Actuaries and Operational Risk Management
4 April 2019 – DRAFT

AAE RMC Workstream Members

Malcolm Kemp (Chair): malcolm.kemp@nematrian.com
Christoph Krischanitz: christoph.krischanitz@arithmetica.at
Daphné de Leval : ddeleval@deloitte.com
Eddy Van den Borre: eddy.vandenborre@aginsurance.be

Aims

(a) To prepare a paper, capable of targeting EU institutions, for promoting actuarial involvement in operational risk management
(b) To prepare a paper or presentation at ECA 2019 covering this topic, a draft of which we would aim to present to AAE RMC in April 2019

Abstract

[To be completed]

Keywords: Operational risk, loss distribution approach

1. Introduction

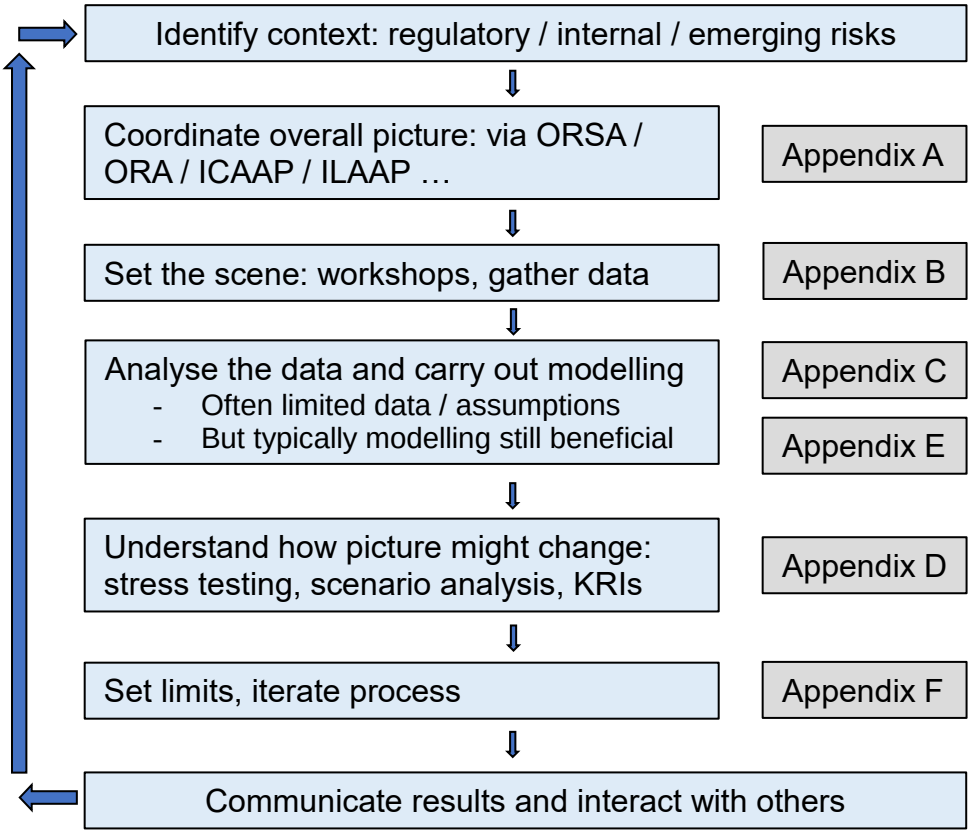
1.1 The purpose of this paper is to survey skills and techniques that actuaries currently bring to the field of operational risk management and how these might develop further in the future. It is the authors' belief that actuarial techniques and training and the professional ethos of actuaries makes actuaries with suitable industry experience well-placed to assist in this area.

1.2 The paper has three main sections. In **Section 2** we set out the disciplines and techniques that are (or could be) used in operational risk management (and likely near-term trends in these disciplines). We illustrate these by reference to those most applicable to insurance companies, thus in effect articulating the roles, responsibilities and skill-sets that might apply to an individual operational risk manager for such an organisation. **Section 3** brings out the merits of multi-disciplinary implementation of these activities but also highlights how individuals with actuarial skill-sets and expertise are particularly well suited to assist in several of the targeted discipline areas. [**Section 4** broadens the discussion to other industry and economic sectors, drawing out analogies relevant not just to (or from) other parts of the financial sector but covering the broader economy and society more generally].

1.3 The paper also includes a range of **Appendices** on specific topics that illustrate some of the skills and techniques covered earlier in the paper. These include Appendices that describe insurer Own Risk and Solvency Assessments (ORSA) and corresponding pension fund Own Risk Assessment (ORA) (Appendix A), how best to facilitate operational risk workshops and other ways of capturing the wisdom of experts (Appendix B), the loss distribution approach (LDA) and other approaches to quantifying operational risk (Appendix C), stress testing and scenario analysis (Appendix D), some thoughts on how best to cope with limited data (Appendix E) and setting operational risk appetite, limits and key risk indicator (KRI) identification (Appendix F). The aim is to cover at least to some degree many of the roles

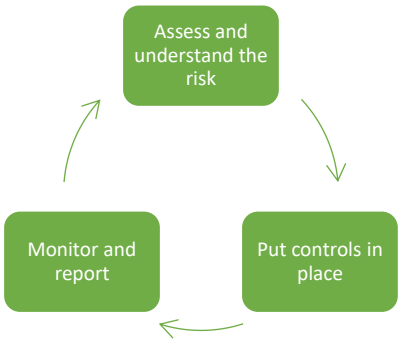
that those working in operational risk are likely to get involved with, see Figure 1[1], with a bias towards those activities where actuaries may be able to add greatest value.

Figure 1: Schematic of the main roles of an operational risk manager



1.4 Actuaries working in operational risk management will also typically contribute to implementing appropriate controls and monitoring and reporting on them, see Figure 2. This paper does not cover these aspects of operational risk management in detail, as they are well covered in standard texts such as Lam (2014).

Figure 2: the Operational Risk control cycle



2. Operational risk management disciplines and techniques

[1] The acronyms used in Figure 1 include: own risk assessment (ORA), own risk and solvency assessment (ORA), internal capital adequacy assessment process (ICAAP), internal liquidity adequacy assessment process (ILAAP) and key risk indicator (KRI)

2.1 An immediate definitional issue arises. In what ways should "operational" risk management be differentiated, if at all, from more generic risk management? In some business sectors, there may be little clear differentiation, except perhaps to hive off a firm's capital and strategic business management activities from its more day-to-day operationally focused risk management. Raising capital from or returning capital to investors and decisions on strategic business purchases or divestments have conceptual differences from a firm's day-to-day business operations. The thesis here might be that a firm's "operating" profit typically incorporates every profit or loss line other than "exceptional" ones (such as divestments). Adopting such a definition, nearly all risks that might disrupt the smooth and profitable running of the whole business can be construed to be "operational", and it becomes a largely irrelevant qualifier.

