Haubenstock, op. cit.).

2.4.7 Limitations of Operational-loss Data

Peters, Shevchenko & Wüthrich (op. cit.), along with numerous others, refer to the wide recognition that operational losses cannot be estimated solely on the basis of historical losses. Dexter et al. (op. cit.) elaborate on this point by raising concerns as to the resemblance of future losses to those of the past, thus questioning whether past data will be useful for future predictions. There is a constant change in the regime of insurers, as new policies and controls are introduced to reduce operational risks (Peters, Shevchenko & Wüthrich , op. cit.). In discussing low-frequency–high-impact or black swan events, Taleb, Goldstein & Spitznagel (2009) express significant concern about the act of trying to predict these, particularly by using history as a primary source of information. It was proposed that the prediction of black-swan events, whether they be operational-risk events or otherwise, is impossible (Taleb, Goldstein & Spitznagel , op. cit.).

2.5 SOURCES OF OPERATIONAL-LOSS DATA

In this section, the two main types of loss data are reviewed: internal loss data and external loss data. The process of combining data from different sources is then discussed briefly.

2.5.1 Internal Operational-loss Data

2.5.1.1 The most obvious source of information on which an insurer may base its operational-risk assessment is its own previous operational-loss experience. Dexter

et al. (op. cit.), Tripp et al. (op. cit.) and Lam (op. cit.), among others, advocate the recording of such events in an internal loss database.

2.5.1.2 Practices that would increase the applicability and usefulness of internal data include the capture of near-miss operational-risk events (Dexter et al., op. cit.) as well as other incidents that may have relevance to operational risk (Lam, op. cit.), and the recording of any correlations between loss events and indicators. A cause-and-consequences approach is preferred as this will avoid double counting and duplicated recognition of losses (Dexter et al., op. cit.; Tripp et al., op. cit.).

2.5.1.3 The potential benefits of internally sourced data lie with the availability of firm-specific data that, if allowance is made for internal controls improvements, should offer some indication of future experience (Dexter et al., op. cit.).

2.5.1.4 Specific advantages of an internal loss database have been discussed in the literature, extending far beyond the mere modelling of events. As an information tool, Dexter et al. (op. cit.) foresee benefit in identifying the aforementioned near-miss events, allowing for a greater appreciation of the impact of an operational-loss event on other risk categories and providing scenarios to be used in the assessment of capital allocation to operational risks.

2.5.1.5 Concerns do, however, arise with the use of this data source; primarily, the applicability of past events to future experiences is questioned (Dexter et al., op. cit.). Moreover, it is pointed out that internal databases suffer from bias because of internal collection problems and because not all risk events are captured, as they are unlikely to all have occurred within the firm and may take a long time to crystallise (Selvaggi, op. cit.).

2.5.1.6 Although an internal loss database is conceptually simple, if there are no commonly agreed measures of exposure to operational risk in a firm, it will be much more difficult for it to accurately collect its own exposure data (Tripp et al., op. cit.). It is therefore apparent that data-based modelling goes hand-in-hand with a well-designed ORM framework.

2.5.1.7 The costs of implementing and running an internal operational-risk database may be an adverse factor (Dexter et al., op. cit.). These will have to be compared with the potential benefits of having data readily available for modelling and capital assessments.

2.5.2 External Operational-loss Data

2.5.2.1 Throughout the literature on the modelling of operational risk, the problem of the lack of sufficient and suitable loss data is echoed, even when internal data have been collected (see for example Frachot & Roncalli, unpublished; Guillen et al., op. cit.). The primary problems with internal loss data were discussed in ¶2.5.1.5. In the light of these problems it is suggested that data collected internally be supplemented with external data for both frequency and severity of operational losses (Frachot & Roncalli,op. cit.; Guillen et al., op. cit.). External databases allow for an increase in the availability of data, particularly in the high-severity–low-frequency region, which serves to facilitate more complete measurement and analysis of operational risks faced by a firm

(Dexter et al., op. cit.). This is of particular relevance for insurers when extrapolating to higher-return periods, such as the one-in-two-hundred event required for regulatory purposes (Gustafsson, 2010).

2.5.2.2 Selvaggi (op. cit.) identifies three sources of external loss data, namely:

- publicly-available losses—databases of operational losses that were documented in the public domain because of their severity or high public profile;
- commercial databases using proprietary loss data—databases created by a third party as a product to be sold, which contain information not necessarily in the public domain, sourced by the database owner from an involved party in the operational-loss event, for example, an insurer, and made available for purchase by others; and
- consortium-based loss data—databases created as a collective industry resource, which are managed by industry organisations and to which subscribing members contribute their own loss data and receive the pooled data and reports that are not commercially available in return.

2.5.2.3 The degree of confidence one may place in each source differs. A recent study[67] surmises that consortium-based data are more consistent and are subject to more rigorous checking than publicly collected data. The same study suggests that the nature of the data also differs, consortium-based databases including legally sensitive events that may not be publicly available. Selvaggi (op. cit.) discusses the threshold above which data are included in the various databases and reveals that for public and commercial databases this is set at approximately one hundred times the level of consortium-based databases. This implies that public and commercial databases only capture the most extreme of events, which may only be applicable to the larger firms in the industry, whereas consortium-based databases offer a broader, more complete view of the operational losses experienced by member firms.

2.5.2.4 The benefits of an industry-wide consortium-based database extend beyond the mere supplementation of data; Cope et al. (op. cit.) hold the view that initiatives such as these serve as an incentive for the enhancement of internal loss collection and management systems in order to become compliant with the high standards set by their administrators.

2.5.2.5 Dexter et al. (op. cit.) imply that the source of the external data is likely to dictate the use to which it is most suited, based on the characteristics of the data themselves, and the relevance of the particular data source to the entity concerned. Selvaggi (op. cit.) suggests that consortium-based loss data are suitable for both scenario analysis and loss-distribution modelling. Because of the aforementioned threshold differences it can be inferred that commercial and external data may be better suited to informing extreme events of a scenario. These sources may therefore best serve to provide greater insight into the tails of the loss distributions created from internal and consortium data. ¶2.5.3 discusses in greater detail how these sources of data can be combined.

67 Ernst & Young, 2011, supra

2.5.2.6 There are, however, challenges with the use of external loss data. Dexter et al. (op. cit.) provide a number of reasons why the comparison of operational risk between firms is not straightforward and may give rise to bias in the analysis of an individual insurer's operational risks:

- firms will have different categorisations of risk and different assumptions of implicit coverage in other risks;
- firms are of different sizes and sell different products;
- the control environment will be different for each firm;
- the back-book of each firm has a different profile of products; and
- even generic risks will vary significantly between firms.

In summarising the above points, Acharyya (op. cit.) finds that a consortium-based database may represent the culture of a particular subscriber and thus may not be useful to another with a different culture.

2.5.2.7 Several collective initiatives have been created to better service the banking industry in its quest for a better understanding of operational risk. Of greatest prevalence are industry-wide loss databases such as ORX,[68] the British Bankers' Association's GOLD[69] and Algo FIRST.[70] It would appear that operational risk in the insurance industry is characterised by a distinct lack of industry-specific collaborations. ORIC—launched by the Association of British Insurers (ABI)—is the only operational-risk consortium aimed solely at insurers of reasonable size. Whether elements of banking-loss databases could be used as proxies for the insurance industry depends on the degree of similarities in the operational-risk drivers. This is an area for further research.

2.5.3 Combining Operational-loss Data from Different Sources

2.5.3.1 The use of data from multiple sources provides an insurer with greater information about potential operational risks it may face, as well as increasing the modelling options available to the insurer.[71] Each modelling method has its own merits that render its results more suited to a particular use (Brandts, op. cit.).

2.5.3.2 The use of a combined approach for the modelling of operational risks by insurers has direct application to the SAM regulatory regime. A more rigorous and better informed quantification approach may place insurers in a better position to comment on the appropriateness of the Pillar I standard formula (see ¶2.2.2) and may enable them to make informed suggestions regarding ways in which it can be improved.[72] By providing a broader range of potential risks on which qualitative risk assessments can be based, and more detailed information regarding their potential impact, multiple sources of data may

68 www.orx.org
69 www.bba.org.uk
70 www.algorithmics.com/en/services/23-prodserv.cfm
71 Ernst & Young, 2011, supra
72 ibid.

also provide the insurer with greater insight into operational risk for the purposes of the Pillar II requirements and, in particular, the ORSA[73] (see ¶2.2.4).

2.5.3.3 In the use of multiple sources of data, particularly from a mixture of internal and external sources, Selvaggi (op. cit.) warns against bias that may arise in the results if merging takes place without proper calibration of these sources. In order to ensure comparability of these, robust methodologies should be employed appropriately to scale the size and number of operational losses (Dexter et al., op. cit.).

2.5.3.4 External loss data, particularly those of public loss databases, are likely to be skewed towards large losses and thus, if inappropriately pooled with internal data, they can lead to unrealistic model results and inflated capital charges (Frachot & Roncalli, op. cit.; Baud, Frachot & Roncalli, op. cit.). The contributing factor to this is the threshold over which losses are recorded. Guillen et al. (op. cit.) demonstrate the effects of this truncation in external loss databases.

