British Actuarial Journal, Vol. 22, part 1, pp. 68–108.
doi:10.1017/S1357321716000179
First published online 9 November 2016

Good practice guide to setting inputs for operational risk models

P. O. J. Kelliher*, M. Acharyya, A. Couper, K. Grant, E. Maguire, P. Nicholas, C. Smerald, D. Stevenson, J. Thirlwell, and N. Cantle

[Institute and Faculty of Actuaries, Operational Risk Working Party, Sessional Research Event, 21 March 2016]

Abstract

This paper seeks to establish good practice in setting inputs for operational risk models for banks, insurers and other financial service firms. It reviews Basel, Solvency II and other regulatory requirements as well as publicly available literature on operational risk modelling. It recommends a combination of historic loss data and scenario analysis for modelling of individual risks, setting out issues with these data, and outlining good practice for loss data collection and scenario analysis. It recommends the use of expert judgement for setting correlations, and addresses information requirements for risk mitigation allowances and capital allocation, before briefly covering Bayesian network methods for modelling operational risks.

Keywords

Internal Loss Data; External Loss Data; Scenario Analysis; Business Environment and Internal Control Factors (BEICFs); Correlations

1. Introduction and Scope

The aim of this paper is to set out good practice for determining the inputs to operational risk models. The paper aims to cover banking and asset management as well as insurance operational risk models. It is aimed not just at actuaries but also at others involved in operational risk modelling.

There will be a focus on capital modelling as opposed to "business as usual" (BAU) operational risk management. It will cover internal and external data, but will also cover operational risk scenarios and scenario-based approaches to operational risk modelling as well as loss distribution approaches (LDA). However, the paper will not cover wider stress and scenario testing (e.g. flu pandemics; oil shocks) covering financial, operational and other risks as required for the purposes of Own Risk and Solvency Assessment (ORSA), Individual Capital Adequacy Assessment Process (ICAAP) or General Prudential Sourcebook (GENPRU).

The paper starts with consideration of regulatory requirements for operational risk models and wider operational risk data collection. This is followed by a review of good practice outlined in existing academic literature, and then by a general overview of what is required from an operational risk framework to produce the inputs required for modelling purposes.

*Correspondence to: Patrick Kelliher, FIA CERA, 20 Blinkbonny Gardens, Edinburgh, EH4 3HG, UK. Tel: +44 7799 767942. E-mail: patrick_oj_kelliher@yahoo.co.uk

The main part of the paper considers the following key inputs to operational risk models:

- internal loss data (ILD);
- external loss data (ELD);
- business environment and internal control factors (BEICFs);
- scenario analysis;
- risk mitigation; and
- correlation and dependency assumptions.

Often loss data is collected, scenarios analysed and operational risk modelled at an aggregate level. This capital then needs to be allocated back to individual legal entities. The paper will therefore cover points to consider in determining the basis for this allocation.

The paper concludes with a brief overview of inputs to Bayesian network models which are increasingly prominent in the modelling of operational risk, but will not cover these in detail.

2. Regulatory Context

2.1. Overview

2.1.1. Banking and investment firms

The key impetus to the development of operational risk models in banking has been the Basel II framework developed by Basel Committee on Banking Supervision (BCBS) who set key global regulatory requirements.[1] This framework was first published in 2004 and finalised in 2006. For the first time, this required banks and investment firms[2] to hold capital to cover their operational risks. It also gave them the option to base this capital requirement on their own operational risk models under the advanced measurement approach (AMA), subject to meeting regulatory requirements. The operational risk capital requirement is added to regulatory requirements for credit and market risk which together form Pillar I – minimum capital requirements – of the Basel regime.

Pillar I is supplemented by Pillar II, requiring banks and investment firms to have proper risk management systems in place and to assess whether they have adequate financial resources to cover their risks, including operational risk, as part of their ICAAP. Banks and investment firms need to consider whether Pillar I capital requirements are adequate given their operational risk profile, while

[1] In the EU, the requirements of Basel II were implemented as part of the Capital Requirements Directive (CRD) and Capital Requirements Regulation (CRR) which have since been revised to reflect revised requirements stemming from Basel 2.5 and Basel III – for the latest version of the Directive, CRD IV, see: "Council Directive 2013/36/EU of 26th June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC" and for the CRR, see: "EU Regulation no. 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms", both of which are available online at http://ec.europa.eu/finance/bank/regcapital/index_en.htm (accessed 25 January 2016).

[2] There are variations in requirements for investment firms depending on what business they transact. Many firms will be classed as limited activity firms where there is a minimum overall capital requirement of 25% of fixed overheads. See articles 95–97 of the CRR above (also available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0575, accessed 25 January 2016); and for UK investment firms see the Financial Conduct Authority's (FCA) "Capital Requirements Directive (CRD IV) FAQs" available online at https://www.fca.org.uk/firms/markets/international-markets/eu/crd-iv/faqs (accessed 25 January 2016).

AMA banks looking to gain or retain approval for their operational risk models as part of Pillar I need to demonstrate how their models are used as part of wider operational risk management.

Meanwhile, Pillar III relating to market discipline sets out requirements for public disclosure of information relating to operational risk and other exposures including Pillar I operational risk capital requirements converted into a risk-weighted asset (RWA) equivalent.[3]

2.1.2. Insurance

While Basel II was being finalised, in the United Kingdom, the Financial Services Authority (FSA) was requiring insurers to undertake an individual capital assessment (ICA) as part of its Individual Capital Adequacy Standards regime (ICAS). Akin to Pillar II under the Basel regime, ICAS required insurers to consider what capital they needed to cover operational and other risks and served to drive forward the development of operational risk capital models in UK insurers. Based on their ICAs, the FSA could give guidance on the amount of capital an insurer needed to hold for operational risk.

At the time when ICAS was introduced, the EU's old Solvency I regime, Pillar I regulatory minimum capital did not cover operational risk. This has now been addressed by Solvency II which includes an operational risk element as part of Pillar I requirements. Like AMA under Basel II, insurers have the option to apply to use their own internal models to determine the amount of this regulatory capital requirement for operational risk.[4] Those that do not use internal models will need to hold capital as specified under the Solvency II standard formula (SF), although as part of Pillar II they need to justify the appropriateness of the SF figure for their operational risks. SF insurers looking to assess operational risk profile will generally need to gather data on operational losses and the state of controls, carry out scenario analysis, and perhaps carry out some modelling in order to assess the appropriateness of the SF capital requirement to cover operational risks.

2.1.3. Financial Reporting Council (FRC) and Actuarial Profession Standards

Finally, while banks modelling operational risks need to consider Basel requirements, and insurers Solvency II, actuaries in the United Kingdom involved in modelling operational risk need to have regard to the requirements of Technical Actuarial Standards (TASs) issued by the FRC (n.d.). Although these do not apply to non-actuaries, these are still noteworthy in terms of guidance for those wishing to model operational risk.

2.2. Basel Requirements

Basel II specifies three means of assessing operational risk capital requirements (BCBS, 2006a, pages 644–683, "The First Pillar – Minimum Capital Requirements"):

- Basic Indicator Approach (BIA) where capital is based on 15% gross income averaged over the past 3 years;
- The Standardised Approach (TSA) where capital is based on 12%–18% gross income depending on the line of business; and
- AMA where operational risk capital is based on a bank's own model of operational risk.

[3] As Basel II capital requirements were based on a minimum of 8% of RWA for credit risk, operational risk requirements were divided by 8% (i.e. time 12.5) to form a RWA equivalent.

[4] Though unlike the Basel regime which simply adds operational, credit and market risk requirements together, there is scope under Solvency II internal models to allow for diversification between operational and non-operational risks.

Use of both the TSA and AMA are conditional on meeting quantitative and qualitative requirements for regulatory approval, although the burden is significantly higher for AMA. Amongst other things this requires the AMA model to combine ILD and ELD, scenario analysis and BEICFs.[5] There is a need for a minimum of 5 years[6] of relevant ILD for the calculation of operational risk capital, which should satisfy a 99.9% 1-year confidence level.[7] Loss data should be split by material business line, risk type and by gross loss amounts and recoveries, with "boundary losses" relating to overlaps between credit and market risk losses also identified. ELD must be used where relevant, though the banks needs to develop criteria for how ELD should be used and any adjustments made (e.g. scaling to a bank's size). Scenario analysis should be used along with BEICFs to provide a forward-looking view of exposure.[8] While AMA models can allow for risk mitigation, the benefit of insurance is capped at 20% of capital, while there are strict criteria for allowing for risk mitigation in operational risk calculations. The overall framework needs to be validated by internal and external auditors as part of the third line of defence.

The requirements of Basel II were elaborated in *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches (BCBS196)* (BCBS, 2011a). This builds on 2009 BCBS research into operational losses and AMA practices in banks (BCBS, 2009a, 2009b). Amongst other things, the paper specifies criteria for gross loss definition, loss data thresholds, grouping of losses, loss event dates to be used in modelling, correlation and dependency assumptions, and scenario analysis. As well as criteria for recording losses, it also suggests that data be collected on "near-miss" events where no loss crystallised or events which result in gains (e.g. for trading loss events where markets move in the bank's favour). Data should be governed by a data policy while the guidelines set out extensive requirements for the third-line validation and verification of AMA models and data.

Before the issue of the guidelines, the UK FSA also had an Operational Risk Standing Group,[9] which looked at the implementation of Basel II operational risk requirements. This group published a number of papers which are noteworthy in terms of the regulatory expectations set out in the papers.

Alongside the AMA guidelines, the BCBS also published *Principles for the Sound Management of Operational Risk* in July 2011 (BCBS, 2011b), updating a previous principles paper from 2003. While more concerned with BAU operational risk management, it does cover loss data, scenarios and BEICFs in the form of key risk indicators (KRIs) and key performance indicators. Of particular interest is the follow-up review of the principles published by the BCBS in October 2014

[5] The requirement on the use of the various data elements differ from country to country, depending on the preferences of the regulator. The consistent aspect is that banks are expected to "use" all of the elements when coming up with their capital, but how they do this is not defined. For example, in the United States the Federal Reserve does not like banks to integrate their scenarios directly into the modelling. They prefer banks to develop an LDA model using ILD (perhaps supplemented with ELD) and then use the scenarios as more of a benchmark to test how appropriate the resulting distribution is to their risk exposure. In other countries the regulators are much more in favour of banks using the scenarios as pseudo-loss data points in the distribution fitting.

[6] Though a 3-year period is acceptable when a bank first moves to AMA.

[7] Note distinction is made between expected and unexpected losses with no capital required for the former if it can be justified that this is covered from "internal business practices", which is generally interpreted to mean losses covered within operational budgets.

[8] For details of Basel II requirements for internal and ELD, scenario analysis and BEICFs, see BCBS (2006a, pages 670–676).

[9] See FSA, "Operational Risk Standing Group", archived page available online at http://www.fsa.gov.uk/about/what/international/basel/csg/orsg (accessed 25 January 2016).

(BCBS, 2014a), which expands on the principles and lists noteworthy practices in operational risk loss collection and scenario analysis in appendices III and IV.

In addition to review of the principles, the BCBS also launched a consultation on revisions to standardised approaches (BIA and TSA) in October 2014 which proposed to increase the associated capital requirements significantly (BCBS, 2014b).[10] While the business line distinction under TSA may be dispensed with, this could still add to the complexity around standardised approach inputs and calculations. At the time of writing, the BCBS has also said it will consult on dispensing with AMA altogether,[11] though it may extend loss data collection and other AMA requirements to non-AMA firms.

2.3. Solvency II Requirements

The Solvency II directive and associated Level 2 text do not delve into great detail about operational risk beyond the specification of the SF operational risk requirement. However, implicit in internal model regulations is the need to ensure that inputs to internal operational risk models are complete, accurate and relevant. This is worthy of a separate paper in itself but suffice to say operational risk inputs to internal models need to meet very high standards to meet with regulatory approval. As noted, even those using SF will need to demonstrate the appropriateness of this requirement to their operational risk profile, which will need to be supported by loss data and scenario analysis.

More specific to operational risk are the requirements of EIOPA's Systems of Governance (SoG) guidelines which were issued in September 2013 and which most EU regulators have adopted with effect from 1 January 2014 (i.e. 2 years before the main implementation date for Solvency II).[12] Inter alia, this sets out the requirement to collect operational loss data and conduct scenario analysis, with the former to include near misses as well as actual losses.