2.2 A narrower definition of "operational risk" is generally used in the financial sector, including the insurance sector. Typically, in this sector, insurance risks and financial risks such as market risk and credit risk are differentiated from "operational" risk. In this industry, "operational risk" is usually defined more narrowly along the lines of "*the risk of loss, arising from inadequate or failed internal processes, people and systems or from external events*". This separation reflects how important market, credit and insurance risk can be to the profitability or even viability of an insurance business. There are also some important practical differences if operational risk defined in this manner. For example, market risk is more dependent on external factors (i.e. market movements), whilst operational risk is more dependent on internal factors (e.g. corporate culture, presence or absence of suitable controls, …). For insurers, operational risks are also usually unrewarded (i.e. outcomes are at best neutral and at worst negative)[2], whilst there may be some expected outperformance accruing to some sorts of risky investment strategies. The same holistic approach, encompassing *all* risks, is relevant in each instance, but terminologies and precise risk subdivisions adopted tend to be sector-specific.

2.3 EIOPA is expected to adopt a definition similar to the one given in Section 2.2 in material designed to assist in the supervision of the management of operational risk by IORPs (but maybe also including legal/compliance risk and some types of emerging risk within the scope of "operational risk").

2.4 Another definitional complication arises from regulatory drivers. The insurance industry, like most of the rest of the financial sector, is relatively heavily regulated in terms of capital requirements and financial conduct rules firms within it must adopt. On the one hand, EU insurers are required to have a specific risk management function that has several prescribed responsibilities. On the other hand, regulators want firms to embed risk management into everything that they do. In this sense, essentially everyone in the firm is supposed to be a risk manager of sorts, or at least to adopt an appropriate risk management orientated mindset. As far as operational risk is concerned, the overall goal is to have everyone in the business mindful of and seeking to mitigate the operational risks most pertinent to them even if specific teams ("functions") carry greater responsibility for the coherence of the risk management being adopted by the whole firm.

[2] That is, insurers' own operational risks are usually unrewarded. However, some insurers insure the operational risk exposures of others, e.g. by providing cyber risk insurance coverage. Some outsourcing firms also seek reward from managing operational risks effectively, as this is a core component of being an effective outsource service provider.

2.5 In practice, this results in an EU insurer's risk management function being responsible for the following in the context of management of the insurer's operational risk:

(a) Formulating and implementing a coherent and effective risk management process
(b) Championing risk management with senior executives and board
(c) Drafting / updating risk policies including ones touching on operational risk
(d) Developing and implementing ways to measure and manage operational risk
(e) Formulating and implementing controls
(f) Capturing loss and other relevant business risk management information and preparing and presenting relevant management information and proposals
(g) Coordinating or developing potential operational risk scenarios to use in the firm's Own Risk and Solvency Assessment (ORSA) or for IORPS its Own Risk Assessment (ORA), see Appendix A
(h) Contingency planning and crisis management

2.6 When carrying out these activities, the risk management function will often want to **leverage the insights of others** within the business. These insights might relate to plausible ways in which a specific type of adverse operational risk might crystallise. It might also relate to how serious the resulting loss might be. Appendix B describes some ways of capturing such insights effectively.

2.7 It is usually helpful to adopt a structured approach to many risk management activities. This often favours the creation and dissemination of **a risk "dashboard" or equivalent**. More sophisticated versions of such dashboards can be interactive, involve collation of information from many different sources and assist in broader management information dissemination. Some of the information contained in such dashboards might not merely target downside risk mitigation but might also assist with upside opportunity identification.

2.8 Managing a risk effectively generally involves at least some **measurement** of it. Different levels of sophistication are apparent in how different firms tackle this issue. Larger firms exposed to multiple types of operational risk may use the so-called loss distribution approach (LDA). With the LDA, loss frequency and severity are modelled separately and then combined (perhaps using Monte Carlo simulation or corresponding analytical approximations). The LDA and other approaches are explained further in Appendix C. Smaller firms with simpler operational processes might focus more on the creation of just a handful of appropriate scenarios or stress tests to apply to the business, selected using expert judgement (coloured by any relevant available data, such as past operational risk loss histories for the firm itself and for its peers). Key risk indicators (KRIs) that capture changes in business line size and therefore changes in effective exposures can assist in assessing what impact might arise if a given stress materialises. Scenario and stress testing and KRIs are discussed further in Appendix D. Nearly all ways of quantifying operational risk face the challenge of limited data. Some of the ways in which practitioners seek to rise to this challenge are described in Appendix E.

2.9 Managing a risk effectively also requires introduction of appropriate governance arrangements such as formulating and implementing an appropriate **risk appetite / tolerance and appropriate risk limits**. Ones particularly relevant to insurance operational risk management are described further in Appendix F. A firm's risk dashboard will typically include information on how well these limits and appetite statements are being adhered to. Very important is the extent of buy-in from the firm's senior management and board. Without leadership from the top, only lip service may be placed on the benefits of effective

risk management. This is as true for operational risk as for other types of risk the firm may face.

More senior risk professionals tasked with getting this buy-in will typically also need a range of **softer influencing skills**. Softer skills that a good (operational) risk manager generally needs to possess are summarised in Table 1, alongside more concrete qualitative and quantitative skills.

Table 1: Desirable skills that a good (operational) risk manager should ideally possess		
Qualitative skills in	**Quantitative skills in**	**Softer skills**
- Risk and Control Self-assessment (RCSA) - Risk maps (risk identification attributing a level of concern on probability and severity) - Business Continuity and Disaster Recovery management - Risk Appetite / tolerance and Key Risk Indicator (KRIs) definition - Quality management (such as COSO, ISO, Six Sigma, Sarbanes-Oxley …) - Scoreboards - Information security management - Anti-fraud management - Management of insurance taken - Health and safety management	- Risk capital modelling - Loss data collection (internal and external) - Defining loss frequency and severity distributions (with data quality as a challenge) based on techniques such as extreme value theory, simulation, fuzzy logic, neural networks, predictive modelling, … - Stress testing and scenario analysis - Risk-adjusted return analysis	- Challenging skills - Leadership - Fostering dialogue - Crisis management - Communication - Broad knowledge of the company, its processes and systems - Industry/sector knowledge - Having easy access to people and information - Agility - Project management - Controlling and auditing - Vigilance - Change management - Networking skills

2.10 To restrict risk management to just what is strictly prescribed by regulation is to miss a trick. Firms with good risk management will aim to ensure that relevant risk management mindsets permeate beyond just those business functions who are required to be involved by regulation. They will also aim to leverage for competitive advantage information and insights being gathered for other purposes, including risk management. We can therefore view risk management as ultimately seeking to include elements of both of the following, even if regulation tends to result in the team within the insurer that formally has the title of "risk management function" focusing more on (1) than on (2):

(1) downside risk mitigation; and
(2) upside opportunity capture.