2.5.3.5 Statistical methodologies for the combination of internal and external loss data have been discussed by Frachot & Roncalli (op. cit.), Baud, Frachot & Roncalli, (op. cit.) and Guillen et al. (op. cit.), among others. Schevchenko & Wüthrich (2006) provide a method of combining the opinions of experts with operational-loss data by making use of Bayesian inference. The interested reader is referred to these papers, as these statistical methodologies are not the focus of this paper.

2.6 USING AN OPERATIONAL-RISK CONSORTIUM IN THE SOUTH AFRICAN INSURANCE INDUSTRY

Research of the industry has found no local industry-wide initiatives in operation to provide operational-risk data to South African insurers. A preliminary investigation has, however, been conducted by the South African Insurance Association (SAIA)—the representative association for short term insurers—on the implementation of an operational-risk consortium that resembles ORIC.

2.6.1 ORIC

2.6.1.1 ORIC is a not-for-profit organisation launched in the UK insurance industry by the Association of British Insurers in 2004. Its primary function is to collect, standardise and report operational-loss and near-miss data in a way in which strict confidentiality of sensitive information is maintained (Selvaggi, op. cit.). There are currently 31 members of ORIC,[74] comprising life, non-life, composite and primary insurers, and reinsurers.

2.6.1.2 ORIC provides support to its members in ways that are both quantitative and qualitative (Selvaggi, op. cit.). In doing so, ORIC performs regular quantitative analyses on the data it has captured. Additionally, risk managers of member firms are encouraged to take part in a dedicated forum and are hosted at workshops on current issues facing the industry.

73 Pillar 2 Operational issues of risk management, PwC, 2012
74 www.abioric.co.uk

2.6.1.3 The database contains data of losses greater than £10 000 (R133 215),[75] categorised at three levels: level 1 and 2 are in accordance with the Basel classification of operational risks and level 3 is the subdivision of level 2 into 70 further categories (see Appendix B) (Selvaggi, op. cit.). An in-depth narrative of the circumstances surrounding the incident is also included, as well as the causes that lead to the materialisation of these risks and subsequent losses.

2.6.1.4 ORIC is heavily involved in the regulatory side of ORM. Members of ORIC sit on the FSA's Operational Risk Expert Group for insurance and participate actively in regulatory discussions (Selvaggi, op. cit.).

2.6.1.5 In an interview with an ORIC staff member documented by Acharyya (op. cit.), it was suggested that a prime use of the database by members was to inform their scenario-analysis process. As part of the identification and assessment process mentioned in ¶¶2.3.2 and 2.3.3, workshops are held by members of ORIC in which business experts make use of reported events to inform discussions and to guide estimates on the frequency and severity of operational risks that a business may face.

2.6.1.6 The respondent also suggested that the database is used as a learning tool (see ¶2.4.5.3) at both a business unit level and a company level. It provides an indication of how loss events should be reported and measured, as well as a template for the development of a company's own internal loss database.

2.6.2 Risk Event Database

2.6.2.1 SAIA has very briefly investigated the feasibility of a comparable project dubbed the 'Risk Event Database' (RED). This involved the creation of an external loss database jointly managed by the insurance associations in the country, ASISA and SAIA, based along the lines of ORIC, but tailored to suit the South African market. SAIA provided the author with a draft version of the proposal for this database.

2.6.2.2 The primary advantage put forward was the provision of good-quality, relevant and unbiased operational-loss data that will enable companies to manage their capital more effectively, as required by the SAM regulatory regime.[76] Additional advantages cited include more timely and effective identification trends in fraud and other operational risks, and the existence of a benchmark to which insurers could compare their own experience.

2.6.2.3 The stated primary advantage is consistent with technical modelling. It is interesting to contrast this philosophy with the more holistic approach that ORIC embodies (see ¶2.6.1.5). If the primary advantage of a South African operational-risk consortium is promoted as being the provision of key inputs into scenario discussions, it may come to be seen as more valuable by the industry.

2.6.2.4 Challenges were also noted. These were largely the same as the areas of concern mentioned in the above discussion about external data for internal use—for

75 Exchange rate of 13,321467R/£ correct as at 02/09/2012. Source: XE Currency

76 Proposal for an External Operational Loss Database for the South African Insurance Industry (v. 1), SAIA

example, issues relating to the comparability of data between firms. Acknowledgement was made of the fact that the database will be of real value only after sufficient time has passed to accumulate a meaningful body of data.[77]

2.6.2.5 This proposal was met with concerns from industry players with regard to the costs of initially joining the database, as well as those associated with subscription for subsequent years.[78] It was thought that only a few larger insurers in the country would be in a position to belong to such a consortium, so that the data would exhibit bias towards these companies and have little application for smaller entities. The amount of data that would be accumulated may not have significantly greater value than insurers' own internal data.

2.6.3 South African Insurers and ORIC

2.6.3.1 As an alternative it was suggested by SAIA that those South African firms that would like to make use of external data join ORIC direct.

2.6.3.2 The companies would enjoy the use of the data from UK members and the added modelling support of the organisation.

2.6.3.3 Concerns raised with this suggestion related to doubts on the comparability of data from insurers in a foreign, first-world country (the UK) with that of local insurers. Additionally, the adequacy of the £10 000 reporting threshold was questioned as it was believed that this would prove to be too high for South African conditions.

2.6.3.4 Belonging to ORIC comes at a cost. Annual subscription fees to ORIC are in the region of £17 500 (R233 126).[79] The author was not provided with specific costing estimates of the South African initiative and it is not known whether these would exceed those associated with belonging to ORIC itself.

3. RESEARCH AIMS AND METHODOLOGY

3.1 Reporting on the operational-risk practices in the South African insurance industry is relatively sparse. In addition, because of the transitory phase in which the industry finds itself, the state of such practices is volatile. This renders previous industry studies not necessarily representative of the situation at present.[80]

3.2 Owing to the aforementioned factors, a qualitative survey of the industry was performed. The questionnaire used in the survey and the responses to it are given in Appendix C.

3.3 The aims of the survey were to:

– assess the insurance industry's perceptions of operational risk and ORM and if, or how, this has changed in light of SAM;

77 ibid.
78 ibid.
79 Exchange rate of 13,321467R/£ correct as at 02/09/2012. supra
80 Noted in an interview with SAIA, 12 June 2012

– assess the industry's opinion regarding the calculation of the capital requirement for operational risk, both on the standard formula and under the internal model approach;
– investigate current and proposed industry practices in ORM and the extent to which these fall short of the impending regulatory requirements; and
– assess the willingness of firms to become involved in an external, industry-wide operational-risk database, how they feel it should be implemented and whether they believe it will have value for their company and the industry as a whole.

3.4 Before the broad-scale distribution of the survey, it was subject to review by a senior legal manager as well as an actuary practising in the insurance industry.

3.5 The authors attempted to contact all long- and short-term insurers registered with the FSB.[81] In total 120 firms were approached with operations across all lines of insurance business. Within each firm the person approached was the chief risk officer, if applicable, or a person of equivalent standing, if not. As 69% of the respondents were senior risk managers, the responses may be considered as having reasonable authority on the subject of operational risk in their respective organisations.

3.6 In total, 29 of the emailed companies participated fully, representing roughly 70% of the market as measured by total gross premium written.[82] Approximately 60% of the respondents reported to earn annual premiums in excess of R1 billion.

3.7 Although questionnaires were distributed to the entire population of registered insurers, the responses received are not believed to be an accurate representation of current operational-risk practices in the industry as a whole. Approximately 50% of respondents were from the theoretically larger insurers as measured by gross premium (see ¶3.6), which indicates that the results of the survey exhibit a bias towards the practices in these larger entities. It is possible that larger companies, particularly those publicly traded, have greater resources and face greater pressure to develop robust risk-management practices. As a result of this non-response bias, the true situation may be less positive than what is reflected below. This is in accordance with the point highlighted in ¶2.6.2.5.

4. RESULTS

4.1 INDUSTRY PERCEPTION OF ORM

4.1.1 In order to establish the significance of operational risks to insurers, insurers were asked to estimate their operational losses as a proportion of net profits. The majority of respondents reported small operational losses, only a very small percentage of respondents indicating significantly high losses. This is shown in Figures 2 and 3. Whilst there does not appear to be a significant difference in the proportionate

81 List sourced from the FSB website.

82 Source: Calculated using figures reported in the Thirteenth Annual Report by the Registrar of Long- and Short-term Insurance in 2010 respectively.

operational-risk experience between companies with differing gross premium figures (Figure 2), it is important to note that a significant portion, just over 20%, of the smallest insurers have suffered the largest operational losses as a proportion of their net profits. This is concerning as they arguably require the most stability. This may be the result of immature risk-monitoring processes. Over 40% of the larger insurers indicate operational losses between 1% and 5% of net annual profits. Although this may not seem significant as a proportion, the average net income was R3,3 billion in 2011 for the three largest life assurers and the largest general insurer by gross annual premium.[83] This therefore implies a 1% gross operational loss of R33 million and a 5% gross operational loss of R165 million. Even if one were to take the maximum tax deductibility on expenses into account at a maximum corporate taxation rate of 28%, these net operational-loss values would range between R23,8 million and R119,1 million—values certainly large enough to warrant focus. A greater proportion of reinsurers, however, report lighter operational-risk experience than primary insurers (Figure 3). Very little distinction can be drawn on the difference between general insurers and life insurers.