2.4. Prudential Regulatory Authority (PRA) ICA and Systems and Controls (SYSC) Requirements

The PRA[13] sets out ICA requirements for insurers in the section 7 of the Prudential Sourcebook for Insurers (INSPRU) standards in its Prudential Sourcebook (PSB). While requiring all risks to be

[10] The paper proposed increasing requirements by two to three times for TSA and dispensing with BIA. For the IFoA's January 2015 contribution to this consultation, see http://www.bis.org/publ/bcbs291/iafoa.pdf (accessed 25 January 2016).

[11] This was mentioned in the BCBS January 2016 press release "Revised market risk framework and work programme for Basel Committee is endorsed by its governing body" (available online at http://www.bis.org/press/p160111.htm, accessed 25 January 2016), as well as in speeches by BCBS members, for example "From the Vasa to the Basel framework: the dangers of instability" by Mr Stefan Ingves, Chairman of the Basel Committee and Governor of Sveriges Riksbank, at Unique Lecture at the 2015 Annual Convention of the Asociación de Mercados Financieros, 2 November 2015, Madrid, Spain (http://www.bis.org/speeches/sp151102.htm, accessed 25 January 2016).

[12] For the guidelines plus supplementary EIOPA commentary and consultation responses, see *EIOPA Final Report on Public Consultation No. 13/008 on the Proposal for Guidelines on the System of Governance* (EIOPA, September 2013, available online at https://eiopa.europa.eu/Publications/Reports/EIOPA-13-413_Final_Report_on_CP8.pdf#search=Final%20Report%20on%20CP8, accessed 25 January 2016). Note in particular Guideline 19 and supplementary text (pages 5.66–79) as well as pages 3.65–67 and 3.121–124. For UK insurers, the PRA's approach to implementing these and other EIOPA guidelines can be found in the PRA's December 2013 Supervisory Statement SS4/13 "Solvency II: applying EIOPA's preparatory guidelines to PRA-authorised firms" (available online at http://www.bankofengland.co.uk/pra/Documents/publications/policy/2013/solvency2preparatory.pdf, accessed 25 January 2016).

[13] The PRA is part of the Bank of England and superceded the FSA in prudential regulation in April 2013, with the FCA taking over from the FSA on conduct regulation at the same time.

considered as part of the ICA as well as consideration of scenario analysis, this does not explicitly cover operational risk. However, the FSA expanded on its expectations of ICA operational risk coverage in a series of insurance sector briefings:

- November 2005 (FSA, 2005, pages 4.14–29) – operational risk measurement was listed as a key area of development, noting that there was a lack of loss data and hence a reliance on scenario analysis.
- November 2006 (FSA, 2006, pages 3.62–63) – this again noted the absence of credible historic loss data and the greater need for management judgement in assessing risk exposures.
- October 2007 (FSA, 2007) – the FSA noted that operational risk was one of the main reasons it had applied a capital add-on to insurers assessments, and set out its expectations including inter alia the need for robust challenge and validation of operational risk assessments and dependency assumptions.

As well as ICAS, the PRA also set out requirements for the management of operational risk in sections 13 and 14.1 of the SYSC part of the PSB, with further requirements for insurers set out in 5.1 of the INSPRU sourcebook. These require consideration of internal and external losses, the state of risk controls and scenario analysis.

2.5. FRC Standards

The FRC issues both generic TASs as well as standards specific to different lines of work. In general, TASs will be targeted at work that is commonly (but not necessarily exclusively) performed by actuaries in the United Kingdom, with distinction made between work reserved for actuaries and required work which is a legal obligation but which may be performed by non-actuaries. While actuaries are bound by their profession to comply with TASs, the standards are a useful guide for non-actuaries in modelling operational risk, setting out detailed lists of points to consider in modelling. Further details of these and other Actuarial profession requirements can be found in Appendix B.

3. Literature Review

The Working Party reviewed a number of papers on operational risk for insight into good practice in setting inputs for operational risk models. The papers reviewed are set out in Appendix A along with a brief synopsis of the points made in relation to operational risk inputs.

In terms of key themes identified by the Working Party from this review:

- A common theme emerging is the difficulty of modelling low frequency, often high severity, events given the lack of historic data and changes in operational risk profile over time.
- There would appear to be a consensus about using a combination of loss data, both internal and external, together with scenario analysis.
- There is a need for a prospective view of risks to complement the historic view provided by loss data. This could be provided by scenario analysis, though care needs to be exercised to ensure scenarios are not anchored on past events and appropriately reflect the change in control environment since the past events occurred.

4. General Requirements

Any operational risk model will only be as good as the firm's underlying framework for the identification, assessment and management of operational risk losses. Without an adequate operational risk management framework, losses may not be captured while scenario analysis is likely

to miss important risks. Priority should be given to addressing any deficiencies in the operational risk control framework over operational risk modelling.

4.1. Operational Risk Categorisation

A key element of the operational risk framework will be a detailed operational risk categorisation system. Operational risk is a heterogeneous category covering all risks associated with people, processes and systems. This will cover risks as diverse as systematic processing errors, cyber crime, health and safety breaches and product literature failings to name but a few of the risks typically covered. There is a need to break operational risk down into more homogenous categories to enable exposures to be properly understood and modelled. This is dependent, however, on a categorisation system that is robust with little scope for ambiguity in terms of how losses and risks should be categorised.

Firms will have their own systems for categorising operational risks but in terms of generic categorisation systems, Basel II identified seven high Level 1 categories of operational risk and 20 Level 2 categories sitting underneath this (BCBS, 2006b). A more detailed yet still freely available categorisation system is that of the Institute and Faculty of Actuaries' (IFoA's) Risk Classification Working Party (Kelliher *et al*., 2013) which starts from the Basel II Level 2 categories and identifies some 350 Level 3 sub-types of operational risk.[14]

Typically, operational risk is modelled for each Level 2 category (or equivalent level in the firm's own categorisation system). The Basel Level 1 categories might be insufficiently granular, while there is likely to be insufficient loss data to model each Level 3 sub-type, and running scenario analysis exercises for each Level 3 would be impractical.

Whatever categorisation system is used should be as detailed as possible to reduce the scope for ambiguity in categorisation. Taking the Basel Level 2 categories as an example, there could be confusion as to whether cyber theft of assets should come under the (external fraud) theft and fraud or the system security categories. This in turn could lead to losses being reported in one category when they are meant to be classed and modelled under another. To use a general insurance analogy, this would be akin to classifying flood losses as fire, say, compromising the modelling of each peril.

Similarly, a common scenario analysis failing is where the same risk is considered under two separate categories due to confusion as to which category it should come under, or worse, that the risk is missed altogether.

The IFoA Risk Classification Working Party categorisation did not just refine the Level 2 categories further with Level 3 sub-categories, it also identified areas where these categories could overlap and suggested demarcation lines. Crucially, this extended not just between operational risks but between operational and non-operational risks as well. There can be significant overlaps – for instance, dealing error losses will depend on market movements.

Basel II gives extensive guidance on the demarcation between operational and other risks for banks, particularly regarding "boundary" losses overlapping between credit and operational risks.

[14] The detailed categorisation can be found online at http://www.actuaries.org.uk/research-and-resources/documents/underlying-spreadsheet-discussion-paper-common-risk-classification (accessed 25 January 2016) with details of the principles of this system – which also covers strategy and other non-operational risks – set out in the Risk Classification Working Party paper: http://www.actuaries.org.uk/research-and-resources/documents/common-risk-classification-system-actuarial-profession (accessed 25 January 2016).

However, the demarcation for insurance risk is less clear. For instance, failure to follow underwriting guidelines may be viewed as a processing error but this will affect claims experience and reinsurance recoveries. Similarly, while non-disclosure of underwriting information may be viewed as a form of fraud, the impact of this will be implicit in claims experience and so may be implicitly covered under insurance risk.

Considerable confusion can also arise between operational and strategy risks. There is no standard definition of strategy risk like there is for operational risk under Basel II and Solvency II. The IFoA Risk Classification Working Party defined strategy risk in terms of risks to goodwill made up of the value of new business and value generated by future back-book initiatives, with operational risk covering risks affecting balance sheet and embedded values. Generally, goodwill is excluded from regulatory capital resources and so strategy risks affecting this should be similarly excluded from capital requirements (see section 5.1.1 below). Whatever definition of strategy risk is used, it is important that the distinction between this and operational risk and what should and should not be included in economic capital modelling, is clearly understood.

To conclude, whatever the organisation, there is a need for the categorisation system to identify the overlaps between categories and to have a clear view as to whether risks should be covered under operational risk or some other category.

5. ILD

5.1. Operational Risk Events and Losses

Just as it is important to have clarity as to which category an operational risk event falls under, it is equally important that loss data collected captures all impacts relevant to operational risk capital modelling. This includes cash outlays such as

- customer compensation costs – this should generally include ex gratia payments as these are typically offered to settle complaints and avoid further costs being incurred;
- other compensation costs including that payable to shareholders, bondholders, staff and members of the general public in respect of operational events;
- regulatory fines including Ombudsman costs;
- legal fees and other additional legal costs associated with operational events – this should include the cost of successfully defending legal action if this cannot be recovered, it should also include the costs associated with shareholder lawsuits;
- additional consultancy costs required to investigate and remediate problems including the cost of section 166 and other reviews carried out at the behest of regulators;
- IT contractor and other external resources brought in to help rectify problems;
- property damage – the cost of repairs under leasehold agreements and/or the impairment of property assets owned, plus the cost of replacement accommodation;
- mailing and other additional customer communication costs;
- overtime, temporary staff and other unbudgeted staff costs arising as a result of the operational risk event; and
- other marginal, unbudgeted costs arising as a result of the event.

Capital modelling will generally consider movements in net equity (own funds in the case of Solvency II). Therefore it is important to consider not just cash outlays but other movements in assets and liabilities arising from an operational risk event such as

- provisions required to be set up, e.g., higher guarantee and option costs arising due to flawed documentation and/or adverse legal rulings;
- re-statements of existing liability values due to valuation errors or deliberate under-provisioning;
- asset values being written off due to valuation errors, issues with asset title or other operational event; and
- loss of tax credits.

For life insurers subject to Solvency II, the present value of future profits may count towards own funds. Therefore there is a need to consider operational risk events which may compromise such future profits. This would include restrictions in charges that can be levied due to flaws in contract wording or regulatory caps imposed. It would also encompass higher future costs arising, e.g., increased disclosure requirements on pension policies.[15]

Similarly, general insurance technical provisions may reflect expected profits implicit in unearned or bound but not incepted premiums (EPIFP). Operational risk impacts which reduce the profits emerging on existing business and EPIFP should be captured in loss data.

5.1.1. Impacts to be excluded

Just as important as capturing all impacts of an operational risk event relevant to capital modelling is the need to exclude those impacts which are not relevant to capital from data used to calibrate models. These include

- Loss of new business profits – the value of future new business profits is typically excluded from regulatory capital calculations so it would be appropriate to exclude the loss of such profits in capital calculations.[16]
- Impairments of goodwill and intangible assets which are also excluded from regulatory capital calculations.
- BAU costs such as the basic salaries of existing employees engaged in managing an operational event – only marginal costs of the event should be considered, not costs already budgeted.

Note that even if impacts could not be captured for operational risk capital modelling purposes, they should still be captured as part of the operational risk data collection process for wider risk management purposes, though they should be capable of being separated out and excluded in loss data for capital modelling purposes.

5.1.2. Reputational damage

Reputation damage will mostly manifest itself in lost sales, the value of which, as noted above, are typically excluded from regulatory capital calculations. There may also be an impact on persistency while unit costs may increase if the reputation damage causes the portfolio to shrink.

[15] It could also include the risk that management information is flawed resulting in assumptions (e.g. for persistency) which are unduly optimistic, resulting in an overstating of future profits implicit in technical provisions.

[16] Though it would still be appropriate to allow for losses on new business due to operational risk events, e.g. pricing errors.

Care should be exercised before including persistency and expense impacts in operational loss data as they may already be captured under insurance risk for insurers under Solvency II, or as part of business risk under banks' ICAAP. If so, including these in operational loss data for modelling purposes could result in double counting of requirements. Where the risk of higher lapses arising from reputational damage associated with operational risk events is captured under insurance as opposed to operational risk capital, however, then this should be reflected in the correlation between operational and insurance risks.