2.11 Few firms have in-house access to every possible **skill-set** they might need. Risk management is no exception. Alongside individuals working in-house, many firms also employ a range of external consultants to assist them in risk management activities. Consulting firms or other service providers may also develop and market operational risk solutions for third parties, e.g. developing insurance products covering cyber risk, or may create technological solutions to make the day-to-day activities of the insurer's own risk managers more efficient.

2.12 Risk management, like other management disciplines is also **not static**. It is therefore instructive to consider how the typical activities of a risk management team in, say, an insurer might be expected to change in the future. ORX and McKinsey (2017) claimed that operational risk is important and increasing, but difficult to manage, that it has been too focused on calculating regulatory capital and on regulatory compliance, remaining the "unloved child of risk management", and that cyber risk is gaining an increasing profile. Areas that in their opinion most needed improvement typically related to:

(a) Sub-optimal management information
(b) minimal integration of advanced analytics
(c) ineffective and inefficient controls
(d) risk culture not sufficiently embedded; and
(e) lack of business and specialist skills

The ORX and McKinsey 2017 paper focuses particularly on cyber risk as an example of an emerging risk. More generally, new technologies bring operational change and hence operational risk. Keeping abreast of their implications is therefore an important skill for many operational risk managers.

3. The role of actuaries in operational risk management

3.1 Many elements of Section 2 are not specific to operational risk. This is as we might expect, since the definition of operational risk used in insurance regulation makes it just one out of several risks an insurer will typically face. Exactly how individual firms structure their operational risk activities varies considerably depending on firm size, business focus, importance relative to other risks and level of maturity of the firm's activities in this space. Exactly who they employ within their operational risk management teams is equally varied.

3.2 Much of the variation in staff background reflects the advantages that multi-disciplinary teams should possess when managing risk. For example, management of some risks is likely to benefit from legal or regulatory understanding (e.g. consideration of the risk that contract terms may be unclear and therefore interpreted unfavourably by Courts). Whilst firms will typically have specialist legal teams or advisors who will lead on formulating legal opinions, some understanding of the sorts of issues involved, perhaps gained from on-the-job experience, is still likely to be beneficial for those tasked with putting such risks into context.

3.3 In this Section, we do not want to play down the benefits that can accrue to a firm from having a variety of skills and backgrounds within their risk management teams. However, we do want to explore whether the actuarial training and professional ethos leave them particularly well positioned to form a core part of such a team.

3.4 The insurance industry employs many actuaries, including many who already associate with working in "risk management". According to internal analyses carried out by the Actuarial Association of Europe, approximately a quarter of European actuaries specifically work in risk management, e.g. in risk management functions or in related fields. A high proportion of chief risk officers or others who head up risk management functions are actuaries. The global actuarial profession has also established a credential, the Chartered Enterprise Risk Actuary (CERA) to assist in developing actuarial training and expertise in this area.

3.5 Some risk management activities play particularly well to skill-sets commonly exhibited by actuaries. Actuaries tend to be associated with a higher level of numerical and quantitative

expertise than many other professions, so these activities include some of the more quantitative and data centric components of risk management. Historically, greater emphasis has tended to be placed on such skills within market and credit risk management teams. This may reflect the easier access to relevant data for such risks (e.g. the extensive amount of market data that is available from a range of third parties). **However, the ORX and McKinsey 2017 paper suggests that typical operational risk management gives insufficient focus to such disciplines, in which case trends should favour those who can bring such skills to the party**.

3.6 Even relatively straightforward skills in collating, summarising and visualising data can be of considerable assistance. This can be seen by asking how firms can best develop or enhance their risk dashboards. Data that these dashboards might usefully contain includes:

(a) Historic losses or near losses for the firm itself
(b) Comparative information for firm's peers
(c) Changes in risk mitigations that may have influenced the past or may influence the future
(d) Other relevant business volume information; and
(e) Summarised outputs of risk and control self-assessment reports and other tools capturing relevant expert judgement

3.7 Most of this information is not "rocket science" to process. Usually, the best way to develop a risk management discipline is to start small, establish proof of concept, identify quick wins, get broader buy-in and then roll out more generally. However, if firms want to maximise value added then it is still likely to be helpful to **utilise individuals who are comfortable with handling data and who understand some of the limitations it may possess**. An enquiring mind helps, as does focusing on data most relevant to the task in hand, testing for and spotting potential spurious outliers, being willing to group data or apply filters where relevant, a caution about over-interpretation and a willingness to try to validate otherwise potentially erroneous data, e.g. by analysing changes through time.

3.8 **The better integration of advanced analytics that the ORX and McKinsey 2017 paper thought would be desirable is also likely to play to the strengths of those actuaries who have particularly strong quantitative skills**, or at least those can effectively manage others who have such skills. A word of caution is that regulatory enthusiasm for more sophisticated models for regulatory capital purposes seems to fluctuate (see e.g. E.4). If operational risk stays overly focused on regulatory drivers then trends in this space might not, therefore, work out quite to this script. However, for firms that want to go beyond basic regulatory requirements and who want to maximise the benefit they can obtain from e.g. their ORSAs/ORAs, we would expect a premium still to be placed on such skills. Many of the techniques involved, e.g. LDA style approaches (see Appendix C), have analogies with how general insurers might price such risks were they to be asked to insure them, a role that is also commonly carried out by actuaries.

3.9 **Actuaries with relevant business expertise and communication skills should also be able to marry up qualitative and quantitative perspectives. Much of operational risk management is about effective development and implementation of processes and policies, and embedding risk culture and disciplines into the business activities and decision-making.** Actuaries also have the advantage of a strong professional ethos, partly instilled as part of actuarial training and partly enforced by disciplinary and other cultural aspects of the professional bodies to which actuaries across Europe belong. Regulators are keenly aware of

the adverse impact that inappropriate incentives can have on individual behaviours within the financial sector. Whilst it would be foolish to assume that professional codes of conduct etc. will magically disincentivise all inappropriate behaviours from taking place, it does provide a bulwark. Some other risk management bodies are trying to create suitable professional frameworks, but few currently seem to be as well developed as those within the actuarial profession.

3.10 As we have noted previously, **successful risk managers also need to possess a range of "softer" influencing and communication skills**. Modern actuarial training does emphasise these sorts of skills despite them not being quantitative in nature, precisely because of the added value offered by individuals with such skills. Of course, it should not be assumed that everyone who receives such training ends up exhibiting such skills, but the same applies to both actuaries and non-actuaries. Likewise, sector-specific business acumen and expertise are hard to gain without some experience within the relevant sector, whatever the professional background and training the individual has previously received. Our view is that the actuarial training and professional ethos predisposes actuaries to be typically more useful as risk managers (see e.g. [*Add link to AAE two-page summary on the role of actuary in risk management when available*]), with the caveat that team variety is also likely to be desirable.