4.1.2 Figure 4 shows the industry's perception of the most significant operational risks, rated on a scale ranging from one to five.

4.1.3 The overall response indicated that external fraudulent activities are of the greatest concern to insurers. The industry has already taken steps to better deal with this risk type through the recent SAIA-led creation of the South African Insurance Crimes Bureau,[84] an organisation through which insurers can share information about perpetrators of external fraud and other crimes, and prosecute offenders.

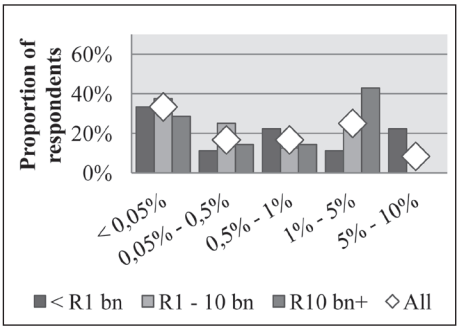

Figure 2. Operational losses as a percentage of net profit by gross annual premium

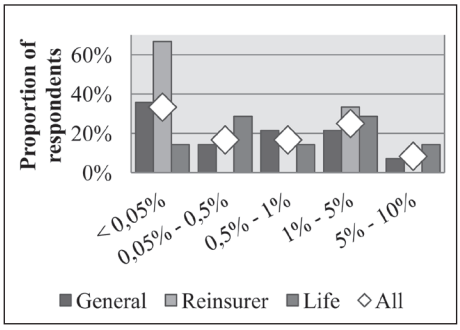

Figure 3. Operational losses as a percentage of net profit by type of insurance entity

83 Source: Calculated using figures from the audited annual financial statements of the following companies:
- Old Mutual: http://financials.oldmutual.com
- Liberty Holdings Limited: www.libertyholdings.co.za
- Sanlam: www.sanlam.co.za
- Santam: www.santam.co.za

84 The interested reader is referred to their website: www.saicb.co.za/

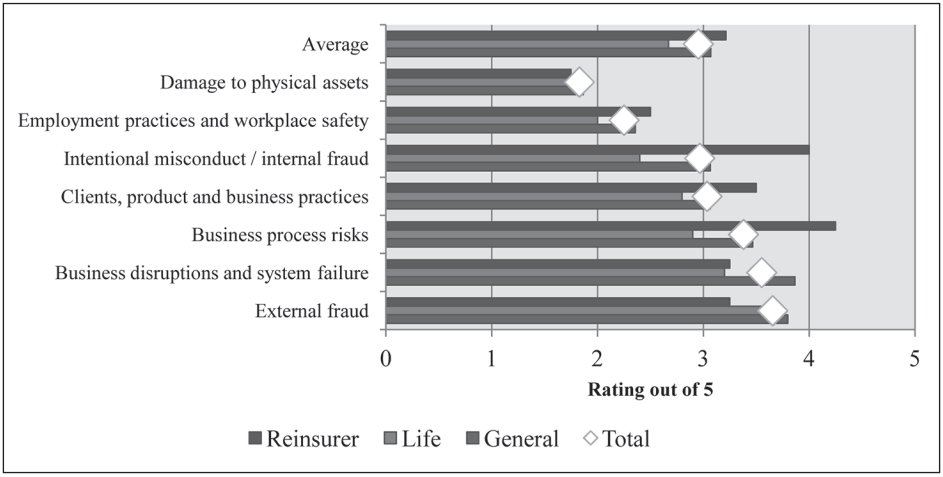

Figure 4. Rating of significant operational risks

4.1.4 On average, reinsurers deem operational risks more significant than general and life insurers. This may be because they are exposed to a greater spread of risks in terms of the number of underlying insurers they reinsure. Possibly, they are indirectly exposed to the operational risks of the cedants over which they have very little control. The most significant risks for reinsurers appear to be business-process risks and intentional misconduct or internal fraud. General insurers consider business disruptions and system failures to be their greatest risk, most likely due to the frequency with which policies are written and claims paid, resulting in greater processing requirements. Life insurers regard operational risks as the least significant of the three by a fair margin. Their greatest operational-risk concern is external fraud, which may be prevalent in their claims experience.

4.1.5 In a study performed by Mr B. Metcalf on behalf of PwC,[85] insurers opined that changes in the regulatory environment were undoubtedly the most significant taking place in the industry. The results obtained from the research conducted for this paper illustrate these concerns with regard to the operational risks; see Figure 5. More than one response was possible so, in Figure 5, figures may add up to more than 100%. The introduction and amendment of regulation imposes very real human and technological costs on insurers and these result in significant additional operational-risk exposure.

4.2 INDUSTRY OPINION ON THE SAM REQUIREMENTS FOR OPERATIONAL RISK

4.2.1 Despite their concern about the effect of regulation on operational risk, insurers appear to perceive some value in the SAM regulations regarding operational risk as shown in Figure 6. Over 62% of respondents responded 'fairly positive' or 'positive'

85 Metcalf, supra

to the question regarding their views on this matter. Only one insurer indicated a 'fairly negative' view.

4.2.2 Some insurers gave further insight into their opinions on this topic. The respondents acknowledged the potential severity of operational risks and appreciated that the regulatory requirements will serve to increase its profile. The precise management specifications were questioned. Some respondents felt that it only provides a minimal strategy and others believed that it is too rigorous and will result in unnecessary costs. One respondent felt very strongly that, whilst ORM is important, the holding of capital is not the appropriate way in which to mitigate the risk.

4.2.3 The standard formula for the calculation of the operational-risk component of SCR was not, however, thought to be overly appropriate. The primary concerns put forward in SA QIS1 were:[86]

– the formula is not risk-sensitive;
– it does not take into account the business specifications of each insurer;

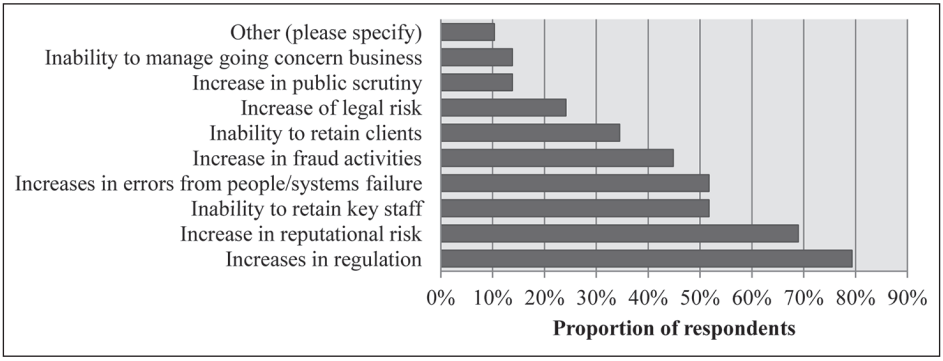

Figure 5. Key operational-risk concerns

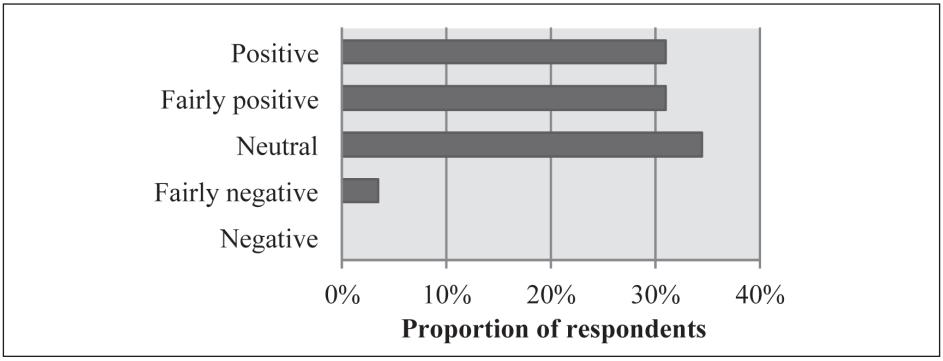

Figure 6. Views on the operational-risk requirements under SAM and the impact on SCR

86 Financial Services Board, 2011c, supra

– it penalises companies in their first year of operation;
– no diversification of operational risk capital is allowed for with other risk capital; and
– linked insurers expressed concern regarding the inclusion of asset-management fees as an expense.

4.2.4 Respondents to this paper's survey took a more measured view of this in their longer responses, saying that, although premiums, reserves and growth may not be accurate as proxies for the calculation of operational risk capital, an individually assessed figure would be difficult to determine. One respondent indicated that, although the formula appears to overestimate the capital required for operational risks given their historic measures, it was possible that some of their losses had not been accurately identified or measured.

4.2.5 In speaking on behalf of the short-term insurance industry, SAIA has voiced the opinion that Solvency II and SAM still do not reflect the advancements in the assessments of operational risk, such as those discussed in ¶2.3.3, and are therefore inadequate. Furthermore, the standard formula for the calculation of ORM, seemingly "calibrated to the average European life and non-life insurer", is inappropriate.[87]

4.2.6 This was further demonstrated by one linked life insurer in their response to the SA QIS1.[88] The capital required in respect of operational risks was calculated by their internal model to be 30% lower than that derived from the standard formula. Interestingly, two out of the four insurers submitting internal model calculations for operational risks calculated capital requirements in excess of the standard formula.