5.1.3. Change risk

Cost overruns and other operational losses affecting change programmes need careful consideration. There is a need to consider two types of change programme, mandatory and discretionary. Mandatory change programmes are those which the firm has to undertake in order to remain in business, and will include most change programmes driven by regulatory requirements like Solvency II and Basel III.[17] Cost overruns and other unbudgeted expenses associated with such programmes should be captured as operational losses.

By contrast, where costs begin to escalate on discretionary programmes such as new products and/or systems, the firm has the option to cancel the programme. Often the benefit foregone from the failure of a discretionary project will be the loss of future new business, the value of which, as noted, should generally be excluded from operational risk models. However, some discretionary project investment may be brought onto the balance sheet as an intangible asset, and failure of the project could result in a balance sheet write-down of this asset.[18] If the asset contributes to economic capital resources, then write-downs of such assets should be included in operational risk modelling.[19]

Note that there may also be knock-on impacts from failure of a systems change programme such as greater reliance on manual processing which should be considered as part of scenario analysis (see section 8.1 below).

5.1.4. Gains and "near misses"

Many operational risk events do not result in a loss or may even result in a gain. For example, a dealing error could lead to a gain if markets move in the firm's favour, while premises may be spared from fire because of wind direction.

BCBS AMA guidelines suggest capturing gains and "near misses" to help identify loss events and to contribute to scenario analysis (BCBS, 2011a, page 89). Similarly, EIOPA is of the view that meeting Solvency II risk management requirements requires "identifying all operational risks that have crystallized and their near misses".[20]

[17] In some instances, there may be an alternative, e.g., closing a particular business line to avoid new regulations relating to sales.

[18] For example, the Co-Op Bank wrote-down nearly £300 million over 2012 and 2013 in respect of a failed IT investment – see pages 7.60 of the *Report of the Independent Review into the Events Leading to the Co-Operative Bank's Capital Shortfall* (Sir Christopher Kelly, April 2014, available online at http://www.co-operative.coop/PageFiles/989442031/kelly-review.pdf, accessed 25 January 2016).

[19] Typically, however, intangible assets are excluded from capital resources so again it would not be appropriate to allow for write-downs of these in operational risk models.

[20] See page 3.124 of EIOPA's September 2013 paper *EIOPA Final Report on Public Consultation No. 13/008 on the Proposal for Guidelines on the System of Governance* above.

The Working Party is also of the view that ILD for capital modelling should capture gains and near misses as well as losses from operational risk events. Without capturing these, the frequency of operational risk failings will be understated. Meanwhile, the shape of the severity distribution will be skewed whereas a symmetric distribution may be more appropriate.

Worse, ignoring gains and near misses could lead to tail risks being missed. For instance, failure to ensure appropriate collateral is posted under a derivative arrangement will generally not result in a loss as this would only crystallise if the counterparty defaulted. However, were the counterparty to default, operational failings in collateral management could exacerbate the loss.

Capturing such failings, even though they do not normally result in a loss, can highlight risks which can give rise to losses at the tail. Also, our understanding of correlations can be greatly improved from analysing multiple near misses arising from a common event. This is especially useful when the potential size of the loss avoided is high.

5.1.5. Gross versus net losses

Often operational losses may be offset by recoveries under insurance policies or other risk mitigation techniques (e.g. third-part indemnities – see sections 5.1.6 and 10.2 below). Modelling losses net of these recoveries will lead to implicit allowance for risk mitigation in capital calculations. This could cause issues with the 20% limit on the capital benefit from insurance under Basel II, so the BCBS recommends that at the least, loss data used for AMA models should exclude any insurance recoveries (BCBS, 2011a, pages 21–24 and 90–103).

The Working Party believes capital models should model losses gross of (i.e. before) insurance and other recoveries, which should be modelled separately. Modelling losses net of recoveries obscures both gross exposure and the benefit of insurance and other risk mitigation techniques. Insurance and other mitigation arrangements may change, in which case net data will no longer be relevant.

There may also be regulatory limitations on the amount of benefit that can be taken in respect of insurance and other risk mitigation techniques – as well as the 20% limit above, there are qualitative requirements to be met before these can be allowed for under both Basel II and Solvency II.[21] Failure to meet regulatory criteria could lead to the mitigation benefit being scaled back or omitted. For this reason, there is a need to separately quantify the benefit from risk mitigation which requires gross loss and recoveries to be modelled separately.

5.1.6. Third-party losses

Many firms will be exposed to failings by third parties such as outsourcers providing administration services and asset managers managing the firm's assets. Generally, the third parties will indemnify the firm for any loss incurred, but disagreements may arise with respect to who is liable for a particular failing and/or the contract may not require indemnification. In extremis, even if the third party is liable, if it is insolvent it will not be able to compensate the firm in full. Firms may have significant latent exposure to third-party operational failings.

[21] See BCBS (2006a, pages 678–679) and Solvency II, Chapter V, section 10, articles 208–215 of delegated regulations 2015/35, October 2014, available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0035 (accessed 25 January 2016).

The Working Party believes that firms should try to collect details of third-party operational loss events affecting the firm to properly understand and model this exposure. Consistent with the separate modelling of gross losses and recoveries, gross loss impacts should be collected separately from recoveries under indemnity agreements. Ideally, they should also obtain data on third-party operational risk events which do not affect the firm but which may point to problems with the third party's control framework.

Firms should also try to capture gains and near misses – e.g., an asset manager may breach mandate limits on equity exposure but if markets rise, this could result in a gain. Similarly, outsourcers might have a narrow escape from business continuity events which could have had the potential to disrupt service to the firm's customers.

It is recognised that this may be difficult, particularly if existing contractual arrangements do not oblige third parties to report on loss events. Going forward, however, new agreements should require such reporting.

While not quite a third party, a firm's pension scheme is generally run at arm's length from the firm under a separate trust. Nonetheless, the firm may still be exposed to operational risks run by the pension scheme as the assets and liabilities of the scheme will come through on the firm's balance sheet under International Accounting Standard 19 (IAS19). Operational risks could increase deficits (or reduce surpluses), leading to balance sheet strains. Examples of these risks include

- errors in record keeping leading to under-estimation of liabilities;
- historic under-payment of pensions and other benefits for which beneficiaries need to be compensated;
- flaws in legal documentation (e.g. in respect of the definition of accrued benefits) or adverse interpretation by courts of this documentation could lead to increases in scheme liabilities; and
- dealing and other asset manager errors could affect scheme assets.

Ideally, the pension scheme will maintain a register of operational risks affecting the scheme, and the governance arrangements between the firm and the scheme would be such that these operational risks and events are reported to the firm. The Working Party acknowledges, however, that this may not be possible in practice given the separate nature of the scheme.

Finally, where a life insurer has a with-profit fund (WPF), it may be possible to charge some operational losses back to the WPF and hence to policyholders. Consistent with the treatment of gross and net loss data in section 5.1.5 above, loss data should capture the gross loss and the amount charged back to WPF separately. If only the net amount after chargeback is captured, then changes in what can be charged back to the WPF will invalidate historic data.

5.2. ILD Collection

Having determined the ILD to be collected, firms need to ensure processes and procedures are in place to capture these data. This should tie in with wider operational risk management and incident reporting procedures. The BCBS recommends that banks should develop data policies and procedures around ILD, including reporting thresholds, loss dates and grouping of losses (BCBS, 2011a, page 20).

Typically, first-line business units will be tasked with recording and reporting on any operational risks that come to light. Detailed instructions should be provided to those charged with recording internal losses to ensure

- losses are correctly categorised under the correct category;
- there is clarity as to which impacts should or should not be captured, consistent with section 5.1 above; and
- insurance and other recoveries (as well as WPF chargebacks) are separately recorded and not netted off, while gains and near misses are also captured.

Loss reporting should capture details on what gave rise to the event including any controls which may have failed. As well as informing BAU operational risk management and helping prevent further recurrences, this information can help in causal analysis of losses and identifying common dependencies between risks.

Note that in designing the loss reporting process, care should be given to the burden this places on first-line staff. If this is overly burdensome, if first-line staff are not engaged with the process, and/or if they do understand the requirements, then the quality of loss data will suffer.

Ideally, there would be a seamless process for the reporting of losses which is intuitive and easy to complete. This should be supported by training on the importance of accurate loss reporting, including the need to report on gains and "near misses", supported by succinct yet comprehensive guidance on the loss elements from section 5.1 above. Reporting should ideally be done online as opposed to by paper to prevent loss data being lost and to make it easier to collate and interrogate data.

This process should also tie in with the incident reporting process with first-line staff encouraged to report issues before they crystallise as a loss, gain or "near miss". Loss reporting should be an extension of incident reporting rather than a separate process. Finally, internal audit should check whether all incidents and losses are being reported in a timely and complete manner. There should be sanctions in place for those who do not do so.

5.2.1. Loss reporting thresholds

Reporting on operational losses can take considerable time depending on the amount of information to be captured. For practical purposes, a firm may decide only to capture losses above a certain de minimis level.

This is covered in detail in the BCBS's AMA guidelines.[22] This specifies that applying thresholds should not result in the omission of data that is material to the quantification of operational risk exposure. This level of materiality could perhaps be assessed by modelling the impact of higher thresholds applied to data. Excluded losses will contribute to discrepancies between reported operational losses over the threshold and accounting data covering losses in aggregate, so their materiality can also be inferred from such discrepancies (see section 5.2.5 below).

One issue to be aware of in the application of loss thresholds is near misses. These should not be excluded even if no loss arises, as often the loss avoided could be significant. Instead, consideration

[22] See BCBS (2011a, pages 104–120) – note that while Basel II cites €10,000 as a threshold, this confirms that this is just an example and that firms should set thresholds appropriate to their own business and operational risk profile.

should be given to the potential loss that could have arisen, with the event only excluded from reporting if the potential loss was below the threshold.

Rather than excluding losses from ILD on materiality grounds, there may be a case for "light touch" reporting below a certain threshold level, for instance, only reporting the loss amount without any supporting detail. This could avoid some of the problems associated with applying loss thresholds while reducing the reporting burden on the first line.

5.2.2. Dates of internal losses

There can be a considerable lag between when an operational risk event occurs, the discovery date when it first comes to light, when provision is made for the loss and when it is finally settled. To take Payment Protection Insurance (PPI) mis-selling as an example, many policies were mis-sold before the millennium, while the FSA started to flag its concerns in 2005.[23] Banks started to set aside substantial provisions from 2011 onwards, and have had to provide additional amounts since then.[24]

In its AMA guidelines, the BCBS covers internal loss dates in detail (BCBS, 2011a, pages 121–138). It highlights three key "reference dates": the date of occurrence, the discovery date and the accounting date, and specifies that no other dates are acceptable for building a calculation data set. It notes that discovery and accounting dates are likely to be the most prudent choices for developing a bank's data set for modelling operational risk as the occurrence date may fall outwith the time series used for capital modelling.[25]

The Working Party believes the three reference dates above should be captured as a minimum. In just the same way as there is a need to capture accident, reporting and settlement dates for general insurance losses to understand exposure to incurred but not reported (IBNR) claims and those that are reported but not yet settled, there is a need to capture the occurrence, discovery and accounting dates of operational losses to understand the lag between event occurrence and the emergence of losses, and hence the latent exposure that can exist for many operational risks. It is acknowledged, however, that it may be difficult to identify a date of occurrence. For example, with cyber theft it may be difficult to identify the date systems were originally breached and this may need to be estimated.

5.2.3. Grouping internal losses

One problem that can arise with loss data thresholds is where multiple losses from the same incident fall each fall below the threshold but in aggregate are material. More generally, separate reporting of individual losses associated with a common event may overstate the frequency of losses but understate the severity of the event. For instance, PPI mis-selling has generated millions of claims for banks, but these should be viewed in aggregate rather than as individual data points. Modelling individual losses as opposed to modelling these in aggregate could understate capital requirements.

[23] FSA, October 2006, "The Sale of Payment Protection Insurance – results of follow-up thematic work", available online at http://www.fsa.gov.uk/static/pubs/other/ppi_thematic.pdf (accessed 25 January 2016).