3.11 Parts of the firm other than the risk management function may also have prescribed risk management responsibilities, some of which may cascade into operational risk. For insurers, some risk management responsibilities are specifically assigned by regulation to the **actuarial function** (another control function that an EU insurer is required to have that also typically makes extensive use of actuaries). These include a requirement to contribute to the firm's risk management process including its ORSA. In the context of operational risk, this is likely to include commenting on operational risk scenarios used in the ORSA. This regulatory edict presumably stems from the realisation that in an insurance company those working in the actuarial function typically have a peculiarly good understanding of insurance and other risks and exposures present across the whole business. Effective utilisation of these insights is therefore likely to be important in implementing a robust risk management process. As with other business areas, the actuarial function will also typically contribute to formulating operational risk scenarios or other ways of measuring and managing risk relevant to its own activities. For the actuarial function these would often include ones relating to model risk, given the substantial amount of modelling activities that members of the actuarial function may undertake.

3.12 Many firms adopt a "three lines of defence" model for managing risk. The lines typically include:

Line 1: The operational units, which manage the risks inherent to their activities
Line 2: The risk management function, which sets the risk management framework
Line 3: Internal audit, which reviews the adequacy and effectiveness of the risk management system

3.13 In some firms, the actuarial function is principally a Line 2 function, given the risk management roles assigned to it as per Section 3.11. In others, it is more a Line 1 function, especially if it has a strong input into pricing and capital management. Individual actuaries may of course switch between the two as their career progresses. As we have noted earlier, much of operational risk management is control orientated. Responsibilities the actuarial

function has in the area of operational risk may therefore be more Line 2 than is typical for the remainder of its responsibilities.

4. Operational risk management beyond the financial sector

[To be completed?]

References

BCBS (2017) Basel III: Finalising post-crisis reforms. *Basel Committee on Banking Supervision*
Curti, F., Ergen, I., Le, M., Migueis, M. and Stewart, R. (2016). Benchmarking Operational Risk Models. *Finance and Economics Discussion Series. Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board*
EIOPA (2014). Guidelines on own risk and solvency assessment. *EIOPA*
IRM and ORIC (2015). Operational risk modelling: common practices and future development. *Institute of Risk Management*
Kemp, M.H.D. (2013). Tail Weighted Probability Distribution Parameter Estimation. *Nematrian*
Lloyd's, Risk Management Toolkit
Mango, D.F and Carpenter, G. (2007). Enterprise Risk Analysis (p. 114-160)
ORIC and IRM (2015). Operational risk modelling: common practices and future development. *The Institute of Risk Management*
ORX and McKinsey (2017). The future of operational risk. *ORX*
Panjer, H.H. (1981). Recursive evaluation of a family of compound distributions. *ASTIN Bulletin*, 12
Maribel Tejada (2015), LinkedIn. Franchise Value and risk as part of company value and How to ensure robust value creation? Integrating franchise risk within risk appetite
SAS (2019). Predictive Analytics: What it is and why it matters, *SAS website*, viewed 2 April 2019
Towers Watson (2013). Another bite at the apple – Risk appetite revised
TPR (2015). Integrated Risk Management. *The (UK) Pensions Regulator*

Appendix A: Own Risk and Solvency Assessment (Insurers) and Own Risk Assessment (Pension Funds)

Introduction

A.1 In this Appendix we discuss operational risk management aspects of the Own Risk and Solvency Assessment (ORSA) and the Own Risk Assessment (ORA) that EU insurers and pension funds (IORPs) respectively are now required to undertake. In many jurisdictions across the globe insurers are now required to undertake ORSAs, although there are some differences in how this term is interpreted in different jurisdictions. Comments below relate specifically to EU requirements, which for ORSAs derive from the Solvency II Directive and associated Delegated Regulations and Implementing Technical Standards. The ORA is a new concept within the EU's IORP II Directive which came into force in early 2019. It has fewer direct equivalents in other jurisdictions.

A.2 There are several important differences between the Solvency II Directive and the IORP II Directives, which influence the nature of an ORSA versus an ORA, e.g.:

Solvency II Directive	**IORP II Directive**
Maximum harmonisation Directive	Minimum harmonisation Directive, see IORP II Recital (3)
Extensive role for EU Commission and EIOPA in formulating and setting guidelines	Much less scope for EIOPA to create binding guidance
Has led to Delegated Regulation (Level 2), implementing technical standards (Level 3), …	Social and labour law reserved to member states
Harmonises solvency requirements across EU (for single market)	No specific solvency requirements across EU, although EIOPA keen to promote Common Balance Sheet approach when IORPs are carrying out their ORAs
Own Risk **and Solvency** Assessment	Own Risk Assessment
Reporting to the supervisor and to the public	Reporting to the supervisor and communication to members

ORSAs (Insurers)

A.3 EIOPA-BoS-14/259 ("Guidelines on own risk and solvency assessment") sets out 20 guidelines including ones on:

(a) General approach, role of Board, documentation (including policy, record, internal report, supervisory report), frequency
(b) Need for a forward-looking perspective of overall solvency needs
(c) Valuation and recognition bases
(d) Continuous compliance with regulatory capital requirements and technical provisions
(e) Deviations from assumptions underlying SCR calculation
(f) Linking ORSA to strategic management and decision-making
(g) Additional guidelines for groups

[Add additional practical commentary on these guidelines?]

A.4 *[Comment on how operational risk is typically taken into account in ORSA?]*

ORAs (pension funds)

A.5 According to article 28 of the IORP II Directive, IORPs must carry out an Own Risk Assessment (ORA) at least every three years or without any delay following any significant change in the IORP risk profile or in the pension schemes operated by the IORP. ORA should follow the principle of proportionality and includes a qualitative assessment of operational risk. Reference merely to a "qualitative assessment" perhaps reflects an expectation on the part of policymakers that a high proportion of operational risk management activities in this field will focus on implementing controls and monitoring and reporting on them (see Figure 2).

A.6 At the time of writing there is no specific information on how to take operational risk into account in an (EU) ORA or even how to conduct an ORA. Nor is there much specific information in most existing individual member state regulatory frameworks. In the UK, the Pension Regulator introduced a framework some time ago called Integrated Risk Management which applies to IORPs under its jurisdiction, see TPR (2015). However, it does not contain a great deal on operational risk per se.

A.7 At a meeting of the EIOPA Occupational Pensions Stakeholder Group in October 2018, EIOPA indicated that they were planning to develop **guidance for national supervisors by around mid-2019 in four areas**:

(1) Governance documents, including Statement of Investment Policy Principles (SIPP) and Own Risk Assessment (ORA)
(2) Practical implementation of EIOPA's common framework on risk assessment
(3) Operational risk, including cyber and outsourcing risk; and
(4) Environmental, Social and Governance (ESG) risk assessment.