4.2.7 SAIA acknowledges several challenges with the internal model, particularly related to the sufficiency and quality of data that insurers will need to

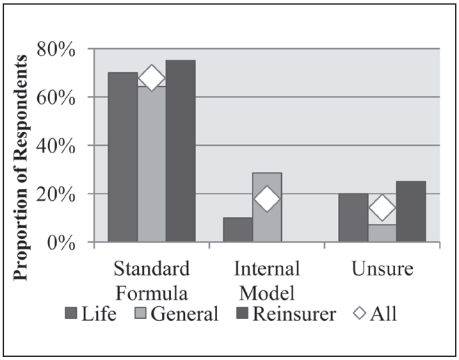

Figure 7. Intended formula to be used for the calculation of regulatory capital by type of insurer

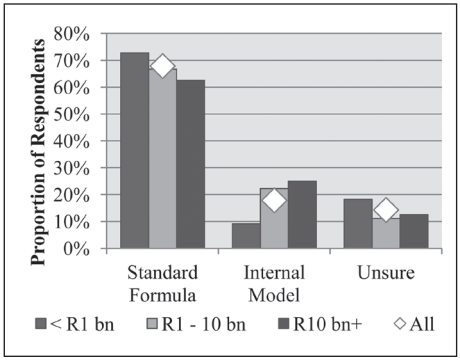

Figure 8. Intended formula to be used for the calculation of regulatory capital by gross annual premium

87 Insurance Gateway. http://insurancegateway.co.za
88 Financial Services Board, 2011c, supra

possess. This is evident in the responses of insurers when questioned on which formula they plan to make use of, as shown by Figures 7, 8 and 9.

4.2.8 Overall, 68% of respondents indicated a definite intention to make use of the standard formula, a further 14% being unsure. There seems to be a positive correlation between the intention of a company to develop an internal model and its market share. As discussed in ¶3.7, larger insurers were more likely to respond to the questionnaire. Hence, the proportion of insurers that will actually use internal models may be even less than what is observed here. Reinsurers, however, do not adhere to the relationship between gross premium written and formula usage, none of the respondents indicating a clear intention to use an internal model. General insurers are more likely than life insurers to use an internal model, which may be because the current general-insurance regulatory-capital requirements are not particularly risk-based, whereas CAR is a risk-based approach for life assurers. Therefore SAM represents a greater evolutionary jump for general insurers. Additionally, general insurers are more likely to specialise in specific product lines and are more likely to have unique risk profiles. Life assurers, in contrast, should have very similar risk drivers. This implies that a single standard approach may be less appropriate for general insurers.

4.2.9 No conclusions can be drawn on the industry's perceptions of the degree to which ORM has changed, or will change, in light of the SAM regulations. The survey elicited an even spread of responses from 'not at all' to 'to a high degree'.

4.2.10 At the time of issue of the questionnaire, the SAM implementation date had been amended to 1 January 2015.[89] Despite the delay of a year in the implementation of SAM, only 60% of respondents indicated that their organisations would be compliant with the SCR in respect of operational risks. The implementation date has since been delayed by another year to 1 January 2016.[90]

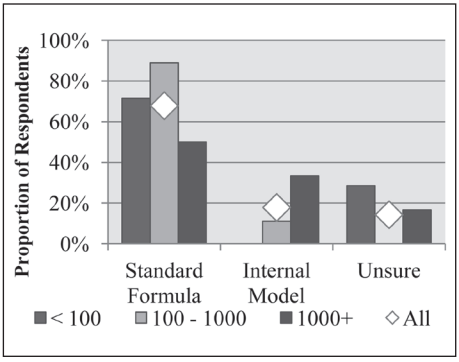

Figure 9. Intended formula to be used for the calculation of regulatory capital by number of employees

4.2.11 It is not only Pillar 1 that will give rise to challenges for insurers. The justification of the appropriateness of the standard formula for operational risk under the ORSA is expected to cause difficulties.[91]

4.3 ORM PRACTICES

4.3.1 Risk Policy

4.3.1.1 South African insurers appear to be aware of the importance of operational risk and all respondents indicated that a strategy for its management

89 Financial Services Board, 2012c, supra
90 Solvency Assessment and Management (SAM) 2013 Update. Financial Services Board, 2012f
91 Insurance Gateway. http://insurancegateway.co.za, retrieved 22/05/2012

is at least in the developmental phase. As shown in Figure 10, 75% of insurers report to follow the best-practice strategies proposed in the literature. The responsibility of risk management lies chiefly with the board of directors; however, the majority of respondents report that dedicated risk managers and committees have also been appointed within the organisation.

4.3.1.2 A significant proportion of insurers define risk appetite to some degree, as shown in Figure 11. However, as discussed in ¶2.3.1.5, those who only do so only at an aggregated level should move towards doing so at an individual risk level.

4.3.2 Risk Identification

In providing a general opinion on operational risks, one respondent raised concerns regarding the difficulty of ensuring that all relevant risks facing the insurer are identified. Further research should be conducted on the processes followed regarding the preliminary identification and categorisation of operational risks amongst South African insurers. Much of the focus of this paper was directed to the next phase of the framework.

4.3.3 Risk Assessment and Measurement

4.3.3.1 A wide variety of approaches are used by insurers for quantifying their exposure to operational risks. The most popular among respondents was scenario analysis, alternatively known as stress testing. Stochastic modelling proves to be the least popular, which is indicative that the vast majority of the academic literature around ORM has yet to find significance in the South African insurance context. An area of concern uncovered by the responses was the significant variation in the extent to which operational-loss data were recorded. As shown in Figure 12, of the respondents, 31% report data recording 'to a lesser degree' and 41% report recording practices 'to a high degree' or 'totally'.

Figure 10. Extent to which a strategy for ORM has been adopted

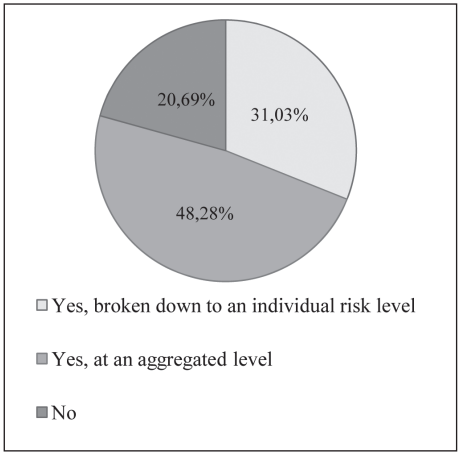

Figure 11. Extent to which a risk appetite/ tolerance level for operational risk has been defined

Universal recognition of the value of the knowledge created by historic operational-loss data has therefore yet to be attained.

4.3.3.2 In the event that an operational-risk consortium database were to be introduced into the industry, it would be important to ensure that contributors record data at comparable levels. This observation also serves to limit the extent to which the database could retrospectively capture loss events. Near-miss occurrences are used by 57% of respondents as part of their tools for risk identification and assessment. Despite expressing concern regarding the failure of the standard formula to allow for correlation and diversification effects of operational risks amongst each other and with other risks,[92] just under 50% of respondents—which represents a high proportion—admitted that they had not been recording interrelations and correlations between identified risks.

4.3.4 Risk Management

4.3.4.1 When asked to describe the distribution of resources between the management and measurement of operational-risk activities, respondents indicated that the two functions enjoyed a relatively even split. This is indicative that the recommended multifaceted approach is being adopted by the players in the industry. When considering the quantitative approaches discussed in section 4.3.3, however, it would appear that the industry needs to interrogate itself on whether it is making optimal use of the universe of quantitative modelling methods available. Scenario analysis is limited by the human difficulty of considering the valence of an outcome, i.e. the behavioural-finance perspective of estimating probabilities. Stochastic modelling provides a technical way of mitigating some of this bias. The industry may be under the misapprehension that a balanced management approach is sufficient.

4.3.4.2 The extent to which the measurement of operational risk drives the management of it was not established conclusively. South African insurers perceive sound ORM practices as highly important, but, as shown by Figure 13, they do not all report fully comprehensive and effective practices within their organisations. The majority take

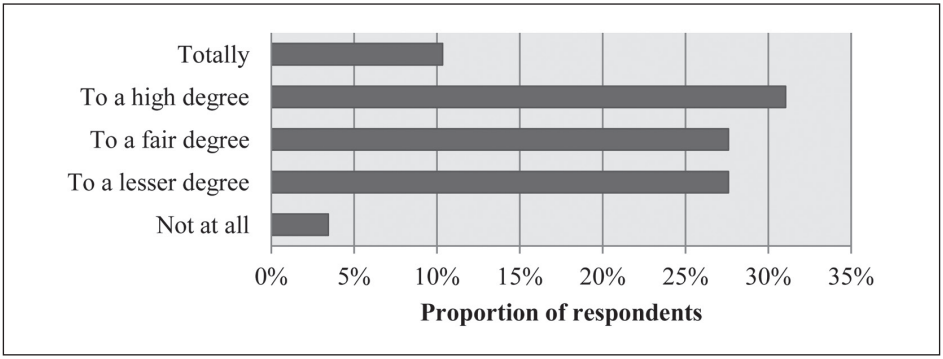

Figure 12. Extent to which operational-risk data are recorded

92 Financial Services Board, 2011b, supra

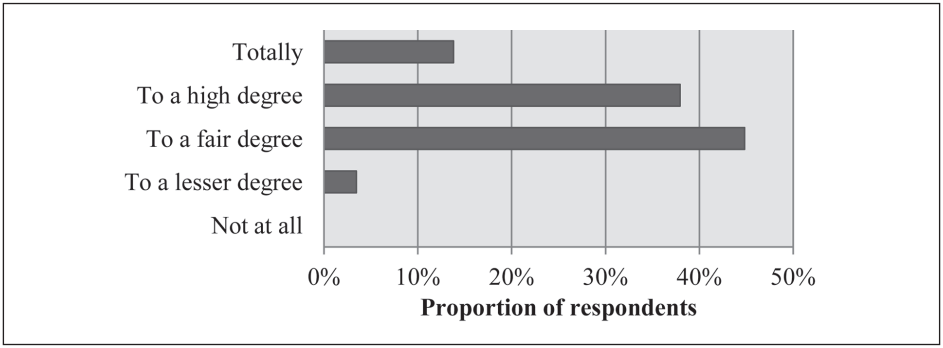

Figure 13. Self-assessment on the effectiveness of ORM

a measured view by indicating practices that are effective 'to a fair degree'. What is meant by 'a fair degree' is open to interpretation and thus it is likely that significant variation amongst respondents in this group will be found.