[24] For example, Lloyds Banking Group (LBG) set aside £3.2 billion in its Q1, 2011 results has had to provide ca. £10 billion since then – see LBG's "Q1 2011 Interim Management Statement" available online at http://www.lloydsbankinggroup.com/globalassets/documents/investors/2011/2011may5_lbg_q1_ims.pdf (accessed 25 January 2016) and its "2015 Half Year Results Press Release" available online at http://www.lloydsbankinggroup.com/globalassets/documents/investors/2015/2015_lbg_hy_results.pdf (page 10, accessed 25 January 2016).

[25] See BCBS (2011a, page 131) for issues with occurrence dates.

BCBS AMA guidelines require banks to develop criteria to identify where individual losses are related and when these should be aggregated (BCBS, 2011a, pages 139–159). It also covers where banks may group unrelated losses – for instance, high frequency, low impact losses could be grouped and modelled in aggregate.

The Working Party believes the AMA guidelines should also be considered by insurers who face similar issues in terms of multiple losses arising from common failures (e.g. pensions mis-selling). At the least, firms should be able to identify losses from a common cause and give appropriate guidance to the first line in how to report such losses.

An idea might be to record common causal events as part of operational loss data. For instance, individual PPI claims could be linked to a common PPI mis-selling event identifier. This could be extended to other types of loss such as insurance claims, e.g., higher claims arising as a result of flawed policy wording. This could help inform assumptions about dependencies between risks.

5.2.4. Recurring losses

For banks, expected operational losses included in operating budgets can be excluded from AMA capital calculations. Thus there is a need to identify the extent to which operational losses have already been allowed for in existing operating budgets to compare with the original assessment of expected losses. There is also a need to identify losses which are recurring in nature and which should be included in the expected loss estimates going forward.

Recurring losses are also an issue for life insurers but for different reasons. If operational losses can be reasonably expected to occur over the lifetime of the in-force business, then there may be need to capitalise these expected losses over this period and add them to technical provisions as well as allow for these in embedded value calculations. Depending on how such losses are treated in expense analyses, however (see below), they may be already implicitly allowed for in maintenance expense assumptions and so such an adjustment would be unnecessary. Either way, recurring losses should be identified for further consideration to determine whether they are implicitly allowed for or whether additional allowance is required for these.

5.2.5. Governance and validation of ILD

ILD submissions by first-line business functions should be subject to independent review and challenge to ensure losses have been correctly categorised and that all relevant elements have been captured. This review may be conducted by second-line risk management and/or third-line internal audit functions. In its AMA guidelines, the BCBS suggests internal and/or external audit review and validation (BCBS, 2011a, pages 14–15, 43–69). However, the second-line function should also review loss submissions in order to keep abreast of developments in operational risk profile. They may also be able to provide different technical and analytical skill sets than those available to internal audit.

As well as review of individual loss submissions, ILD should also be reconciled with accounting data as far as possible. This requires a granular breakdown of accounting data by expense type (compensation payment, fine, etc.). There may be issues with certain lines of expense which may capture costs unrelated to operational risk, e.g., consultancy spend may not distinguish between that incurred as part of remediation work and more general advice work, while similarly IT contractor spend may not be split between those involved in remediation and those involved in

broader system development. As noted in section 5.2.1 above, accounting data may also pick up on losses below thresholds which are not included in operational loss data.

For insurers, operational losses included in expense analyses should be identified. If these losses contribute to maintenance and claim costs from which expense assumptions are derived, then there will be an implicit allowance for operational risk in technical provisions and embedded value calculations which use these assumptions. Note however that such operational losses are frequently treated as "one off" costs in expense analyses so it cannot be assumed that they are implicitly captured.

5.3. Limitations of ILD

ILD is objective and is specific to the firm's operational risk profile. However, there are a number of limitations with such data. First, most organisations have only been systematically collecting operational risk data for 15 years or less. This is unlikely to be sufficient to model low frequency, high impact operational risks faced by firms. To use a general insurance analogy, it would be akin to modelling UK windstorm damage using data only going back to a given point (e.g. the year 2000) when this may exclude a large loss (e.g. the great storm of 1987) in the data set.

Even for the period for which data has been collected, it may not capture all losses that have arisen due to the lag that exists between loss occurrence and emergence for many operational risks. For instance, a firm may already have been infiltrated by cyber criminals but the breach has still to be detected. Looking back to 2010, e.g., banks' loss data sets would have not included the large-scale losses which have emerged since in respect of LIBOR fixing even though this was prevalent before 2010.

Another issue is that even for reported losses, ILD may be incomplete as the loss has still to be fully settled. As the example of PPI has shown, provisions set aside may prove inadequate, and so there is a need to separately consider how existing loss estimates may vary over time – the BCBS AMA guidelines suggest this could be considered as part of scenario analysis (BCBS, 2011a, page 135).

Finally, a key issue with ILD is that it is historical in nature as opposed to forward looking. It will not capture new exposures (e.g. risks associated with the segregation of client funds for a new wrap proposition) while some historic data may be irrelevant due to changes in controls (e.g. improved fraud controls) or to changes in the underlying exposure (e.g. mortgage endowment mis-selling losses may no longer be relevant due to time bars).

To conclude, ILD is unlikely to be adequate on its own to model operational risk. There is a need to consider both larger data sets (i.e. ELD) and to take a prospective view of operational risks through scenario analysis and consideration of BEICFs.

6. ELD

One way to enhance ILD is to use ELD. ELD may be used to calibrate severity distributions and/or to model operational risks which are not present in ILD.

6.1. Sources of ELD

There are a number of sources of external operational loss data. One is the Operational Risk eXchange Association (ORX), which was founded in 2002 for financial services firms to share details

of operational loss events on a confidential basis.[26] It sets standards for operational risk categorisation and loss data which helps ensure consistency in submissions and facilitate ease of comparison. In terms of size, it currently has 85 member firms – mostly banks and asset managers but now including insurers – and processes 15,000 loss events per quarter. As of 30 June 2015, its global banking database had over 450,000 loss events with a total value of €273 billion.

For insurers, another source of external data is that provided by ORIC International.[27] Similar to ORX, it was founded in 2005 for insurers to share information on operational losses, and sets standards to ensure consistent classification and recording of losses. Originally, set up for UK insurers under the auspices of the ABI, it is expanding internationally and now has 40 members.

Both ORX and ORIC require participating firms to share their own losses in order to participate in the wider database. Some firms may prefer not to share their own losses, which would preclude them accessing confidential loss sharing databases. Such firms could still access databases which collate publicly available details on operational losses. One such source would be IBM Algo First which has details of over 13,000 loss events.[28]

6.2. Collecting and Adjusting ELD

There are three key challenges to using external data in operational risk models. The first is ensuring consistency between the external data and the firm's model. External data should be capable of being mapped to the risk categories used by the firm to model risk.

It should separate out insurance and other recoveries, and capture the same loss elements as internal date (see sections 5.1 and 5.1.1 above). Ideally, it should also capture gains and "near misses".

The second challenge will be scaling external losses to reflect the size of the firm. Ideally, external loss details would include details of firm size to allow losses to be scaled, e.g., for employee relations, there would be details of headcount and/or payroll of the firm that suffered the loss to enable the loss to be scaled to one's own employee totals. In practice, to preserve anonymity of contributing firms, this information may not be available.

An acceptable alternative may be if the ELD provider scaled losses to standard sizes which firms could then adjust according to their own size. However, there is no generally accepted way of scaling external data.

The third challenge is ensuring that the loss data reflects any changes in controls or in the business environment since the losses occurred. Typically, operational controls are strengthened after an event and hence the frequency and/or severity could be very different after the event than before. Complicating matters, while a firm may have sight of changes in its own control framework and business environment, it is unlikely to have such detail on its peers.

[26] For further details, see the ORX Association website at http://www.orx.org/Pages/HomePage.aspx (accessed 28 January 2016).

[27] For further details, see ORIC International's website at https://www.oricinternational.com/ (accessed 25 January 2016).

[28] One such sources would be IBM Algo First that has details of over 13,000 loss events.

As for internal losses, external data should be subject to a review and challenge process to ensure: that it is properly mapped to the firm's own categories, that relevant impacts have been captured and that recoveries have been separated out. Note the amount of external losses may be far greater than internal losses so this review process needs to be proportionate. For instance, there may be large volumes of low severity card fraud losses in bank external data, so it might be appropriate to only review a sample.

The review process should also consider the relevance of losses for a firm. For instance, LIBOR fixing by an investment bank may not be relevant to a small building society, while unit pricing errors may not be relevant to a life insurer which only writes non-linked business. However, some insurance losses may be relevant to banks and vice versa – external losses should not be automatically discarded just because they arise in a different industry.

6.3. Limitations of ELD

External data will not be suitable for modelling operational risk: if the data cannot be mapped to a firm's own risk categories, if it does not cover the loss impacts assessed as part of internal data, if it does not split out insurance and other recoveries, if different firms use different loss data thresholds and/or if external data is not scalable. It may still be useful, however, for informing scenario analysis and aiding BAU operational risk management in terms of learning from other organisations' mistakes.

Even if external data can be used in modelling, it is worth noting that it shares a lot of the weaknesses of ILD. Even though it covers a greater number of firms, this does not guarantee that it will capture low frequency risks. What often happens with high impact operational risks is that they hit multiple companies around the same time rather than being spread out over a prolonged period.

So, for instance, banks were hit around the same time with PPI mis-selling and LIBOR fines, while pensions mis-selling crystallised for life insurance companies at the same time as part of an industry-wide review mandated by the regulator.

This is not to say that a high impact loss cannot crystallise elsewhere before it affects one's own firm, but extending data to other companies may still miss out on low frequency, high impact risks. Using the general insurance analogy from section 5.3 above, extending windstorm claims data to cover other companies back to say 2005 still misses out the 1987 event.

Like ILD there are also issues with the relevance of historic ELD. This is exacerbated by the multiple companies involved who will be adjusting their product mix, controls, risk appetite and operational risk profile over time. As noted, while we may have sight of changes in profile in one's own firm, changes in other companies' profiles may be obscure.

In summary, even if external data could be incorporated into modelling, there will still be an issue with historic data not capturing low frequency, high impact risks though it would capture a greater range of loss events. Like ILD, there will still be issues around the relevance of historic data to the firm, with the added question as to whether historic losses in other firms are relevant.

7. BEICFs

A key limitation of both internal and ELD is its historic perspective of loss exposure. A forward-looking perspective of operational risks is required which has regard to changes

both in gross exposure and in the controls environment. BEICFs can contribute such a perspective.

Most organisations will carry out Risk Control Self-Assessments or more stringent control assessments to meet corporate governance requirements.[29] This can give a perspective of the current state of controls. Tracking control assessment results over time can highlight any improvement or deterioration in the control environment, which can help assess the relevance of ILD.

Firms should also have KRIs in place to track operational risks. These should ideally be leading indicators that would highlight issues before they arise (as opposed to lagging indicators triggered by an event). Examples of KRIs include

- number of complaints – while a lagging indicator, changes in complaint volumes can point to conduct risk issues emerging;
- staff turnover – rising turnover will affect the experience levels of staff and hence manual processing errors, it may also highlight employee relations issues emerging;
- six sigma – many firms track these as a metric of process error, and a deterioration in score can point to rising levels of process failures; and
- IT outages – this could highlight weaknesses in IT infrastructure which could lead to a major failure in future.

In addition, key control indicators could provide an early warning of potential operational losses in the future. An example of such an indicator may be the number of business continuity plans which are incomplete, which can indicate how resilient the firm would be to business continuity events.

While BEICFs can yield valuable insights into risk profile, they can be difficult to incorporate into models (BCBS, 2011a, pages 255–256). They could however be used to adjust model results. They should also be fed into the scenario analysis process which in turn should feed into operational risk models.

8. Scenario Analysis

Operational risk scenario analysis is an essential input to operational risk modelling as well as a key tool for identifying and managing operational risks. While inherently subjective, done well it should draw on the knowledge of subject matter experts (SMEs) across the business to form a prospective view of risk having regard to the state of controls, and can identify risks which have yet to crystallise.