A.8 At the time of writing, the EIOPA guidance on ORA has yet to be finalised but is expected to include material on:

- What sorts of risks are to be covered in the ORA
- The structure and contents of ORA documents, to whom it will be disclosed, when and how the ORA will be reviewed and how consistency is to be achieved between information used in the ORA and information used in other relevant documents the IORP may produce
- How the IORP membership structure will be allowed for in the ORA

A.9 Operational risk management principles expected to be highlighted in the EIOPA guidance context include ones relating to:

- Risk culture and control environment, including Board approval processes etc.
- Existence of an appropriate risk management system (including a risk management function)
- Integration of operational risk management within the IORP's overall risk management system, proportionate to the size and structure of the IORP
- A risk appetite / risk tolerance statement
- Appropriate identification and assessment of operational risks (including ones arising from new activities) and monitoring and reporting of exposures (including breaches of risk tolerance, material losses and external developments)
- Contingency planning to ensure continuity of activities

A.10 EIOPA is also expected to highlight outsourcing risks in its guidance. Pension administration and investment management activities can be particularly important in terms of operational risk exposures for many IORPs, once one includes outsourced activities within the complete picture of what IORPs do.

A.11 We can also expect IT-related risks to be given some prominence, as these are commonly highlighted by individual supervisors who contribute to EIOPA's own governance structure. For example, key IORP operational risks that the Belgian supervisor (FSMA) has recently highlighted include:

- Data protection risks arising from e.g. the EU's General Data Protection Regulation ('GDPR')
- Cyber risks
- Outsourcing

ICAAP and ILAAP (banks and investment firms)

A.12 EU banks and investment firms are required by the EU's Capital Requirements Directive to carry out an internal capital adequacy assessment process (ICAAP) and more recently have also been required to carry an internal liquidity adequacy and assessment process (ILAAP).

A.13 The ICAAP (taken in conjunction with the ILAAP) has conceptual similarities with an insurer's ORSA. Indeed, some jurisdictions, e.g. Australia, even call their equivalent of an ORSA an ICAAP.

Appendix B: Facilitating operational risk workshops and other ways of capturing the wisdom of experts

B.1 A common way of engaging management and staff in the task of measuring, managing and mitigating operational risk is to hold workshops. The aim of such workshops is often to identify operational risk exposures that the business lines may face and to identify how best to address these risks. This may be combined with brainstorming of scenarios or stress tests that might be used to quantify operational risk, see e.g. Appendices C and D. They will often also have an information gathering element, e.g. they may be used to identify business volume measures that would help to project forward future operational risk exposures, see e.g. E.10(c). They may also include brainstorming of emerging risks, particularly if the business environment or the specific business model being followed is changing.

B.2 Clearly important with such workshops is to communicate what the workshop aims to cover, to maximise the effective engagement of participants. Other important steps include:

- Participant identification (and numbers). Having too many individuals may make a workshop unwieldy and limit the effective capture of information from individuals. Some particularly important individuals may need to be met individually or in very small group contexts. Although there is a tendency to seek out the most senior individuals available, less senior individuals may have a better understanding of day-to-day business activities in the relevant department, and their insights may be equally valuable.
- Advance communication. Ideally, this should highlight high-level support for the workshop, why the input from the selected individuals will be valuable and the broader business benefits that are expected to flow from the workshop. Participants should be advised about what will be expected of them and how the workshop will operate.
- Preparation. Those leading the workshop are likely to obtain better information sharing from the participants if they familiarise themselves with operational risk issues likely to be faced by the participants (e.g. from previous workshops or by extrapolating from other businesses or business units)
- Deciding on workshop structure. There are many ways of eliciting insights from participants, but for them to be effective they generally need have a clear focus on what the workshop is aiming to deliver. Usually this will involve articulating a set of potential risks (covering all important areas) and then capturing relevant information on these risks. The information to be sought is likely to include most or all of the information set out below.

Data being sought	**Comment**
Risk mapping	I.e. how the risk in question fits into the broader business context (including processes and systems)
Likelihood	May be a score from 1 = low likelihood (e.g. <5%) to 5 = high likelihood
Severity	May be a score from 1 = low severity (in context of business as a whole) to 5= high severity
Historical experience	Examples of past losses or near misses
Credible worst-case scenario	
Mitigation in place	
Effectiveness of mitigation	
Mitigation planned	
Person(s) responsible for mitigation	

Risk owner	E.g. relevant manager
Documentation on mitigation	E.g. its location
Other	

B.3 Once a suitable level of consensus is reached, the aim should be to select the most important risks and to develop a tentative ranking, which may need to be replayed later to the workshop participants and more senior management for further review. If it is practical, it can be helpful to obtain different perspectives on the same risks as this can assist in carrying out a dispersion analysis. Such an analysis can identify risks that are currently underappreciated by some participants, which could indicate possible weaknesses in current mitigation strategies.

B.4 Operational risk managers should also be on the lookout for possible cultural failings that may be politically difficult to introduce but may be suggestive of a poor control environment and heightened exposure to operational risk. These include arrogance (e.g. overconfidence in the processes being bound to be sound) and concentration risk (e.g. excessive reliance on small numbers of individuals, controls or processes)

B.4 The main results of these workshops and the surrounding processes are likely to be:

(a) A list of key risks
(b) A tool that can assist in monitoring potential changes to these risks
(c) Advancement of the firm's risk culture and focus

B.5 Sometimes the workshops or follow up sessions will target additional information that aims to assist in more detailed quantification of the risks or in how they may best be aggregated. This will depend on the extent to which the firm uses more advanced techniques for quantifying operational risk and is seeking expert judgement input into this process, see e.g. Appendices C and E. Care is then needed to ensure that the same information is being asked from all such experts, who of course also need to have sufficient understanding of the business to be able to form valid expert views on the risks involved.

B.6 Capture of the information may use the Delphi method (also known as Estimate-Talk-Estimate, ETE). This is structured communication method, originally developed as a systematic, interactive forecasting method, which relies on a panel of experts. It is based on the principle that forecasts / decisions from a structured group of individuals are likely to be more accurate than those from unstructured groups. With this method, the experts answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymised summary of the experts' forecasts from the previous round along with the reasons they provided for their judgements. Experts are encouraged to revise their earlier answers in the light of replies of other panel members. The hope is that as the facilitation progresses, the range of answers will decrease and the group will converge on the 'correct' answer, the process finishing once sufficient convergence has happened.

Appendix C: The loss distribution approach (LDA) and other approaches to quantifying operational risk

C.1 There are three main types of approach used to quantify capital required to face operational risk:

(1) The frequency-severity / Monte Carlo / Advanced Measurement approach;
(2) The stress testing / scenario analysis approach (and hybrids between this and (1)); and
(3) The Bayesian / causal approach (non-linear modelling).

C.2 The first and the third approach, and in some circumstances the second, can be viewed as special cases of a more general framework which is often called the loss distribution approach (LDA).