4.3.4.3 It would appear that, in accordance with the suggestion of Lam (op. cit.), the ORM function is embedded in the individual lines of business. This means that individual business units report on their own operational risk, most probably on an aggregated basis within the unit, as noted in Figure 11. To a lesser extent, a centralised management function is reported. This would be where one risk-management analysis is taken out in respect of operational risks in the business as a whole. Ideally, both an embedded and a centralised approach should be used by insurers (Lam, op. cit.) but this was reported to be the case by only nine of the respondents. The use and clear documentation of controls for the identified risks is prevalent in over 90% of responding firms. In addition, several insurers indicated that risks were recorded before and after control measures.

4.3.5 Risk Financing

4.3.5.1 As discussed in ¶4.2.7, the majority of insurers will be making use of the SAM standard formula to calculate the capital required to cover operational risks. Capital management forms part of the risk-management strategy of the majority of insurers. Metcalf[93] concludes that insurers see significant benefit from the calculation of economic capital.

4.3.5.2 The costs of any ORM practices would also be included in the risk-financing considerations of insurers (see ¶2.3.5.1). These costs not only have the potential to dictate the choice of level of sophistication of risk-management controls (¶2.3.5.4), but also to influence significantly the choice of model for the calculation of regulatory capital (see ¶2.3.5.4). It was felt by one respondent that despite the additional costs of implementing a formal risk-management policy, the industry would benefit from it overall.

93 Metcalf, supra

4.3.6 Risk Monitoring

For the purposes of monitoring their operational risks, insurers report on the use of KRIs as well as action plans. Risk meetings happen quarterly, rather than monthly, as was suggested in Lam's (op. cit.) basic operational-risk practice. The significance of quarterly meetings as opposed to monthly meetings was not made clear in the literature. However, one can infer that the more frequently operational risks are discussed, the more aware and in control of its risks the organisation will be.

4.4 USE OF LOSS DATA IN THE SOUTH AFRICAN INSURANCE INDUSTRY

Respondents displayed mixed reactions towards the use of loss data as a means of evaluating their operational risks. Of the respondents, 40% saw this as being 'highly appropriate', but almost 28% felt it to be at least 'somewhat inappropriate'. In the longer responses, reference was made to the fact that, because operational-risk exposures are constantly evolving, the relevance of historical loss data diminishes as they become older.

4.5 A SOUTH AFRICAN OPERATIONAL-RISK CONSORTIUM

4.5.1 Before the specific questions regarding a South African operational-risk consortium were posed, the awareness of the concept was assessed. Only 59% of respondents were aware of the existence of industry-wide operational-risk databases. This should be kept in mind as one continues through the responses that follow, as insurers may not be fully aware of the benefits, or the cost implications, of such an initiative. It is difficult to assess the direction in which responses may display bias.

4.5.2 A mixed response was obtained regarding the usefulness of a consortium-based database, a quarter of respondents being unwilling to make a definitive call and responding 'unsure'. Arguments both for and against the idea of a consortium-based database were presented.

4.5.3 Those in favour cited benefits to be derived from the improvements in exposure resulting from a focus on better data collection, enhancement of systematised solutions and the automation of processes and internal controls. Through the sharing of ideas and experiences, it was reasoned that emerging operational risks, as well as any risk trends, could be more easily identified. Greater volumes of data were welcomed for their potential to assist with a more accurate capital calculation. One respondent went as far as to say that an initiative such as this is imperative for the insurance industry.

4.5.4 Opposing arguments centred around the uniqueness of each insurer in the industry in areas such as culture, structure, product features, and operational requirements. Respondents felt that operational risks were largely dependent on the aforementioned factors. The relevance of data between companies was therefore questioned, particularly in respect of the larger operational risks faced by insurers.

4.5.5 Despite their concerns, a significantly large proportion of respondents indicated a willingness to join an operational-risk consortium. As shown in Figure 14, of the respondents, 86% expressed interest in joining at least at a subscriber level and, more importantly, 75% were prepared to contribute data in addition to their subscription. Whilst these results are encouraging, one should note that insurers were not presented with

the potential costs of belonging to the consortium. As previously discussed in ¶¶2.6.2.5 and 2.6.3.4, and as pointed out in a response, although the concept of a consortium-based database is viewed favourably by insurers, the costs involved are deemed to be prohibitive by many.

4.5.6 Roughly 52% of respondents believed that an initiative like this would be feasible. One respondent discussed at length the time-frame over which feasibility could be assessed, believing that it is only over a longer term that an appreciation for the initiative would grow. This uncovers an important point to consider: the consequences to the industry of failing to implement proper operational-risk initiatives now may only be realised some time in the future, at which point much of the valuable knowledge communicated through historical events will have been lost. The costs, both in respect of the value loss as well as the monetary costs of dealing with these consequences, may far exceed those that would be incurred in implementing the initiatives now. Further research needs to be carried out on this issue, which, in itself, can be classified as an operational risk to the industry as a whole.

4.5.7 Figure 15 shows that there was little consensus as to who the optimal administrator of the database would be. Counter-intuitively, both life insurers and general insurers indicated that the short-term industry body, SAIA, should be the administrator. The reinsurers favoured the FSB. A single respondent felt that the consortium should be operated by an independent party with the ability to fulfil the necessary confidentiality requirements. Respondents indicated, however, that the FSB should play a key role in leading the process. Although it was not explicitly stated, one may assume that this means that the FSB would require the use of industry-wide data as part of internal capital modelling in the same way that Basel II dictates its use in the 'Advanced Measurement Approach' for banks. This would then make belonging to an operational-risk consortium a regulatory requirement.

4.5.8 The FSB should, however, be pre-emptive with regard to industry data. The creation of a South African operational-risk consortium may take some time.

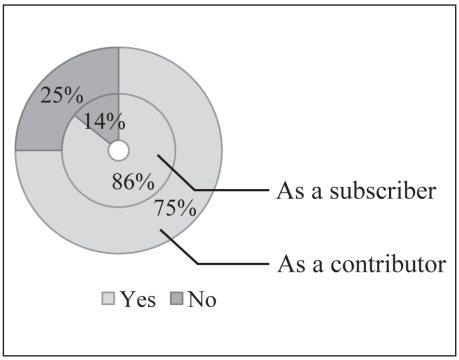

Figure 14. Willingness to join an operational-risk consortium

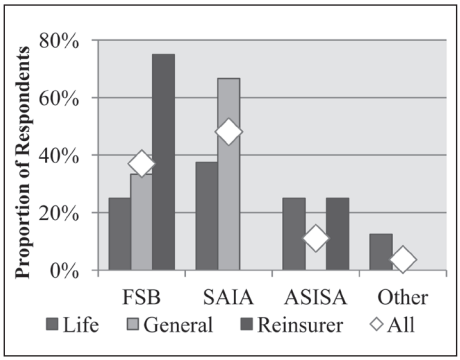

Figure 15. Choice of body responsible for managing an operational-risk consortium

In the interim, insurers should aim to record losses and near misses in a standard way in preparation for a consortium, so that the industry does not lose data years (see ¶4.5.6).

5. SUMMARY AND CONCLUSION

5.1 By drawing on a wide variety of documentary resources and literature both from the industry and from academia, as well as on existing and proposed regulation, this paper has provided a basis through which operational risk can be identified and assessed in respect of the South African insurance industry.

5.2 Operational risks are of great significant to South African insurers. The industry displays views on operational risk that indicate a wide range of maturity between entities. Insurers, as a whole, appear to realise the importance of operational risk, beyond the need to simply hold capital to cover it, and have begun to develop frameworks for its management. Areas in which the need for improvement can be seen include the collection and utilisation of internal historical loss data. Several advantages of the use of such data are discussed in this paper, extending beyond the bounds of pure statistical modelling.

5.3 Regulation stands out as the main driver for developments in the area of operational risk. South African insurers appear to be less able, or at least less willing, to embrace a risked-based regulatory regime to its fullest extent, preferring a standardised approach for the calculation of their exposure to risk.