Scenario analysis will often be carried out for each Level 2 risk category, but it could be carried out by function or scenarios could be identified on an ad hoc basis as part of 1:1 interviews with SMEs, based on their concerns. Separate scenario analysis may be carried out for different business units, legal entities and/or territories. Whichever way they are carried out, a key challenge will be ensuring that all material risks have been considered as part of the scenario process.

In terms of roles and responsibilities, typically the second-line risk management function will facilitate the exercise with SMEs from first-line business functions. Review of scenarios may be carried out by risk management, internal audit and/or external parties. Scenarios should be reviewed

[29] FRC, September 2014, "The UK Corporate Governance Code" available online at https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf (accessed 25 January 2016). Section C.2.3 of this code requires annual reviews of control frameworks.

and approved by senior management and ideally the Board, not least to ensure that key exposures identified are brought to their attention.

The BCBS AMA guidelines (BCBS, 2011a, page 254)[30] sets out key elements of the scenario analysis process which the Working Party believes all firms should follow. These cover scenario analysis preparation, assessment, documentation and oversight.

8.1. Preparation

Preparation is essential for scenario analysis and involves identifying key SMEs, ensuring they are properly briefed on requirements, and providing supporting information to help them with the scenario assessment.

As wide a range as possible of SMEs with relevant experience should contribute to scenario analysis. When considering scenarios by risk type, there is a need to think widely about which functions could be affected by sub-types of a risk. Taking processing risks, e.g., a firm should consult not just customer service SMEs but also those involved in payroll processing and asset dealing.

Once SMEs have been identified, they need to be properly briefed on requirements. They should understand the importance of scenario analysis to capital modelling and financial strength, as well as the wider management of operational risks. Detailed instructions should be providing covering what impacts need to be considered and also what should not be considered (see sections 5.1 and 5.1.1. above). Where scenario analysis is carried out by risk type, the underlying (Level 3) sub-types should be supplied so SMEs understand what risks come under the category to be considered – a common failing in scenario analysis is where the same risk is considered under two separate categories, or where a material risk is missed because SMEs assume it is covered under a different category. Where scenario analysis is carried out by function, every effort should be made to identify potential risks faced by that function, going beyond what the function may have on its risk register. Supplying this information on risks to be considered helps ensure no material risks are omitted from scenario analysis.

SMEs should also be supplied with background material to help them with the exercise, including

- ILD, including gains and near misses;
- ELD – consideration should be given not just to losses from external loss databases such as ORX and ORIC, but also any other relevant examples outside financial services, e.g., recent theft of data from Target in the United States;
- details of current risks and issues;
- result of control assessments and KRI values; and
- strategy details which may affect risk profile, e.g., new products and channels which may affect conduct risks, or new systems which may affect processing errors.

[30] Also of note is the commentary on Guideline 19 – Operational Risk of the EIOPA Systems of Governance guidelines and in particular page 5.69 (see *EIOPA Final Report on Public Consultation No. 13/008 on the Proposal for Guidelines on the System of Governance* above).

8.2. Assessment

There are a number of ways scenario analysis can be conducted. Some conduct a series of 1:1 interview with SMEs, others carry out workshops with SMEs, while others elicit views through survey. A variation of the survey approach is the Delphi technique where follow-up surveys are issued based on survey responses until a consensus emerges. While more difficult to arrange and manage, workshops can lead to useful interaction between SMEs.

Whichever approach is adopted, a key challenge is to avoid biases in what is a subjective exercise. One such bias is the "anchoring" of scenarios on past experience. This extends not just to past events, but to the results of past scenario analysis, and there may be a bias towards scenarios already identified as opposed to new scenarios. SMEs should be encouraged to think of new risks that could crystallise. Another problem is that SMEs may be too focussed on future control failures and may not properly consider legacy failings which could emerge.

SMEs may also be reluctant to identify large losses for fear this would reflect negatively on them. This may be particularly true of losses that exceed minimum capital requirements such as Basel II TSA or Solvency II SF requirements for operational risk. Facilitators should ensure that the SMEs can speak freely without fear of recrimination, and that scenario analysis should focus on understanding the risks faced rather than producing any particular capital figure. This ties in with a broader risk culture of openness and willingness to acknowledge and learn from mistakes, which should be promoted by the Board and senior management.

Note some firms provide SMEs with estimates of the operational risk capital arising from their scenario outputs. This can help guard against ad hoc loss estimates and outputs giving rise to unfeasibly large capital figures. However, the Working Party is not convinced of the merits of this, as there is a risk that SMEs may "game" their estimates to produce capital figures they feel comfortable with, rather than assess potential losses in a neutral manner. It would probably be better to validate outputs against such capital estimates as part of the review and challenge of results.

There is an issue with the quality of ad hoc loss estimates and other parameters derived as part of the scenario process. Rather than trying to finalise figures as part of a workshop or interview, time should be built in to the scenario analysis process to firm up loss estimates, perhaps in consultation with Finance and Actuarial. This time can also be used for further investigation of issues raised as part of the scenario analysis. There may be a need for follow-up workshops, interviews, etc., which should be allowed for in planning the exercise.

As for ILD, scenario analysis impacts need to split out insurance and other recoveries from gross losses. There may be a problem of bias towards scenarios involving uninsured risks, away from insured risks which may be more significant in gross terms. Consideration should also be given to pension scheme risks and impacts.[31]

8.3. Documentation

It is essential that points raised during the assessment process are captured and documented. This should include not just the scenarios ultimately chosen but also those risks and scenarios considered

[31] Pension scheme risks and their impacts should also be considered.

but rejected. This can help demonstrate to regulators the breadth of coverage of the scenario analysis exercise.

Ideally, the scenario discussion would address all risks in a category/function and assess which are material before selecting a subset as the representative scenarios to be quantified. If this discussion were captured and documented, it would provide evidence that all risks have been considered as part of the scenario process.

Documentation should also capture the impacts by type and the rationale for frequency parameters and loss parameters chosen. Scenario analysis results should be collated in a standard template which can help ensure that no item is missed and aid comparison and validation of results. This should be updated as loss estimates are refined and issues identified are followed up, along with an audit trail of adjustments to results.

Finally, the minutes of the scenario workshops should also be kept, to show who was present and to demonstrate that there was effective challenge during the workshop.

8.4. Review, Challenge and Governance

Scenario analysis results will be inherently subjective so should be subject to extensive review and challenge. BCBS AMA guidelines suggest this review and challenge may be carried out by the third-line Internal Audit function and/or an external reviewer. This may be because of the role of the second-line risk management function in facilitating scenario analysis. However, the Working Party believes there may be a role for risk management to review and challenge scenario analysis provided those reviewing and challenging the results are sufficiently independent. Involving Risk Management in the review of operational risk scenario analysis results also helps to feed these results into emerging risk analysis, reverse stress testing and wider risk management.

Aside from independence, the other key attribute of the review function is knowledge of operational risks, which they should use to challenge whether all material risks have been considered. They should also consider whether the scenario has been properly categorised. Loss estimates and other parameters need to be challenged and validated, which may include estimating operational risk capital arising from scenario outputs as described in section 8.2 above, but which should consider other information sources, e.g., regulatory fines could be assessed against historic fines while market movements could be validated against economic capital models of market risk.

Having being through review and challenge, scenario results should be reviewed and approved by senior executives and ideally the Board or its risk committee. One approach would be to assign final responsibility for scenario results to the executive director responsible for the business area most closely aligned to managing category of risk, who would then be required to present to his peers and the Board.

Requiring senior management and the Board to endorse scenario analysis results in this way helps to ensure focus on the quality of results while also eliciting the perspective of those at the top of the organisation which can prove invaluable. It will also bring key operational risk exposures to their attention and may prompt consideration of mitigation strategies.

9. Maximum Loss Caps

Many firms apply a cap to the severity distribution of losses in their operational risk models.[32] This represents the worst case loss that may be incurred in a particular category.

It is often assessed as part of the scenario analysis process. However, it is important to note that the event which gives rise to the maximum loss may not be related to the scenario chosen. For instance, considering the damage to physical assets risk category, a London-based firm operating across multiple sites may base its scenario around a fire at one of its offices or perhaps a terrorist attack like the Bishopsgate bombing in 1993. However, the worst event in terms of severity could be a catastrophic storm surge breaching the Thames Barrier, which may have been rejected as too remote a scenario for operational risk modelling.[33] Whatever the scenario chosen in section 8, separate consideration needs to be given to the scenario which gives rise to the maximum loss.

The process for determining maximum loss should try to identify loss boundaries such as

- the total number of customers – including historic customers – who may be affected by an operational risk event, their account/policy values and hence the worst-case loss per customer;
- limits on fines that can be levied, e.g., breach of Competition Law could lead to a fine of up to 10% of turnover;
- the impact of time bars and the statute of limitations on the number of customers who can make a complaint against the firm;
- for employee relation risks, losses may be bounded by the number of employees (including past employees) and the maximum loss per employee which may be related to salary or bounded by statutory limits on awards; and
- impairment of assets – this may be capped by the value of particular asset classes.

These can help derive a maximum loss figure. It may also be useful for validation purposes to express maximum losses derived from consideration of scenarios as a percentage of customer or accounting totals, e.g., the loss under a worst-case mis-selling scenario could be expressed as a percentage of total policy/account values.

10. Allowances for Risk Mitigation

Allowances for insurance (e.g. against fire damage) and other risk mitigation will have a key impact on operational risk capital, but both Basel II and Solvency II limit credit taken for risk mitigation depending on the characteristics of the arrangement. Therefore risk mitigation details are an important set of inputs into operational risk models.

[32] In the United States, however, regulators are unlikely to approve such an approach. Also, in the United Kingdom, the FSA's "Operational Risk Standing Group" noted issues with loss caps (see the 13 February 2008 memo from Gerard-Paul Sampson of the FSA's Prudential Risk Division to the ORSG on Operational risk models, a copy of which is available online at http://www.fsa.gov.uk/static/pubs/international/op_risk08.pdf, page 13, accessed 25 January 2016).

[33] The Thames Barrier is supposed to have a 1-in-1,000 probability of being breached in any given year.

10.1. Insurance

As well as the amount of cover, which is a function of sum insured and policy excesses, there is also a need to consider

a. Term of policy and any corporate policy on rolling over cover – without the latter the benefit of cover may need to be pro-rated by outstanding term.

b. Counterparty default risk of the insurer and hence claim payment credit ratings and potential recoveries on default.

c. Gaps in cover, e.g., policy may cover fire damage but not damage from civil unrest, or policies which only cover claims made and not claims IBNR in the policy year.

d. Linked to (c), there may be ambiguity over whether a particular loss is covered and that the insurer may refuse to pay the claim.[34]

With regard to (c) and (d), in theory a firm could look to split frequency assessment into the frequency of insured and uninsured events and simulate recoveries accordingly. In practice, this may be too complex and either a subjective "haircut" may be applied or no credit allowed for insurance at all.

10.2. Other Risk Mitigation

Another source of recoveries relates to third-party indemnification, e.g., by outsourcers in respect of administration errors, but the modelling of such recoveries needs to consider

- the terms of the outsource agreement and what exactly can be recovered under the indemnity;
- any weaknesses in wording which could lead to dispute over indemnification;
- the financial strength of the outsourcer and whether they would be able to honour indemnities; and
- the process for identifying errors and recovering under indemnities – the greater the delays, the greater the exposure to outsourcer default and there may be time bars on indemnification, e.g., the outsourcer may only indemnify losses which have arisen in the past 5 years.

Operational risk modelling could also assume recoveries through legal action but consideration needs to be given to whether such action would be successful – a legal opinion would probably be required to support this – and whether the counterparty to the litigation would have the means to redress even if successful.

Lastly, insurance firms may model operational losses charged to the WPF and hence to policyholders. However, there is a need to consider whether losses charged to the WPF are consistent with its Principles and Practices of Financial Management (PPFM) and also with Treating Customers Fairly (TCF) principles and other FCA rules. Assumptions as to which losses could be charged to the WPF should be reviewed and approved by the With-Profit Actuary and the With-Profit Committee.