C.3 The frequency-severity approach typically involves the following steps:

(1) We model (usually separately) the frequency and severity of the operational loss that might arise for process i and risk k. Each is expressed statistically, i.e. we identify a statistical distribution applicable to each operational risk loss of a given type[3] and we also identify a statistical distribution for the number of losses of a given type that might arise over some specified period.
(2) Given these statistical distributions we identify the cumulative distribution of S where:

$$S = \sum_{i,k} S_{i,k} \qquad S_{i,k} = \sum_{j}^{N_{i,k}} X_{i,k}^{(j)}$$

and $N_{i,k}$ = number of losses from process i and risk k, $X_{i,k}^{(j)}$ = cost of loss j from process i and risk k and $S_{i,k}$ = sum of losses from process i and risk k in period

C.4 In some cases it is possible to find an analytical expression for S but usually a Monte-Carlo approach or some other approximation (e.g. the Panjer algorithm[4]) is needed.

C.5 Such an approach is only practical if there is enough historical data[5] (or in theory market-implied) data available to model the different risks and processes. It is therefore better suited to high frequency / low severity risks. It tends to rely on past data, so may not be effective in capturing new or emerging risks. Usually the risks are simulated independently, so there is then the question of how to aggregate the different risks together, i.e. what diversification benefits to assume. Different aggregation methods may be used, e.g. correlation matrices, copulas, etc. depending on the level of sophistication desired for the resulting statistical estimation process. If the focus is on relatively extreme outcomes (e.g. for 1-in-200 year Value-at-Risk computations) then this may favour use of distributional

[3] According to IRM and ORIC (2015) the most common distributions used for loss frequencies are the Poisson and negative binomial distributions and for loss amounts are the lognormal, Weibull and generalised Pareto distributions. IRM and ORIC (2015) do not specify what is the most common calibration approach, e.g. maximum likelihood, generalised method of moments, or some other methodology such as one of the tail weighted approaches described in Kemp (2013).
[4] See e.g. Panjer (1981)
[5] Some of this data might be derived from industry-wide databases, provided the data is considered relevant for the firm in question.

forms that align with those underlying Extreme Value Theory ('EVT'), e.g. the generalised Pareto distribution[6].

C.6 Stress testing can also be used to quantify operational risk. Stress testing is described further in Appendix D. Usually firms carry out stress tests that focus on individual areas of operational risk exposures (e.g. there might be one stress test for mis-selling, another for investment administration errors, …), although for reverse stress testing broader combinations of stresses all happening together may be explored.

C.7 If the primary approach to quantification involves single exposure-level stress tests then the firm will again have the challenge of how to aggregate the results of individual stress tests together to come up with an aggregate operational risk quantification. Sometimes (particularly for smaller firms) the aggregation may involve a simple summation, on the grounds of proportionality, despite the potential weaknesses of such an approach[7]. Alternatively, a correlation-based aggregation approach (akin to ones used in the Solvency II Standard Formula when aggregating different risk modules) may be adopted.

C.8 Larger firms may adopt a more sophisticated approach to aggregating individual stress tests along the lines of the following:

(1) For every risk, relevant business unit experts are asked to build up scenarios that, say, model:
   (a) average frequency;
   (b) average severity scenario; and
   (c) one or more 'adverse' severity scenarios (perhaps including an 'extreme' scenario), with the nature of an 'adverse' or an 'extreme' scenario being defined in a manner that can be given a specific statistical meaning (e.g. a given quantile of the relevant loss distribution)
(2) Suitable distributional families are chosen for loss frequency and severity and parameters are selected to fit to the inputs in (a), (b) and (c)
(3) Total losses are simulated as per the frequency-severity approach, using these distributions and associated distributional parameters (usually using Monte Carlo technique)

C.8 This approach, like the more traditional purely data driven frequency-severity approach, involves building up a statistical distribution for losses and so can be viewed as an example of a *loss distribution approach* (LDA). The more traditional frequency-severity approach is arguably more backward looking, i.e. more 'historic' in focus. This variant that incorporates stress-testing / scenario analysis is arguably more forward looking, as it now includes a priori views (coloured by expert judgement) on what distributions to use. The approach is therefore more capable of addressing cases where there is not enough historical data to use a purely statistical approach (e.g. most emerging risks). It is also more capable of handling low frequency high severity risks. Conversely, it is more difficult to conduct back tests as relevant historical loss data will generally not be available. It is also highly dependent on qualitative inputs from the relevant business line experts (i.e. on them truly possessing the relevant expertise). Some care is needed in articulating what exactly these experts need to

[6] Please note, however, that for traditional EVT to apply we need the tail behaviour of the distribution to converge in a specific way. It is possible to extrapolate using any selected distributional family and not just the generalised Pareto distribution typically viewed as relevant within this variant of EVT, see e.g. Kemp (2013).
[7] For example, the result becomes sensitive to how many exposures we decompose the whole book into, since the more stresses we consider the greater will be their sum.

supply, to avoid the risk that different people will interpret terms such as 'adverse' or 'extreme' differently.

C.9 An approach that blends a purely data driven LDA with expert judgement in the guise of well-crafted stress tests and scenario analysis is an example of what IRM and ORIC (2015) call a *hybrid approach*. They surveyed a range of insurers, the majority of whole used an internal model to calculate their Solvency Capital Requirement. At the time that they wrote, the most common modelling approach appeared to be what they refer to as a "Hybrid Model – Scenarios and loss data combined". They believed that such a modelling approach should represent the standard going forward. Their observation was that:

> "*It is unsurprising that pure Loss Distribution Approach (LDA) models are not popular, due to the bias towards backward-looking and relatively scarce loss event data to provide sufficient comfort in that methodology. We have also concluded that a pure LDA model will not be satisfactory for decision making and supporting the overall management of operational risk. At the other end of the spectrum, models built without loss data analysis may lack robustness and should only be considers as a transitional step for firms currently improving their risk event collection and analysis capabilities.*"

C.10 IRM and ORIC (2015) include as examples of hybrid approaches ones where loss event data is used for one or more of the following:

(a) As a direct input into scenario quantification
(b) To parameterise scenario quantification
(c) To support the validation or back-testing of scenarios
(d) To derive parts of the loss distribution, but with using scenario outputs used to shape other (generally more extreme) parts of the distributional curve

The approach described in C.8 can be viewed as including elements of (a), (b) and probably (d).

C.11 The Bayesian / causal approach is a typically more quantitatively focused variant of the scenario-based approach, being based on qualitative formulation of scenarios by relevant business line experts. However, superimposed on these scenarios is an analysis of causal relationships between different risks. Typically, the steps involved include:

(1) Exposure assessment, collecting business units' views on the number of items exposed to operational risk loss for e.g. next year
(2) Frequency assessment, perhaps modelled using a binomial distribution
(3) Severity assessment, perhaps using 3 scenarios involving e.g. optimistic (25th percentile), middle (50th percentile) and pessimistic (75th percentile) scenarios from which are derived suitable distributions
(4) Combination of these inputs taking account of the presumed causal relationships between different risks

C.12 In theory, such an approach can combine availability of historical judgement with expert knowledge, so can be thought of as a different and more generalised way of incorporating a priori views into the generic LDA approach. It can also perhaps highlight better key variables and contagion channels that might most impact the firm, which can allow concentration of risk mitigation efforts in these areas. However, it is still dependent on availability of relevant

historic data (or if expert judgement is used instead in specific areas, on the reliability of this expert judgement). It also places a high reliance on conditional probabilities, i.e. the probability that risk A will arise given risk B happens. Formulating robust views on these conditional probabilities is likely itself to require expert judgement.