5.4 Industry commentary suggests that the allowance for operational risk in the standard formula is not truly risk-based. In this case, the capital calculated will not reflect the true cost of operational risk within the organisation. It would therefore appear that further consideration is needed regarding the standard formula for the calculation of operational-risk capital. It is, however, recognised that the aim of acquiring third-country equivalence with Solvency II may limit the freedom that the local regulator has to make changes to the standard formula.

5.5 At this stage, a firm conclusion cannot be drawn as to the feasibility of a South African operational-risk database. Despite initial negative reactions received by SAIA, further investigations should be carried out. Other industry-wide, data-oriented initiatives have been successfully implemented by SAIA[94] and therefore, at such an early stage, it is difficult to conclude total unfeasibility for another one of a similar nature. The responses depicted by Figure 14 indicate that insurers do see value in the idea of a consortium and thus may be much more willing to join than SAIA has predicted. For those that were opposed to the idea, the direct costs of subscribing to an operational-risk database were cited as the primary disadvantage. The potential indirect costs of not initiating a collective operation risk effort were not as widely appreciated. The key to reducing the

94 STRIDE and the Insurance Crimes Bureau. www.saia.co.za

direct costs is to obtain an adequate number of subscribers, so that the costs can be split into manageable amounts per subscribing member. The fact that 41% of respondents were not aware of the concept of an operational-risk consortium indicates that further industry involvement and education is required. Feasibility would then need to be reconsidered.

5.6 There are a number of areas for further research. These include:

- ways of improving the standard formula for operational risk given the concerns regarding its applicability;
- objectives of collecting data, i.e. use in understanding risk management and not just for informing risk modelling;
- a further investigation into the practical aspects of an operational-risk consortium for the South African industry, particularly a cost–benefit analysis, including the indirect costs associated with delaying the introduction of the consortium;
- whether banking operational-risk consortia can be used as proxies for the insurance industry;
- modelling the data captured in an operational-risk database of the South African insurance industry, should one ever be implemented, primarily to indicate weaknesses in ORM by individual organisations and by the industry as a whole;
- investigating the processes used by the South African insurance industry for the preliminary identification and categorisation of operational risks; and
- investigating how disparate the operational risks are within the insurance industry, and the different methods of approaching these risks within the industry, e.g. by type of insurer, primary product line etc.

5.7 The actuarial profession will also need to ensure that due focus is given to operational risk when SAM is included in professional guidance.

5.8 A comment from one of the respondents to the survey deserves the last word:

> Business is practical and results driven theory does not ensure results. The focus must be on the results and not the theory. I expect that there will be insurers that will fail even though they have met the requirements of the theory.

ACKNOWLEDGMENTS

The authors wish to thank all the insurers who participated in the questionnaire. Their contribution has provided invaluable insight into the industry's perspective on operational risk. Without their co-operation this paper would not have been possible. The names of the participating insurers are withheld as per the terms of their participation in the survey.

The authors acknowledge the help of contributors from the South African Insurance Association, who provided their time and insights, including valuable information regarding potential developments of an operational-risk database in South Africa.

REFERENCES

Acharyya, M (2012). The scope of developing optimization models for insurer's operational risk from risk-return trade-off perspective. Society of Actuaries. www.soa.org/Files/Research/Projects/The-Scope-of-Developing-Optimization-Models-for-Insurer-s-Operational-Risk-from-Risk-Return-Trade-Off-Perspective.pdf

Alexander, C (ed.) (2003). *Operational Risk: Regulation, Analysis and Management.* Prentice Hall–Financial Times, London

Baud, N, Frachot, A & Roncalli, T (unpublished). Internal data, external data and consortium data for operational risk measurement: How to pool data properly? Crédit Lyonnais working paper, Groupe de Recherche Opérationnelle

Brandts, S (unpublished). Operational Risk and Insurance: Quantitative and qualitative aspects. Unpublished dissertation, Graduate Program Finance & Monetary Economics, Goethe University, Frankfurt, 2004

Collis, D (1996). Organizational Capability as a Source of Profit. *In* Moingeon & Edmondson. 1996: 139–63

Cope, E, Mignola, G, Antonini, G & Ugoccioni, R (2009). Challenges and pitfalls in measuring operational risk from loss data. *The Journal of Operational Risk* **4**(4), 3–27

Cyert, WM & March JG (1963). *A Behavioral Theory of the Firm*. Prentice-Hall, Englewood Cliffs, New Jersey

Dexter, N, Ford, C, Jakhira, P, Kelliher, P, McCall, D, Mills, C, Probyn, A, Raddal, P & Ryan, J (2007). Quantifying operational risk in life insurance companies. *British Actuarial Journal* **13**(2), 257–337

Embrechts, P, Furrer, H & Kaufmann, R (2003). Quantifying regulatory capital for operational risk. *Derivatives Use, Trading & Regulation* **9**(3), 217–33

Frachot, A & Roncalli, T (unpublished). Mixing internal and external data for managing operational risk. Crédit Lyonnais working paper, Groupe de Recherche Opérationnelle

Guégan, D, Hassani, BK & Naud, C (2011). An efficient threshold choice for the computation of operational risk capital. *Journal of Operational Risk* **6**(4), 9–19

Guillen, M, Gustafsson J, Perch Nielsen, J & Pritchard, P (2007). Using external data in operational risk. *The Geneva Papers* **32**, 178–89

Gustafsson, J (2010). A mixing model incorporating three sources of data for operational risk quantification. *Insurance Markets and Companies: Analyses and Actuarial Computations* **1**(1), 54–68

Haubenstock, M (2003). The operational risk management framework. *In* Alexander. 2003: 241–61

IOR (unpublished). Operational Risk Sound Practice Guidance – Risk Appetite. Institute of Operational Risk. 2009. www.hayderisk.com/IORRiskAppetiteSPGVersion1.pdf, 06/10/2012

Lam, J (2003). *Enterprise Risk Management.* John Wiley & Sons, Inc., Hoboken, New Jersey

Levinthal, DA & March, JG (1993). The myopia of learning. *Strategic Management Journal* **14**, 95–112

Levitt, B & March JG (1988). Organizational learning. *Annual Review of Sociology* **14**, 319–40

Moingeon, B & Edmondson, A (eds.) (1996). *Organizational Learning and Competitive Advantage.* Sage, London

Peters, GW, Shevchenko, PV & Wüthrich, MV (2009). Dynamic operational risk: modelling dependence and combining different sources of information. *The Journal of Operational Risk* **4**(2), 69–104

Shevchenko, PV & Wüthrich, MV. (2006). The structural modeling of operational risk via Bayesian inference: combining loss data with expert opinions. *The Journal of Operational Risk* **1**(4), 9–30

Selvaggi, M (2009). Analysing operational losses in insurance. Report from ABI Research Department. ISBN 978-1-903193-46-X

Slawski, J & van den Heever, R (unpublished). Operational risk management. Convention, Actuarial Society of South Africa, 2011

Taleb, NN, Goldstein, DG & Spitznagel, MW (2009). The six mistakes executives make in risk management. *Harvard Business Review* **87**(10), 78–81

Tripp, M, Bradley HL, Devitt, R, Orros, GC, Overton, GL, Pryor, LM & Shaw, RA. (2004). Quantifying operational risk in general insurance companies. *British Actuarial Journal* **10**, 919–1012

Wei, R (unpublished). Operational risks in the insurance industry. Department of Insurance and Risk Management, The Wharton School, University of Pennsylvania, Philadelphia, 2003

APPENDIX A

THE STANDARD FORMULA[95]

The standard formula for the calculation of the capital requirement relating to operational risks, SCR_{op} is given in Equation A.1:

$$SCR_{op} = \min\left\{0,3 \times BSCR; Op_{lnul}\right\} + 0,25 \times Exp_{ul} \quad \text{(A.1)}$$

where:

$BSCR$ is the basic solvency capital requirement;
Op_{lnul} is the operational risk charge in respect of linked and non-linked operations; and
Exp_{ul} represents expenses in respect of unit-linked business.

Op_{lnul} is calculated according to Equation A.2.

$$Op_{lnul} = \max\left\{Op_{premiums}; Op_{provisions}\right\} \quad \text{(A.2)}$$

where:

$Op_{premiums}$ represents operational risk charge in respect of premiums; and
$Op_{provisions}$ represents operational risk charge in respect of provisions.