11. Correlation and Dependency Assumptions

Operational risks are generally modelled by individual (Level 2) category and then aggregated. The aggregation process will have a significant impact on operational risk requirements. The inputs

[34] For example, when Standard Life tried to claim on its Professional Indemnity (PI) policy in respect of a loss caused by defective product literature, its insurers initially refused, although Standard Life was ultimately successful in its claim. For details see Rahul Odedra's February 2012 article "Standard Life wins £100 million claim against PI insurers over Sterling fund", *Professional Adviser*, a copy of which is available online at http://www.professionaladviser.com/ifaonline/news/2142894/standard-life-wins-gbp100m-claim-pi-insurers-sterling-fund (accessed 25 January 2016).

required to the process will depend on the aggregation method chosen.[35] In terms of increasing complexity

a. Addition of individual category requirements with no allowance for correlation – no dependency assumption required but this is likely to significantly overstate operational risk requirements.
b. As (a) but with a "haircut" to reflect diversification – there is a need to assess the appropriate level of haircut having regard to the degree of diversification between operational risks.
c. Assumption of independence between requirements (i.e. aggregate equals the root of the sum of squares) – again no assumption is required but it is unlikely this would meet with regulatory approval as it is likely to understate capital requirements.
d. As (c) but with an addition to reflect dependencies between risks. Similar to (b) there is a need to assess the appropriate level of loading having regard to the degree of dependency between operational risks.
e. Correlation matrix – there is a need to set correlation assumptions between risks.
f. Copula aggregation – again there is a need to set correlation assumptions[36] between risks as well as make an assumption about dependency structure (e.g. Gaussian copula).
g. Bayesian networks (see section 13 below) and other causal approaches to operational risk modelling.

(b) and (d) will rely on expert judgement in setting the "haircut"/addition. This should go through the same process as other material expert judgements in the firm's modelling process. The following considers how correlation assumptions may be derived for the purposes of (e) and (f).

11.1. Correlations Derived from Data

Correlation assumptions could be derived for internal and ELD, e.g., by considering correlations between quarterly loss totals for each category (Cope & Antonini, 2008). However, loss data and hence empirical correlations may be driven mainly by low impact, high frequency losses. These may give a misleading picture of correlations at the tail.

For instance, there may be little correlation between low impact, high frequency losses under two categories (e.g. manual processing errors and card fraud) which may be correlated at the tail (e.g. weak IT system implementation leads to systemic processing errors and also exposes a firm to large-scale cyber theft). Alternatively, while there may be strong correlations between low impact, high frequency losses in two categories (e.g. weakness in customer service recruitment leads to manual processing errors and petty theft), there may be less connection between high impact, low frequency events (e.g. large-scale system processing errors and deliberate under-reserving).

Another issue with correlations derived from data is that even if there is a strong underlying correlation between two low frequency risks, the empirical correlation may still be low due to the infrequent occurrences of loss events. For instance, if we were to simulate five operational risks $\{X1, \ldots, X5\}$, each distributed binomially with $p = 0.1$ probability of a loss and assuming a Gaussian

[35] For more details on diversification methods and benefits, see, e.g., the Institute of Risk Management – Internal Model Industry Forum (2015).

[36] Including the type of correlation (linear/rank/etc.).

copula with a medium 50% correlation between variables, the empirical correlation between the number of losses would be ≈25%.

11.2. The Role of Expert Judgement

Given the limitations of correlations derived from data, the Working Party believes that expert judgement is essential to determine correlation assumptions. However it would probably be impractical to ask SMEs to identify correlations for each pair of risks. If one had 20 Level 2 risks, this would require 190 separate correlation assumptions which would be too much to ask for and difficult to validate. The resulting correlation matrix is also unlikely to satisfy the positive semi-definite property required to be valid.

To address this, one approach may be to group risks and assume a common correlation between groups of risks. For instance, splitting 20 Level 2 risks into four groups of five, we would need ten correlation assumptions within each group (40 in total) plus six correlation assumptions between groups, which may be more manageable. If one assumed a uniform correlation within groups the task of setting correlations becomes easier still.

Risks could be grouped by some common factor, for instance, by

- high-level risk type, e.g., Basel Level 1 categories;
- type of risk, e.g., people, process, system or external event; and
- function, e.g., conduct risks mapped to sales, processing risks to operations, people-related risks to Human Resources (HR), etc.

Given the heterogeneity of operational risk categories, however, it is likely there will be a loss of granularity, e.g., two sub-types of risks in two otherwise uncorrelated groups could be strongly correlated. (It should be noted that this applies not just to groups but also within Level 2 categories given the broad range of sub-risks in each category.)

Another approach to determining correlation may be to consider the results of broader stress and scenario testing work, e.g., flu pandemic scenario testing could highlight common dependencies between processing risks (due to backlogs arising) and mis-selling (due to falling markets giving rise to customer losses). This could also help with setting correlations between operational risks and market and other non-operational risks.

Whichever approach is adopted, expert judgements on correlation assumptions should be subject to rigorous review and challenge given their subjectivity. Key correlation assumptions should be identified through sensitivity analysis which should be subject to particular scrutiny. As for scenario analysis, this review should be independent and performed by those with an understanding of operational risks and how these interlink.

12. Allocating Operational Risk Capital by Legal Entity

Often scenario analysis will be performed at a higher level than legal entity, and similarly loss data may be combined across entities for the purposes of modelling. The resulting aggregate capital requirement will then need to be allocated back to individual entities. For with-profit insurers, there would also be a need to allocate operational risk capital between the WPF and other funds.

In determining the split of aggregate requirement by legal entity, the following should be considered:

a. Often there will be a split between banking and insurance subsidiaries and service companies providing staff and other resource to these, governed by a service-level agreement (SLA) between these entities. This should be reviewed to see if there are any implications for allocation, e.g., the SLA may preclude the servicing company from charging back losses associated with employee relation risks, so this element of operational risk capital should not be allocated to the bank or insurance subsidiary.
b. Some risks may rest at a group, holding-company level and may not be allocated back to subsidiary entities, e.g., financial reporting errors relating to consolidation.
c. However, in this example, even if errors at group are the key driver of financial reporting operational, it may still be appropriate to hold operational risk capital for financial reporting errors at a legal entity level, e.g., errors in PRA returns for that entity.
d. By the same token, some scenarios may be driven by individual legal entity exposures which may not be relevant to other entities. For instance, the key conduct risk exposure may relate to segregation of client funds at a wrap platform subsidiary, but this may not be relevant to an annuity subsidiary. The latter may still have some residual conduct risks so there may still be a case for allocating some operational risk capital to this subsidiary to address this risk.

Both (c) and (d) highlight a weakness of carrying out scenario analysis at a level higher than legal entity – risks which are material at an individual entity level may be less material overall and may get missed. As far as possible, risks and scenarios identified as part of an aggregate exercise should be retained as even if these are not used as a basis for quantification at an aggregate level, they may still be relevant for individual entities and can help inform the allocation.

Finally, allocation of operational risk capital to the WPF should be consistent with PPFM and TCF. The Working Party believes that the allocation of operational risk capital to a WPF fund should be reviewed and approved by the fund's With-Profit Actuary and/or With-Profit Committee.

13. Bayesian Networks

A more sophisticated approach to modelling operational risks than traditional approaches based on loss data and/or scenario analysis, Bayesian networks seek to derive a combined probability distribution of operational losses from all types, having regard to underlying causal variables (e.g. staff turnover affecting processing errors and internal fraud losses). It thus addresses the modelling dependencies explicitly without the need to consider correlation assumptions.

Parameterising Bayesian network models is beyond the scope of this paper,[37] but the Working Party would make two observations on inputs to these models. First, Bayesian networks will be underpinned by assumptions of probability (e.g. of a rise in the staff turnover rate) and conditional probability (probability of process error given a rise in staff turnover). Many of these probabilities can be determined

[37] For a fuller description of Bayesian networks and other advanced Operational Risk modelling techniques, see Milliman's (Corrigan, J., Luraschi, P. & Cantle, N.) February 2013 paper *Operational Risk Modelling Framework* available online at http://uk.milliman.com/uploadedFiles/insight/life-published/operational-risk-modelling-framework.pdf (accessed 25 January 2016); and the KPMG/Canadian Institute of Actuaries' November 2014 paper *Research Paper on Operational Risk* available online at http://www.cia-ica.ca/docs/default-source/2014/214118e.pdf (accessed 25 January 2016).

from empirical data, but others may be based on expert judgement or a combination of the two. There needs to be a process for identifying the key expert judgements in terms of the sensitivity of operational risk capital values to changes in parameters and for reviewing and challenging these in a similar fashion to scenario analysis. Going forward, there should be a process for revising prior assumptions in light of emerging experience, allowing a revised posterior distribution.

Second, while the Bayesian network can reflect both the current risk profile and state of controls and future changes in these over time, there may be a case for conducting scenario analysis in addition to act as a check on Bayesian network model results and whether it addresses the full range of risks.

14. Conclusion

Hopefully, this paper will have given the reader an idea of the issues affecting inputs to operational risk models and sets out good practice in this area to address these issues.

In terms of key conclusions, based on our review of literature and consideration of the limitations of historic loss data, the Working Party believes that scenario analysis is an essential supplement to loss data in order to properly model operational risks.

Similarly, we believe expert judgement is necessary to determine correlation assumptions given the limitations of correlations derived from historic data. Reliance on scenario analysis and expert judgements for correlations will introduce significant subjectivity into operational risk which needs to be controlled by robust and independent review and challenge.

Inputs to operational risk models need to comply with regulatory guidance. In particular, the BCBS AMA guidelines set out detailed requirements around loss data collection and scenario analysis which the Working Party believe should also be considered by non-bank firms. Like the BCBS and EIOPA, we believe firms should capture gains and "near misses" as well as operational risk losses. Finally, the Working Party also believes that firms should try to capture information on the operational risks and losses of pension schemes, asset managers, outsourcers and other third parties to which it may be exposed, even if these losses are indemnified.

References

Abdymomunov, A., Blei, S. & Ergashev, B. (2015). Integrating stress scenarios into risk quantification models. *Journal of Financial Services Research*, **47**(1), 57–79.

Barakat, A., Chernobai, A. & Wahrenburg, M. (2014). Information asymmetry around operational risk announcements. *Journal of Banking and Finance*, **48**(11), 152–179.

Basel Committee on Banking Supervision (BCBS) (2006a). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version: Part 2, Section V*, June. BCBS, Basel, pp. 644–683, available at http://www.bis.org/publ/bcbs128b.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2006b). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version, Annex 9*, June. BCBS, available at http://www.bis.org/publ/bcbs128d.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2009a). *Results from the 2008 Loss Data Collection Exercise for Operational Risk*, July. BCBS, available at http://www.bis.org/publ/bcbs160a.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2009b). *Observed Range of Practice in Key Elements of Advanced Management Approaches(AMA)*, July. BCBS, available at http://www.bis.org/publ/bcbs160b.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2011a). *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches (BCBS196)*, June. BCBS, available at http://www.bis.org/publ/bcbs196.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2011b). *Principles for the Sound Management of Operational Risk*. BCBS, available at http://www.bis.org/publ/bcbs195.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2014a). *Review of the Principles of the Sound Management of Operational Risk*. BCBS, available at http://www.bis.org/publ/bcbs292.pdf (accessed 25 January 2016).

Basel Committee on Banking Supervision (BCBS) (2014b). *Operational Risk – Revisions to the Simpler Approaches*. BCBS, available at http://www.bis.org/publ/bcbs291.htm (accessed 25 January 2016).

Berger, W. (2014). *A More Beautiful Question: The Power of Inquiry to Spark Breakthrough Ideas*, New York, Bloomsbury.

Cope, E. & Antonini, G. (2008). Observed correlations and dependencies among operational losses in the ORX Consortium Database (in collaboration with the ORX Analytics Working Group), available at http://www.orx.org/Lists/PublicDocuments/Observed_Correlations_and_Dependencies_Among_Op_Losses_in_the_ORX_Consortium_Database27November2008.pdf (accessed 25 January 2016).

Cope, E.W. (2012). Combining scenario analysis with loss data in operational risk quantification. *Journal of Operational Risk*, **7**(1), 39–56.

de Jongh, P., de Wet, T., Raubenheimer, H. & Venter, J. (2015). Combining scenario and historical data in the loss distribution approach: a new procedure that incorporates measures of agreement between scenarios and historical data. *Journal of Operational Risk*, **10**(1), 45–76.

Dutta, K.K. & Babbel, D.F. (2014). Scenario analysis in the measurement of operational risk capital: a change of measure approach. *Journal of Risk and Insurance*, **81**(2), 303–334.