C.13 We see that it is possible in a formal sense to frame essentially all the above approaches as examples of the LDA approach but making greater or lesser use of expert judgement. This means that it ought to be possible to back-fit operational risk capital that firms hold as if they were adopting an underlying LDA approach, and to benchmark capital held accordingly. Curti et al. (2016) includes such an exercise for banks. Operational risk is difficult to model at high quantiles (i.e. for high confidence level value-at-risks) and difficult to link to macroeconomic factors. Benchmarks that seek to place operational risk capital levels onto comparable bases ought therefore to be helpful for firms (and regulators) in assessing how robust are the models they are using. Firms are often incentivised to minimise their capital employed and this can lead operational risk modellers to adopt insufficiently conservative assumptions in their models.

C.14 A tool that some commentators expect will become increasingly important in some areas of operational risk management is predictive analytics. It is already used to detect potential fraud. For example, SAS (2019) asserts that "*Combining multiple analytics methods can improve pattern detection and prevent criminal behavior. As cybersecurity becomes a growing concern, high-performance behavioral analytics examines all actions on a network in real time to spot abnormalities that may indicate fraud, zero-day vulnerabilities and advanced persistent threats*". Actuaries are becoming increasingly involved in data analytics, and are typically more comfortable than most other professions with the data-driven analyses involved, given the focus placed on data quality and relevance in many areas of actuarial work.

Appendix D: Stress testing, scenario analysis and Key Risk Indicators

D.1 *[To be completed]*

Appendix E: Coping with limited data

E.1 A common criticism levelled at operational risk measurement is that it may be very difficult or impossible to do with any reasonable level of accuracy, given the very limited data that firms will (hopefully) have on their own loss experience and the potential lack of comparability that might arise if they are basing their quantification of other firms' data.

E.2 This reflects a stylised decomposition of operational risks into two types:

(a) High-frequency, low severity risks, e.g. capturing relatively unimportant policy information wrongly and therefore miscalculating some policy benefits or premiums; versus
(b) Low-frequency, high severity risks, e.g. large-scale systematic fraud, mis-selling episode affecting multiple customers or large investment dealing error

Risks falling into category (a) are inherently more amenable to statistical measurement, because of the extra data that is likely to be available to model them robustly.

E.3 At issue is that, originally, commentators may have hoped that operational risks in (a) would predominate. However, actual experience suggests the opposite is the case, i.e. that most operational risk exposures (weighted by size of loss) fall into (b), and so are much harder to measure reliably.

E.4 The loss of faith in the practicality of robustly quantifying operational risk is perhaps most starkly evidenced by the abandonment in Basel III[8] of all advanced measurement approaches for quantifying operational risk, and their replacement by a new minimum capital requirement for operational risk that involves a standard formula based on the following components:

(a) A Business Indicator (BI) which is a financial-statement based proxy for operational risk built up from three components, an interest, leases and dividend component (ILDC), a services component (SC) and a financial component (FC)
(b) A Business Indicator Component (BIC), which is calculated by multiplying the BI by a set of regulatory determined marginal coefficients α_i, that are 12% if BI ≤ €1bn but rise to 18% for the part of the BI above €30bn
(c) An Internal Loss Multiplier (ILM), which is a scaling factor that is based on a bank's average historical losses and the BIC. For firms that are small enough (i.e. with BI ≤ €1bn) the ILM is set to 1 and the operational risk capital is then a straight multiple (12%) of the BI.

E.5 The dependency on historic losses means that Basel III also contains general and specific criteria on loss identification, collection and treatment. When Basel III is in force, firms will be required to have documented procedures and processes which must be comprehensive and capture all material activities and exposures from all appropriate subsystems and geographic locations. Supervisors may require that the internal loss data be mapped onto specified supervisory categories. Loss capture processes need to capture when the event began ("date of occurrence"), when the firm became aware of the loss ("date of discovery") and the date (or dates) when recognised against P&L, as well as information on recoveries and descriptive information about the drivers or causes of the loss event. Losses gross and net of insurance need capturing.

[8] See BCBS (2017).

E.6 The issue, therefore, is not so much that (larger) firms won't have some relevant internal data. It is that regulators are sceptical about whether the data that is available will be adequate to allow robust estimation of capital needed to face low frequency, high severity operational risk types.

E.7 The operational risk component of the Standard Formula SCR computation for insurers is also relatively formulaic (expressed as factors applied on premiums and provisions) and is therefore also quite a blunt way of measuring operational risk.

E.8 Firms will still, however, wish to identify more forward-looking risk-sensitive approaches to quantifying operational risk, for their own internal risk management purposes. Sections C.7-8 provide clues as to how this might be done. The lesson highlighted there is that if there is insufficient actual data available to robustly estimate aggregate operational risk exposures, we need to supplement this information in some way with expert judgement, probably coloured by knowledge of others' losses and by views formed about how representative others' experience is to the firm in question. Put another way, information that might be available from external databases, suitably interpreted using expert judgement can assist when firm-specific data is limited or largely non-existent.

E.9 At the extreme, the whole process could exclusively rely on expert judgement, but then it would likely lack transparency. It would be akin to a case reserve prepared by a property-casualty (i.e. non-life) insurance assessor based on gut feel as to how large the eventual loss might be. Originally, most insurance claims reserves were established in this manner. Over time, however, actuaries developed more quantitative ways of assessing reserves, e.g. using chain ladders and manipulating claims triangles, making use on any available relevant data. Of course, this doesn't stop there being large uncertainties in some claims reserving exercises, e.g. for new lines of business where there is little or no relevant past data that is amenable to statistical manipulation. Using statistical terminology, the task involves the application of *credibility theory*, i.e. introducing a priori views (here 'expert judgement') alongside views derived from the data, and weighting the two differently depending on how 'credible' (i.e. robust) are the views derived from the data.

E.10 In our opinion, quantification of operation risk has many similarities to the task of claims reserving in non-life insurance:

(a) The best, indeed, arguably the only, way of dealing with limited data is to supplement it with expert judgement, provided the expert judgement is well-informed.
(b) Some credibility-weighting is then needed between views derived from the firm's own data and views derived from this expert judgement. Credibility weighting also needs to be applied to loss data derived from other firms' experiences, as it will not always be obvious how relevant such data is to the firm in question.
(c) As with non-life insurance, it is necessary to adjust for factors that may have altered the base operational risk exposure sizes in the past or may do so in the future. These adjustments should be informed by business metrics that link to the relevant exposures.