The formulae for $Op_{premiums}$ and $Op_{provisions}$ are given in Equations A.3 and A.4 respectively.

$$Op_{premiums} = 0,055 \times \left(Earn_{L} + Earn_{SLTH} - Earn_{LUL}\right) + 0,038 \times \left(Earn_{NL} + Earn_{NSLTH}\right) \quad \text{(A.3)}$$
$$+ \max\left\{0; 0,055 \times \left(\Delta Earn_{L} - \Delta Earn_{LUL}\right)\right\} + \max\left\{0; 0,038 \times \Delta Earn_{NL}\right\}$$

where:

$Earn_{L}$ represents total earned premium gross of any reinsurance in respect of life business, including unit-linked business;
$Earn_{SLTH}$ represents total earned premiums gross of any reinsurance in respect of similar-to-life-techniques (SLT) health business;
$Earn_{LUL}$ represents total earned premiums gross of any reinsurance in respect of unit-linked life business;
$Earn_{NL}$ represents total earned premiums gross of any reinsurance in respect of non-life business;
$Earn_{NSLTH}$ represents total earned premiums gross of any reinsurance in respect of non-SLT health business;
$\Delta Earn_{L}$ represents the change in earned life premiums gross of any reinsurance from year $t-1$ to year t where the change is an increase in excess of 10%;

95 Financial Services Board, 2011a, supra

$\Delta Earn_{LUL}$ is similarly defined for unit-linked life premiums; and
$\Delta Earn_{NL}$ is similarly defined for earned non-life premiums.

$$Op_{provisions} = 0,006 \times \left(TP_L + TP_{SLTH} - TP_{LUL}\right) + 0,036 \times \left(TP_{NL} + TP_{NSLTH}\right) + \max\left\{0; 0,006 \times \left(\Delta TP_L - \Delta TP_{LUL}\right)\right\} + \max\left\{\left(0; 0,036 \times \Delta TP_{NL}\right)\right\} \quad \text{(A.4)}$$

where:

TP_L represents technical provisions in respect of life business, including unit-linked business;
TP_{SLTH} represents technical provisions in respect of SLT health business;
TP_{LUL} represents technical provisions in respect of unit-linked life business;
TP_{NL} represents technical provisions in respect of non-life business;
TP_{NSLTH} represents technical provisions in respect of non-SLT health business;
ΔTP_L represents the change in the technical provisions for life business from year $t-1$ to year t where the change is an increase in excess of 10%;
ΔTP_{LUL} is similarly defined for technical provisions for unit-linked life business; and
ΔTP_{NL} is similarly defined for technical provisions for non-life business.

APPENDIX B

BASEL CATEGORIES OF OPERATIONAL-LOSS EVENTS

The Basel Committee suggests a categorisation of operational-loss events into seven level 1 and twenty level 2 events, as shown in Table B.1. Level 2 is subdivided into 70 further categories as shown in Table B.2.

Table B.1. Basel categories of operational-loss events

Event Type Category (Basel Level 1)	Sub-Category (Basel Level 2)
Internal fraud	Unauthorised use of computer systems
	Theft and fraud
External fraud	Theft and fraud
	Systems security
Employment practices and workplace safety	Employee relations
	Safe environment
	Diversity and discrimination
Clients, products and business practices	Suitability, disclosure and fiduciary
	Improper business or market practices
	Product flaws
	Selection, sponsorship and exposure
	Advisory activities
Damage to physical assets	Disaster and other events
Business disruption and system failures	Systems
Execution , delivery and process management	Transaction capture, execution and maintenance
	Monitoring and reporting
	Customer intake and documentation
	Customer or client account management
	Trade counterparties
	Vendors and suppliers

Table B.2. Subdivision of level 2

Event Category		
Level 1	Level 2	Level 3
Internal fraud	Unauthorised use of computer systems	Unauthorised use of computer system to defraud firm or customer
		Unauthorised transactions
		Under-reported transactions
		Over-reported transactions
		Falsifying personal details
	Theft and fraud	Theft of assets
		Destruction of assets
		Forgery impersonation
		Disclosure of confidential information
		Accounting irregularities
		Misappropriation of assets
External fraud	External fraud	Theft of assets
		Forgery impersonation
		Fraudulent billing by suppliers
		Fraudulent claims
	Systems security	Hacking
		Theft of information
		Viruses
Employment practices and workplace safety	Employee relations	Harassment
		Terminations, including tribunals
		Industrial activities
		Management
		Loss of key personnel
	Safe environment	Health and safety
		Public liability
		Employee liability
	Diversity and discrimination	Equal opportunities
		Human rights

Clients, products and business practices	Suitability, disclosure and fiduciary	Regulatory impact Data protection act Regulatory compliance of appointed representatives Customer complaints Treating customers fairly
	Improper business or market practices	Money laundering Other improper market practices Insider dealing Tax evasion Anti-trust
	Product flaws	Product defects (unauthorised, etc) Product literature defects Product design Unintentional guarantees
	Selection, sponsorship and exposure	Client fact-finding Client exposure
	Advisory activities	Mis-selling due to mortgage endowment Mis-selling (other)
Damage to physical assets	Disaster and other events	Natural disaster losses Losses from external sources (terrorism, vandalism) Physical assets failure (not systems)
Business disruption and system failures	Systems	Hardware Software IT network Telecommunication Utility outage/disruption External interference (excluding fraudulent activity)
Execution, delivery and process management	Transaction capture, execution and maintenance	Customer service failure Data entry error Transaction system error Management information error Accounting error Incorrect application of charges Incorrect unit pricing/allocation Management failure Inadequate process documentation Training and competence
	Monitoring and reporting	Failed mandatory reporting Inaccurate external reporting
	Customer intake and documentation	Incomplete/incorrect application documents Contract document incorrect Inappropriate underwriting Inappropriate reinsurance Missing documentation

APPENDIX C

THE SURVEY

The survey was conducted via a reputable online surveying tool. Access to the questionnaire could be gained only via a unique link provided to potential respondents by email. This was done in an attempt to remove potential data-capturing errors and to allow for compatibility with a broad range of computing systems. In addition to this, a spreadsheet version of the questionnaire was attached to the email as an alternative in case respondents were unable or unwilling to make use of the online tool. The questionnaire, with the responses to each question, was as follows.

QUESTIONNAIRE AND RESPONSES

This questionnaire forms part of an honours research project in the School of Statistics and Actuarial Science at the University of the Witwatersrand.

The aim of the project is to investigate the concept of operational risk and operational risk management in the context of the South African insurance industry; the industry's perceptions, current and proposed practices and the impact of the impending regulatory requirements of SAM.

It also aims to investigate the feasibility, benefits and practical aspects of establishing an external consortium-based operational-risk database for the South African insurance industry.

The benefits of this research include an increased understanding of the impact of operational risk and its management in the local market. It will provide insight into the current status of ORM and what improvements will be required going forward.

Your answers are important; missing information will adversely affect the reliability of the results.

The information will be used for research purposes only. The research report may be made publicly available by the School, and the results may be published. Your anonymity will, however, be maintained.

SECTION 1: COMPANY INFORMATION

0a. What is your current role in the organisation?

68,97%	Chief risk officer (CRO)/senior risk manager
13,79%	Chief financial officer/senior financial manager
6,90%	Chief actuary/senior actuary
6,90%	Junior actuary/financial manager
0,00%	Other

0b. Approximately how many full time employees does your organisation currently employ?

17,24%	Less than 50
6,90%	50–100
20,69%	100–500

13,79% 500–1000
41,38% 1000+

0c. What is the approximate annual gross revenue of your organisation?

10,34% Less than R500 million
0,00% R250–R500 million
27,59% R500 million–R1 billion
34,48% R1–10 billion
24,14% R10–R50 billion
3,45% R50 billion+

0d. In which regional centres does your organisation have an office?

	Yes	No
Johannesburg	86,21%	13,79%
Pretoria	37,93%	62,07%
Cape Town	58,62%	41,38%
Bloemfontein	27,59%	72,41%
Port Elizabeth	27,59%	72,41%
Nelspruit	20,69%	79,31%
Durban	41,38%	58,62%
Pietermaritzburg	10,34%	89,66%
Other (please specify)	10,34%	89,66%

SECTION 2: OPERATIONAL RISK & MANAGEMENT PRACTICES

1. What was the approximate magnitude of operational losses in your organisation during the previous financial year? (% of net profit)

33,33% Less than 0,05%
16,67% 0,05%– 0,5%
16,67% 0,5%–1%
25,00% 1%–5%
4,17% 5%–10%
4,17% 10%+

2. Who is responsible for operational risk management?

41,38% Board of directors
0,00% Compliance officer
24,14% CRO
31,03% Role is shared between different persons
0,00% Appointment within the next 12 months
3,45% Other

3a. Do you have a dedicated risk manager?

86,21%	Yes
13,79%	No

3b. Do you have a risk committee?

89,66%	Yes
10,34%	No

3c. How often does the risk committee meet?

0,00%	Ad hoc
10,34%	Monthly
68,97%	Quarterly
0,00%	Annually
17,24%	Other (please specify)
3,45%	Not applicable

4. How comprehensively does your organisation manage operational risks?

0,00%	Not at all
3,45%	To a lesser degree
44,83%	To a fair degree
37,93%	To a high degree
13,79%	Totally
0,00%	Unsure

5. How important does your organisation think sound operational risk management practices are?

0,00%	Not at all
0,00%	Slightly important
13,79%	Fairly important
55,17%	Highly important
31,03%	Absolutely important

6. Does your organisation currently use the following to evaluate its operational risk?

	Yes	No
Scenario analysis/stress testing	44,83%	55,17%
Factor based on volume measures (e.g. premium, revenue, economic capital)	13,79%	86,21%
Stochastic modelling	3,45%	96,55%
Firm-developed model	13,79%	86,21%
Modified SAM standard formula	3,45%	96,55%
SAM standard formula	41,38%	58,62%
Other	13,79%	86,21%
Don't know	3,45%	96,55%

7. *Does your organisation have a strategy for operational risk management?*

75,00%	Yes, as an integrated part of overall organisational risk management
7,14%	Yes, informal
17,86%	No, will be implemented within the next 12 months
0,00%	No, other priorities are more pressing

8. *Has your organisation defined its risk appetite/risk tolerances for operational risk?*

31,03%	Yes, broken down to an individual risk level
48,28%	Yes, at an aggregated level
20,69%	No