Ergashev, B.A. (2012). A theoretical framework for incorporating scenarios into operational risk modelling. *Journal of Financial Services Research*, **41**(3), 145–161.

Financial Reporting Council (FRC) (n.d.). Technical Actuarial Standards, available at https://www.frc.org.uk/Our-Work/Codes-Standards/Actuarial-Policy/Technical-Actuarial-Standards.aspx (accessed 25 January 2016).

Financial Services Authority (FSA) (2005). *ICAS – One Year On*. FSA, London, pp. 14–29, available at http://www.fsa.gov.uk/static/pubs/other/isb_icas.pdf (accessed 25 January 2016).

Financial Services Authority (FSA) (2006). *Risk Management in Insurers*. FSA, pp. 62–63, available at http://www.fsa.gov.uk/pubs/other/isb_risk.pdf (accessed 25 January 2016).

Financial Services Authority (FSA) (2007). *ICAS – Lessons Learned and Looking Ahead to Solvency II*. FSA, available at http://www.fsa.gov.uk/pubs/other/icas_isb.pdf (accessed 25 January 2016).

Finke, G., Singh, M. & Rachev, S.T. (2010). Operational risk quantification: a risk flow approach. *Journal of Operational Risk*, **5**(4), 65–89.

Ieva, F., Paganoni, A.M. & Ziller, S. (2013). Operational risk management – a statistical perspective. *Far East Journal of Mathematical Sciences*, 123–138.

Institute of Risk Management – Internal Model Industry Forum (2015). *Diversification Benefit: Understanding its Drivers and Building Trust in the Numbers*. Institute of Risk Management – Internal Model Industry Forum, London, available at https://www.theirm.org/media/1454273/IRM_Diversification-Booklet_hi-res_web-Final.pdf (accessed 5 February 2016).

Jiménez-Rodríguez, E.J., Feria-Domínguez, J.M. & Martín-Marín, J.L. (2008). Scenario analysis for modelling operational losses in the absence of data: the Spanish Bank in perspective. *Journal of Financial Management and Analysis*, **21**(2), 1–10.

Kahane, A. (n.d.). The Mont Fleur scenarios: what will South Africa be like in the year 2002?, available at http://www.generonconsulting.com/publications/papers/pdfs/Mont%20Fleur.pdf (accessed 25 January 2016).

Kelliher, P., Wilmot, D., Vij, J. & Klumpes, P. (2013). Common risk classification system for the Actuarial Profession. *British Actuarial Journal*, **18**(1), 91–162.

Moosa, I. & Li, L. (2013). An operational risk profile: the experience of British firms. *Applied Economics*, **45**(16–18), 2491–2500.

Seth Young, Ernst and Young (2010). Quantifying operational risk – presented at CAS Seminar on Reinsurance, available at http://www.casact.org/education/reinsure/2010/handouts/cs14-patel.pdf (accessed 25 January 2016).

Shell International (n.d.). Energy needs, choices and possibilities – scenarios to 2050, available at http://s06.static-shell.com/content/dam/shell-new/local/corporate/corporate/downloads/pdf/scenarios-energy-needs-choices-and-possibilities.pdf and http://www.shell.com/global/future-energy/scenarios/previous.html (accessed 25 January 2016).

Torre-Enciso, M.I.M. & Barros, R.H. (2013). Operational risk management for insurers. *International Business Research*, **6**(1), 1–11.

Towers Perrin & OpRisk Advisory based on sponsorship from the Joint Risk Management Section of the Society of Actuaries, the Canadian Institute of Actuaries and the Casualty Actuarial Society (2009). *A New Approach for Managing Operational Risk – Addressing the Issues Underlying the 2008 Global Financial Crisis*, available at https://www.casact.org/cms/files/research-new-approach_1.pdf (accessed 25 January 2016).

Appendix A: Literature Review

The Working Party reviewed a number of papers on the topics of operational risk and scenario analysis. These were split into (a) those of interest with regard to operational risk inputs, (b) other operational risk papers and (c) other scenario analysis papers.

A.1. Papers of Interest with Regard to Operational Risk Inputs

Table A1.

Title, Authors and Source	Key Points
Paper: "Operational risk management – a statistical perspective" *Authors*: Ieva, F., Paganoni, A.M. & Ziller, S. *Source*: *Far East Journal of Mathematical Sciences*, 2013, **2013** (Ieva *et al*., 2013)	This article presents a statistical model for operational risk management The authors distinguish different types of operational event, they model the probability of event occurrence (the frequency distribution) and the economic impact of the single event (the severity distribution), and then the aggregated distribution is obtained through convolution of frequency and severity, for each event type The main problem is the estimation of parameters of the severity distribution above a suitable threshold that they consider as an unknown parameter to be estimated as well An application to a case study is also presented
Paper: "A theoretical framework for incorporating scenarios into operational risk modelling" *Author*: Ergashev, B.A. *Source*: *Journal of Financial Services Research*, 2012, **41** (3), 145–161 (Ergashev, 2012)	The paper introduced a framework that incorporates scenario analysis into operational risk modelling The basis for the framework is the idea that only worst-case scenarios contain valuable information about the tail behaviour of operational losses In addition, worst-case scenarios introduce a natural order among scenarios that makes possible a comparison of the ordered scenario losses with the corresponding quantiles of the severity distribution that research derives from historical losses Worst-case scenarios contain information that enters the quantification process in the form of lower bound constraints on the specific quantiles of the severity distribution The framework gives rise to several alternative approaches to incorporating scenarios
Paper: "Scenario analysis in the measurement of operational risk capital: a change of measure approach" *Authors*: Dutta, K.K. & Babbel, D.F. *Source*: *Journal of Risk and Insurance*, 2014, **81** (2) (Dutta & Babbel, 2014)	Operational risk is gaining the same importance as market and credit risk in the capital calculation Although scenario analysis is an important tool for financial risk measurement, its use in the measurement of operational risk capital has been arbitrary and often inaccurate The paper proposed a method that combines scenario analysis with historical loss data Using the change of measure approach, the paper evaluated the impact of each scenario on the total estimate of operational risk capital

	The method can be used in stress testing, what-if assessment for scenario analysis and loss given default estimates used in credit evaluations
Paper: "Combining scenario analysis with loss data in operational risk quantification" *Author*: Cope, E.W. *Source*: *Journal of Operational Risk*, 2012, **7** (1) (Cope, 2012)	A method for integrating information obtained from loss data and scenario analysis is presented in this paper The stochastic process that generates losses within a unit of measure is modelled as a superposition of various sub-processes that characterise individual "loss-generating mechanisms" (LGMs) An end-to-end method is provided for identifying LGMs, performing scenario analysis and combining the outcomes with relevant historical loss data to compute an aggregate loss distribution for the unit of measure It is shown how the preferred output of scenario analysis can be straightforwardly encoded into a non-parametric Bayesian framework for integration with historical loss data
Paper: "Integrating stress scenarios into risk quantification models" *Authors*: Abdymomunov, A., Blei, S. & Ergashev, B. *Source*: *Journal of Financial Services Research*, 2015, **47** (1) (Abdymomunov *et al*., 2015)	The study enhanced the method of integrating scenarios into risk models In particular, the study provided additional theoretical insights of the method with focus on stress testing value-at-risk models The study extended the application of the method, which is originally proposed for scenario analysis in the operational risk context, to market and credit risks The paper provided detailed application guidance of the method for market, credit and operational risks The two key features of the method are as follows: (a) it ensures that a stressed model produces a higher risk estimate than the model based on historical data only and (b) it does not require assumptions on stressed loss distributions, thereby simplifying the scenario-generation process
Paper: "Combining scenario and historical data in the loss distribution approach: a new procedure that incorporates measures of agreement between scenarios and historical data" *Authors*: de Jongh, P., de Wet, T., Raubenheimer, H. & Venter, J. *Source*: *Journal of Operational Risk*, 2015, **10** (1) (de Jongh *et al*., 2015)	Many banks use the loss distribution approach in their advanced measurement models to estimate regulatory or economic capital. This boils down to estimating the 99.9% value at risk of the aggregate loss distribution and is difficult to do accurately Also, it is well known that the accuracy with which the tail of the loss severity distribution is estimated is the most important driver in determining a reasonable estimate of regulatory capital To this end, banks use internal data and external data (jointly referred to as historical data) as well as scenario assessments in their endeavour to improve the accuracy with which they estimate the severity distribution This paper proposed a simple new method whereby the severity distribution may be estimated using both historical data and experts' scenario assessments

Table A1. *(Continued)*

Title, Authors and Source	Key Points
	The way in which historical data and scenario assessments are integrated incorporates measures of agreement between these data sources, which can be used to evaluate the quality of both In particular, the study showed that the procedure has definite advantages over traditional methods where the severity distribution is modelled and fitted separately for the body and tail parts, with the body part based only on historical data and the tail part on scenario assessments
Paper: "Scenario analysis for modelling operational losses in the absence of data: the Spanish Bank in perspective" *Authors*: Jiménez-Rodríguez, E.J., Feria-Domínguez, J.M. & Martín-Marín, J.L. *Source*: *Journal of Financial Management and Analysis*, 2008, **21** (2) (Jiménez-Rodríguez *et al*., 2008)	Basel II has encouraged the Spanish banking sector to evolve sophisticated techniques for managing operational risk more effectively The study conducted a scenario analysis combined with the loss distribution approaches to calculate the capital charge for operational risk, and more specifically, for the internal fraud event type The scenario analysis is an essential technique when lacking data in order to complete the Internal Operational Loss Database (IOLD) The paper applied this analysis in the case of the IOLD provided by a Spanish saving bank As there is only one observation recorded due to the internal fraud and, being aware of the under-reporting phenomenon, the authors designed two hypothetical scenarios to offset the missing data Furthermore, the study developed a stress testing to calibrate the potential impact on capital at risk due to mechanical changes in both scale and shape parameters of the severity distribution As a result, the study found a positive relationship between the degree of asymmetry and kurtosis that characterised the loss distribution and the capital consumption
Paper: *A New Approach for Managing Operational Risk – Addressing the Issues Underlying the 2008 Global Financial Crisis* *Authors*: Towers Perrin & OpRisk Advisory based on sponsorship from the Joint Risk Management Section of the Society of Actuaries, the Canadian Institute of Actuaries and the Casualty Actuarial Society, 2009 *Source*: https://www.casact.org/cms/files/research-new-approach_1.pdf (Towers Perrin & OpRisk Advisory, 2009)	The paper begins with the assertion that operational risk has either caused or exacerbated nearly every catastrophic Financial Institution loss that has occurred during the past 20 years, highlighting that the 2008 financial crisis was largely caused by a series of extremely large operational failures. Given its contribution to past losses, the paper then explores whether a better approach to managing operational risk exists Within the paper there is a focus on principal–agent risk, with the American Insurance Group event during the 2008 financial crisis cited as an example of this. Principal–agent

	risk refers to situations where the interests of the company and employees are misaligned allowing situations where individuals then pursue activities that are in their self-interest (personally or otherwise) and not in the interests of the company The paper notes that traditional audit-based approaches have been relied upon to date by the financial sector and that virtually all major global accounting firms recommend the traditional approach. While these traditional approaches have many useful features, including structure, governance and an intuitive approach to risk identification and assessment, there are also drawbacks including inconsistency with how the actuarial and risk management functions approach risk The paper notes that traditional methods can easily become over-controlled particularly in low risk areas while significantly higher risk areas remain under-controlled. The paper then offers a new top-down approach which focusses first on major risks and drills down only in those areas where more granularity is required. Importantly, it allows practitioners to tailor their approach to those areas requiring most attention, contributing to the provision of cost-effective risk management processes The authors do however recommend maintaining some of the features of traditional operational risk management ("ORM"), enhancing them with the use of more modern top-down ORM techniques. The combination not only offers improved risk management effectiveness but can also significantly reduce cost. The aim of modern ORM techniques is to provide key decision makers with the ability to measure both the expected and unexpected loss within the context of both the existing control environment and the risk tolerance standards of the stakeholders. It assists decision makers in developing/acquiring tools and methodologies to assess and monitor internal control quality on a periodic basis Section 8 of the paper provides the detail on how to calculate expected and unexpected operational losses, in terms of modelling frequency and severity and also how to combine internal and external data within the process
Paper: "Quantifying operational risk – presented at CAS Seminar on Reinsurance" *Author*: Seth Young, Ernst and Young) *Source*: http://www.casact.org/education/reinsure/2010/handouts/cs14-patel.pdf (Seth Young, Ernst and Young, 2010)	The paper provides a high-level overview of operational risk and includes sections covering operational risk frameworks, methodologies for quantifying operational risk and risk mitigation The paper starts with the Basel II and Solvency II definition of operational risk and argues that for Property & Casualty Insurance companies it is one of the least managed risk within their overall universe of risks The paper provides some of the motivations for an operational risk framework, including raising awareness with senior management, providing meaningful risk mitigation and overall leading to an improved control environment. However, it