E.11 It is intuitively reasonable to expect some link with non-life insurance pricing and reserving techniques, since insurance can in principle be taken out for most forms of operational risk.

Appendix F: Setting operational risk appetite and limits and key risk indicator (KRI) identification

F.1 Risk appetite represents the willingness and the ability of the insurer to take risk. Risk appetite articulates the level of risk a company is prepared to accept to achieve its strategic objectives. Risk appetite frameworks help management to better understand a company's risk profile, find an optimal balance between risk and return, and foster a healthy risk culture in the organization. As such risk appetite links to the possible impairment of the objectives (mission) of the company and the business strategy to achieve this mission. A good company's risk strategy, risk appetite (risk preferences) and tolerance address key risks in relation to its mission impairment, usually organised around different performance domains, such as achieving a targeted performance, preserving capital adequacy, maintaining liquidity, protecting franchise value. Risk management then boils down to the safeguarding of resources (sometimes referred to as 'buffers') - financial as well as non-financial in nature - that allow the company to absorb temporarily adverse events. In case of operational risk it is could sound a bit strange to talk about 'risk appetite'. Contrary to other risks (e.g. market risk, insurance risk) operational risks are usually not willingly incurred nor are they return driven. This means that as long as people, systems, and processes remain imperfect, operational risk cannot be fully eliminated. Operational risk is, nonetheless, manageable as to keep losses within some level of risk tolerance, determined by balancing the costs of improvement against the expected benefits.

F.2 An operational risk appetite can be expressed either quantitatively, either qualitatively. The *quantitative* approach typically expresses risk appetite in terms of limits and thresholds linked to earnings and/or solvency. Limits for operational risk outcomes may be set by the Board on an aggregate level or at the level of a single event. Examples of earnings related such statements are: 'The total annual operational risk losses, arising from both expected and unexpected event, should not exceed an amount of [amount] or 'No single unexpected operational risk loss in a single year should exceed [amount]. Expressing operational risk appetite in terms of capital consumption could be relevant as well: 'Economic [or required, or operational capital at risk] capital for operational risk may not exceed x% of total economical [or required, or operational capital at risk] capital'. Or 'Operational risk events should not destroy more than x% of the own funds in a 1 in […] year event'. A red-amber-green framework with thresholds indicating wat is acceptable, tolerable and unacceptable is typically defined in view of triggering the right escalation or action (being a change in risk profile, an increase in capital, introducing more rigorous controls, etc.). It evident that in defining operational risk appetite in a quantitative way, stress testing and scenario testing are appropriate tools for analyzing the impact of unlikely, but not impossible events, which enable the company to gain a better understanding of the operational risks that it faces under extreme conditions and the losses these would produce. That is where the actuary can step in.

F.3 Another way in expressing operational risk appetite could involve a number of rather *qualitative* statements detailing the preferences and target ambition level of the company. Franchise value (as mentioned above) is an interesting umbrella concept for defining such qualitative operational risk appetite framework. The economic worth of a firm indeed includes the value of both, tangible and intangible assets. Franchise value (or capital) represents a firm's intangible assets such as its brand, human capital, corporate culture, competences, knowledge, etc. embedded in the company and which contribute to future growth. Drivers of this franchise value are e.g. the penetration of the brand, the maturity of the organization, the capacity to innovate, the level of knowledge, the competence of the management, the engagement of the staff, etc. Other drivers relate to trust and confidence from a number of

external stakeholders such as the customers, partners, investors, regulator, society, etc. Franchise risk appears due to the existence or growth expectation of franchise value (some target level), the need to identify and assess the 'franchise at risk' (and the corresponding risk drivers) and to define the tolerance in terms of franchise value losses. Paying attention to the possible impact that operational risk can have on the franchise value of the company is paramount. Operational risk (together with other so called 'non-financial risks' such as business risk, strategic risk) could beside a financial loss, indeed cause a loss in reputation, hence seriously jeopardizing the franchise value of the company. With reference to franchise value protection, the question arises how much of this value can be decreased (and tolerated by the company) due to e.g. adverse publicity, poor reputation or regulatory intervention caused by operational risk events. It should be clear by now that franchise value is a rather qualitative risk concept, which by nature lends itself to the definition of corresponding rather qualitative risk appetite statements as further will be demonstrated.

F.4 In this context examples of a qualitative operational risk appetite statement could e.g. be: 'The Company has the ambition to have a better-than-peers quality of operations'. This could be more specific by e.g. indicating that the company wants to be ranked in the top quantile of the insurance sector for operational risk management (supposing such a ranking is available in the insurance sector). Such a qualitative statement could be further specified at the level of one or more operational risk classes (people, processes, systems). Examples are: 'The Company provides a workplace experience that attracts and retains skilled and experienced staff'; 'The Company has a low risk appetite for process failure and system outages'. Some operational risks could even merit a more dedicated statement at a lower level, such as e.g. with respect to cyber risk, risk of using the cloud, fraud or even model risk. 'Where operational risks arise, these should be mitigated and controlled, as long as the cost of controlling does not exceed the benefits from the lower level' could be a general expression of operation risk tolerance as part of the operational risk appetite framework. Examples of more specific tolerance levels are: 'The Company does not accept more than 2 IT outages for more than 1 hour during a certain period [to be specified] or 'The Company does not allow a system down time that exceeds the defined recovery time objective' or 'The company has a zero tolerance for fraud'.

F.5 Quantitative or qualitative risk appetite statements? Operational risk management is about both, measurement and management. Given its complex nature and given the lack of sufficient loss data, the quantification (measurement) of operational risk and the identification of its precise drivers still stay an important challenge. Even if we could appropriately measure this risk, we are of the opinion that appropriately dealing with operational risk is just as much about management than about measurement. Having in place a sound internal governance, a strong control environment with business resilience and continuity plans indeed form the foundation of an effective operational risk management framework. Operational risk is a broad subject. Many skills and types of expertise are required, and whilst we feel that the actuarial profession can make a significant contribution, we cannot do so alone and have to join efforts with other professions.

F.6 Operational risk being a complex process with a lot of drivers makes it difficult to cascade down risk operational risk appetite and tolerance to concrete risk limits in view of making it more operational at the level of the different operations and agents within the company. Key Risk Indicators are though appropriate quantitative indicators, which are highly predictive regarding changes in the risk profile and designed to monitor the development of significant risks amongst which operational risk. KRI are forward-looking and require a reference frame with trigger levels and escalation criteria for monitoring and reporting tolerance level

breaches. KRI are an essential and very practical part of the operational risk management framework, triggering management attention and enabling timely action to be taken to deal with issues arising. Examples are: number of complaints, staff turnover ratio (in particular turnover of experienced staff), number of employees attending training courses, number of legal actions against the company, number of failures or average down-time of IT systems and other equipment, net promotor scores, etc.

F.7 *[Is there appetite to identify in this paper how best to set an operational risk appetite for a pension fund?]*