9. *How is the operational-risk function organised?*

	Yes	No
Embedded in the lines of business	72,41%	27,59%
Centralised	55,17%	44,83%

10. *Please rate the each of the following areas of operational risk in terms of significant risk for your organisation (1 – not at all significant, 5 – very significant)*

3,66	External fraud
3,55	Business disruptions and system failure
3,38	Business process risks
3,03	Clients, product and business practices
2,97	Intentional misconduct/internal fraud
2,25	Employment practices and workplace safety
1,83	Damage to physical assets

11. *What information is collected as part of the operational risk assessment? (Indicate all that apply)*

	Yes	No
Risk description	100,00%	0%
Risk owner	92,86%	7,14%
Control description	92,86%	7,14%
Impact (rands)	92,86%	7,14%
Action plans if risk limit is breached	0,00%	100%
Frequency (#)	78,57%	21,43%
Risk ranking	71,43%	28,57%
Indication of reputational effects	57,14%	42,86%
KRIs	42,86%	57,14%
Risk appetite limit	35,71%	64,29%
Other (please specify)	35,71%	64,29%
Linkages to other risks	25,00%	75,00%

12. *Does your operational risk management system capture the interrelations between the various risks identified?*

37,93%	Yes, in a descriptive way
13,79%	Yes, in a quantitative way (e.g. correlations, copulas)
48,28%	No

13. *What does your organisation regard as being key operational-risk concerns going forward? (Indicate all that apply)*

	Yes	No
Increases in regulation	79,31%	20,69%
Increase in reputational risk	68,97%	31,03%
Inability to retain key staff	51,72%	48,28%
Increases in errors from people/failure of systems	51,72%	48,28%
Increase in fraud activities	44,83%	55,17%
Inability to retain clients	34,48%	65,52%
Increase of legal risk	24,14%	75,86%
Increase in public scrutiny	13,79%	86,21%
Inability to manage going concern business	13,79%	86,21%
Other (please specify)	10,34%	89,66%

14. *What is the mix of management and measurement activities for your operational-risk function? (Allocate the appropriate proportion of 100% to each)*

41,72%	Management
58,28%	Measurement

15. *How effective are your organisation's operational risk management practices?*

0,00%	Not at all
3,45%	Slightly effective
51,72%	Fairly effective
37,93%	Highly effective
6,90%	Totally effective
0,00%	Unsure

16. *How appropriate does your organisation believe that data-based modelling of operational risk management is?*

3,45%	Not at all
24,14%	Slightly appropriate
31,03%	Fairly appropriate
27,59%	Highly appropriate
6,90%	Completely appropriate
6,90%	Unsure

17. *To what extent does your organisation record operational-risk data?*

3,45%	Not at all
27,59%	To a lesser degree
27,59%	To a fair degree
31,03%	To a high degree
10,34%	Totally
0,00%	Unsure

18. *Does your organisation take account of near misses in addition to actual loss events?*

57,14%	Yes
42,86%	No

SECTION 3: SAM REGULATIONS AROUND OPERATIONAL RISK

19. *What is your organisation's view towards the requirements of SAM in the sphere of operational risk management and its impact on the Solvency Capital Requirements?*

0,00%	Negative – it is unnecessary
3,45%	Fairly negative
34,48%	Neutral
31,03%	Fairly positive
31,03%	Positive

Please elaborate:

Use of an internal model rather than dependency on a standard formula calculation.

We do not have any particular views on the SAM requirements in respect of operational risk. We do however feel that SAM provides us with an opportunity to reassess and enhance our capabilities in respect of operational risk management.

We do believe that better data collection and control will really improve the exposure.

We utilise ORM as a tool to improve business processes and service delivery.
It will assist in creating a more accurate calculation of capital requirements, instead of a one shoe fits all approach.

SAM provides minimum ops-risk management strategy.
The implementation will result in greater focus on the enhancement of systemised solutions, the automation of processes and internal controls which will assist in the management of insurance and operational risk. Although SAM principles will aid in the management of risk, it will require additional resources and capital to fully implement and comply with SAM.

Operational risk has been largely ignored in regulatory requirements in the past, but often presents the greatest risk to the survival of an insurer. While we believe that holding capital is NOT the appropriate way to mitigate operational risk, the requirement to do so will raise the profile of operational risk and encourage companies to look more closely at this area.

Even though the need of/for SAM are understood, it is a significant overkill for small insurance entities and results in additional appointments (staff) and/or professional fees in order to attempt to be compliant.

The metrics e.g. NWP is not necessarily a good proxy for OR losses. An internal model will likely be better, especially if good data points are created in Scenarios. Capital will be lower in most cases.

Appropriateness of SAM standard formula for Operational Risk
Operational Risk is very unique to an organisation. Furthermore, operational risk is also very dynamic and changes as an organisation changes. This makes operational risk a very difficult source of risk to calibrate. Arguably a lot of historic losses are required but the older loss data get, the less relevant it becomes. A further challenge is to identify all possible operational risks. All these arguments makes a single industry standard seem quite arbitrary but at the same time an internal view just as difficult to determine. Using premium, reserves or growth as proxies does make sense but is also not necessarily totally accurate. Other relevant proxies could be number of staff, staff turnover, management expenses, level of outsourcing, IT budget, etc. Given our historic measured operational losses, the allowance does seem somewhat excessive. However, it is very possible that some historic losses have not been identified or measured.

20. *How appropriate does your organisation believe that the SAM standard formula for the calculation of the operational-risk component of the SCR is?*

0,00%	Not at all
32,14%	Slightly appropriate
42,86%	Fairly appropriate
7,14%	Highly appropriate
3,57%	Completely appropriate
14,29%	Unsure

21. *How much has your organisation's approach to handling operational risk changed in light of the SAM regulations?*

25,00%	Not at all
25,00%	To a lesser degree
21,43%	To a fair degree
25,00%	To a high degree
3,57%	Totally
0,00%	Unsure

22. Which model will your organisation be using for the calculation of the operational-risk component of the solvency capital requirements of the impending SAM regulations?

67,86% Standard formula
17,86% Internal model
14,29% Unsure

23. Is your organisation currently compliant with the future SAM operational-risk SCR requirements?

60,71% Yes
39,29% No

SECTION 4: EXTERNAL OPERATIONAL-RISK DATABASE

24. Is your organisation aware of industry-wide operational-risk databases such as ORX (global banking industry) or ABI's ORIC (UK insurance industry)?

58,62% Yes
41,38% No

25a. Would an external operational-risk consortium be useful for the South African insurance industry?

3,45% Not at all
20,69% Slightly useful
31,03% Fairly useful
13,79% Highly useful
6,90% Very highly useful
24,14% Unsure

25b. Is such a consortium feasible?

51,85% Yes
48,15% No

Why?/Why not?

Yes. Potentially feasible, however flexibility is required given differing organisational profiles.

No. I believe that a consortium will be feasible in the long term, but not in the short to medium term. The reason is that most insurers will not capture internal loss data for SAM standard formula approach purposes. Post SAM implementation insurers will begin to realise the value of capturing internal loss data for modelling purposes as well as the value of supplementing their internal data with data from other insurers. This need for data will drive the requirements for a consortium. Insurers will initially rely on external loss data from European insurers, similar to what the bank's did under Basel II AMA.

No. Many small operators and niche insurers who will have to make use of standard databases to identify and quantify operational risk.

No. My belief is that the FSB and its myriad of sub committees are fairly competent and communicative.

Yes. Benefits of greater volumes of data.

No. Even though we operate in the same industry and are being measured by the same yardstick – each business is unique in product features and operational requirements.

Yes. Industry imperative.

Yes. Collaborative approach – sharing of ideas.

No. Operational risks are very specific to a company and in most cases depend on a company's culture and structure.

Yes. There is no source of common consolidated data for insurers in South Africa, thus modelling SA-specific operational risk capital on current data is not very reliable.

Yes. An operational-risk consortium will facilitate data and/or information sharing in the industry which will help identify operational-risk trends as well as aid in the identification of emerging risks.

Yes. The data is available – the obstacle to overcome will be companies' unwillingness to share their data.

Yes. FSB can lead this process and making it agnostic to its owners, aggregate and distribute.

No. Data sharing is a problem for insurers.
Operational risks faced by insurers differ due to infrastructure are most severe and this differs from insurer to insurer [*sic*]. Therefore a consortium will not help insurers to manage the larger operational risks faced by insurers.

25c. Which body should be responsible for managing such a consortium?

34,48% FSB
10,34% ASISA
44,83% SAIA
10,34% Other (please specify)

26. *Would your organisation be willing to join such a consortium, provided that strict confidentiality of key information is maintained?*
a. As a subscriber?
85,71% Yes
14,29% No

b. As a contributor?
75,00% Yes
25,00% No

27. *Is there anything else you would like to add on the topic of operational risk management in the South African insurance industry?*
Believe it is a very subjective topic, especially for captive insurers where there are no staff, and most functions are outsourced i.e. dependent on the ability of the outsourced partners to maintain operational-risk managers in their own business.

Business is practical and results driven – theory does not ensure results. The focus must be on the results and not the theory. I expect that there will be insurers that will fail even though they have met the requirements of the theory.

Participation in the consortium would be dependent on (a) cost and (b) relevance to reinsurers.