Table A1. *(Continued)*

Title, Authors and Source	Key Points
	suggests cost–benefit analysis should be investigated before any framework is implemented and that a quick top–down approach may be of more value to the organisation The paper outlines the components of successful operational risk frameworks arguing for greater consistency, transparency and clarity on which risks are being managed. The taxonomy used should be mutually exclusive (i.e. no double counting), exhaustive (i.e. no gaps in the framework) and yet manageable for the business. It is noted that operational risk permeates all aspects of the risk universe and that it is sometimes difficult to isolate the pure operational risk aspects The paper outlines two methodologies used in practice – the loss distribution approach and a scenario approach – and gives the advantages and disadvantages of each method. It suggests risk assessments should be done on both an inherent and residual risk basis, allowing the value of the control framework to be assessed. Whichever method is used there is a choice of internal and external data to assist the parameterisation, noting that care is needed with both sets of data in terms of applicability to the business prospectively. Potential correlation between operational risks also needs to be incorporated in the methodology In terms of risk mitigation the paper provides a structure for risk and control assessments, highlighting the culture of the organisation as important in successful implementation and also providing suggestions on operational risk reporting. The overall conclusion in the paper is that the thinking in the area of operational risk is undeveloped* but that regulatory reform (particularly Solvency II) will facilitate a more robust quantification and assessment of operational risk

*This was written in 2010 and thinking will have developed since then.

A.2. Other Operational Risk Papers

Table A2.

Title, Authors and Source	Key Points
Paper: "An operational risk profile: the experience of British firms" *Authors*: Moosa, I. & Li, L. *Source*: *Applied Economics*, 2013, **45** (16–18), 2491–2500 (Moosa & Li, 2013)	This study provides an analysis of 163 operational loss events experienced by a variety of British firms over the period 1999–2008. In all, ten different hypotheses are tested to examine the distribution of loss severity and frequency with respect to business line, event type and corporate entity type The hypotheses were tested on the relation between loss severity and the decline in the market value of the announcing firm and whether or not the decline in market value is greater if the loss results from internal fraud Inter alia the results indicate that the decline in market value bears no stable relation to the loss amount
Paper: "Operational risk management for insurers" *Authors*: Torre-Enciso, M.I.M. & Barros, R.H. *Source*: *International Business Research*, 2013, **6** (1) (Torre-Enciso & Barros, 2013)	The new European regulation, Solvency II, will inexorably increase the need of an effective management of operational risks and the development and implementation of structured methodologies for its analysis. The paper reviewed the classical technique of modelling, value at risk, and other methodologies for the analysis and quantification of operational risk for insurers
Paper: "Operational risk quantification: a risk flow approach" *Authors*: Finke, G., Singh, M. & Rachev, S.T. *Source*: *Journal of Operational Risk*, 2010, **5** (4) (Finke *et al.*, 2010)	The study discussed ways of quantifying operational risk with a specific focus on manufacturing companies In line with interpretations that depict the operations of a company using material, financial and information flows, the study extend the idea of overlaying the three flows with risk flow to assess operational risk The application of the risk flow concept is demonstrated by discussing a case study with a consumer goods company The model was implemented in six phases using discrete-event and Monte Carlo simulation techniques Results from the simulation are evaluated to show how specific parameter changes affect the level of operational risk exposure for this company Inventory as a means of risk mitigation in the network is discussed and results are presented

Table A3.

Title, Authors and Source	Key Points
Paper: "Information asymmetry around operational risk announcements" *Authors*: Barakat, A., Chernobai, A. & Wahrenburg, M. *Source*: *Journal of Banking and Finance*, **48** (Barakat *et al.*, 2014)	Operational risk incidences are likely to increase the degree of information asymmetry between firms and investors The article analysed operational risk disclosures by US financial firms during 1995–2009 and their impact on different measures of information asymmetry in the firms' equity markets Effective spreads and the price impact of trades are shown to increase around the first announcements of such events and to revert after the announcement of their settlement. This is especially pronounced for internal fraud and business practices-related events Market makers respond to higher information risk around the first press cutting date by increasing the quoted depth to accommodate an increase in trading volumes The degree of information asymmetry around operational risk events may be influenced by the bank's risk management function and the bank's governance structure The research found that information asymmetry increases more strongly after events' first announcements when firms have weaker governance structures, lower board independence ratios, lower equity incentives of executive directors and lower levels of institutional ownership In contrast, the firms' risk management function has little to no impact on information asymmetry. The authors interpreted this as evidence that the risk management function is primarily driven by regulatory compliance needs The results of this study contribute to the understanding of information asymmetry around operational risk announcements The results help to shed light on the role that regulation and corporate governance can play in order to establish effective disclosure practices and to promote a liquid and transparent securities market

A.4. Scenario Analysis Papers

Table A4.

Title, Authors and Source	Key Points
Paper: "The Mont Fleur scenarios: what will South Africa be like in the year 2002?" *Author*: Kahane, A. *Source*: http://www.generonconsulting.com/publications/papers/pdfs/Mont%20Fleur.pdf (Kahane, n.d.)	This describes scenarios developed during the South Africa political crisis which later saw Nelson Mandela take power and is an example of a scenario planning and selection process when change is expected, but the direction of change is not known The work included thinking of specific action events that might happen and then thinking through their repercussions. Each specific action might be a branch in a tree of possible outcomes. Repercussions and downstream actions which had their own effects would cause a new branch After articulating several branches and sub branches, the process stepped back and three representative scenarios were chosen (strong resistance to change, strong acceptance and a muddy middle). These were then exposed to wider input by diverse individuals. The future under three options was then articulated
Paper: "Energy needs, choices and possibilities – scenarios to 2050" *Author*: Shell International *Source*: http://s06.static-shell.com/content/dam/shell-new/local/corporate/corporate/downloads/pdf/scenarios-energy-needs-choices-and-possibilities.pdf http://www.shell.com/global/future-energy/scenarios/previous.html (Shell International, n.d.)	Shell wanted to understand the long-term future where technology, supply, demand and resources used are changing They took a very long view approach at the past to see how wood, coal, oil, gas, nuclear, solar, etc. played out in their life cycles and how demand, supply, technology, etc. affected their use They identified that a few energy sources might be used in the long-term future and used the history and current circumstances to guide them to selecting reasonable scenarios Besides learning about behaviours and factors which shape the use and supply of the resource over time, they learnt about where the unexpected arises from and how that can change their business. The scenarios then factored in surprises which might occur compared with central estimates Transitions and interactions were important to the approach. For operational risk, this seems relevant when political, economic, social, technological, legal and environmental factors are changing and a complex effect is expected to challenge the business

Table A5.

Title, Authors and Source	Key Points
Paper: *A More Beautiful Question: The Power of Inquiry to Spark Breakthrough Ideas* *Author*: Berger, W. *Source*: http://www.amazon.co.uk/More-Beautiful-Question-Inquiry-Breakthrough/dp/1620401452/ref=sr_1_1?ie=UTF8&qid=1431896718&sr=8-1&keywords=Ask+beautiful+questions (Berger, 2014)	Scenarios rely on good questions so understanding what makes good questions, and people's responses to these, is very important. This paper addresses these topics This book outlines 44 key questions that can help those involved in scenario analysis not get lost in details that perpetuate the past There are various themes throughout the book: how to challenge the status quo; the truth that questions are often more important than answers; psychological aspects of how people respond to the questioning process; and the importance of stepping back and asking why?

Appendix B: FRC and Actuarial Profession Requirements

FRC requirements can be split into generic and specific TASs. Note that the FRC is likely to consult on these over 2016, having previously consulted on generic standards over Q4 2014/Q1 2015.[38]

B.1. Generic TASs

At present there are three generic standards covering data, modelling and reporting. As part of the 2014/2015 consultation, it was proposed that these be replaced by a revised standard: Technical Actuarial Standard 100: Principles for Actuarial Work ("TAS 100"). However, implementation of this revised standard has been deferred to coincide with revisions to specific standards.

B.1.1. TAS D: data

This sets out requirements for operational risk data. Amongst other things, this standard requires that

- an assessment of data requirements should be made;
- all data definitions should be documented;
- data validation should be carried out; and
- judgements on type of data and adjustments to the data should be justified.

B.1.2. TAS M: modelling

This sets out requirements for operational risk models. C.2.4 lists potential uses of models which fall under this standard and estimating the capital requirements of an insurer is given as an example.

[38] FRC, "Consultation on a new framework for Technical Actuarial Standards" available online at https://www.frc.org.uk/Our-Work/Codes-Standards/Actuarial-Policy/Recent-Consultations.aspx (accessed 25 January 2016).

In summary

- judgements and methods used need to be justified;
- models must be fit for purpose and parsimonious, i.e., models should be no more complex than justified; and
- implementations (same outputs from identical inputs) and realisations (same outputs each time it is run) should be reproducible.

There are also requirements around documentation, data and assumptions. In particular, documentation is required to justify the relevance of data for the model including the approach for grouped data.

B.1.3. TAS R: reporting actuarial information

The focus of this TAS is on achieving a reliability objective through transparency, completeness and comprehensibility. This could pose a challenge due to the specialist nature of the work and complexity of ideas being considered. Of direct relevance is the requirement to describe each material risk and the approach taken for each one, as well as explanation of the meanings of probabilities presented and nature of statistics upon which they are based.

B.2. Specific TASs

As for generic standards, specific TASs will be reviewed over 2016.

B.2.1. Insurance TAS

Modelling operational losses/assessing operational risk capital is likely to be inside scope for section C.1.7 on regulatory reporting but also potentially sections C.1.12 (pricing), C.1.16 (insurance transformation) and C.19 (embedded values) where relevant.

The most relevant requirements relate to justification of approach taken/judgements made, assumptions basis and explanation of intra period changes in methods/assumptions, justification of approach for probability distributions used and co-dependencies, and the requirement to show a neutral estimate (best estimate) and explanation of any prudence.

B.2.2. Pensions TAS

If operational risk is modelled as part of work to support decisions on contribution requirements, benefit levels, funding assessments, etc. then it is within scope of this TAS. However, International Financial Reporting Standard (IFRS) (e.g. IAS19) currently cover defined benefit (DB) valuations for financial reporting and transfer purposes and operational risk is not included. A notable feature of this TAS is the requirement to explicitly capture/consider the impact of legislative uncertainty.

B.2.3. Other specific TASs

There are two other specific TASs. The Transformation TAS relates to the transfer or modification of liabilities for pension schemes and insurers. This is more focussed on beneficiaries but to the extent operational risk is modelled as part of the assessment of the transformation then this standard would be relevant.

The Funeral Plans TAS relates to funeral plans. If operational risk modelling is carried out within actuarial work on funeral plans then it would be within scope. The requirements are similar to Insurance TAS.

B.3. Other Actuarial Professional Standards

As well as standards prescribed by the FRC, the IFoA may also issue standards which actuaries may be expected to comply with in modelling operational risk.

For instance, in July 2015, the IFoA launched its APS 2X – Review of Actuarial Work standard. This standard applies to modelling operational risk capital and requires work review which may include independent peer review. Section 1.3 lists the relevant circumstances for assessing the level of review required. Section 1.3.1 implies independent peer review where modelling op risk is difficult and complex – which would be in most circumstances. The peer need not be an actuary.

In general, actuaries are expected to adhere to the Actuaries Code and its key principles of integrity, competence and care, compliance, communication and impartiality. These are important in modelling operational risk where inputs can be subjective, models sensitive to assumptions made and where results may be used for regulatory purposes.