CERA Global Risk Conference 2021

from 14 to 17 June 2021

Presented on actuview

CERA Global Risk Conference 2021
from 14 to 17 June 2021

Actuaries and Operational Risk Management

Malcolm Kemp

Nematrian

About the author

Malcolm Kemp

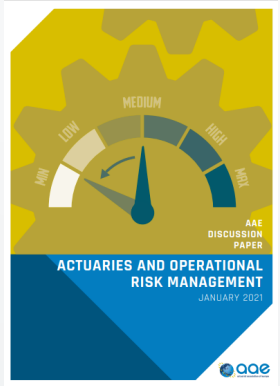
Malcolm is chairperson of the Actuarial Association of Europe's Risk Management Committee. He is an internationally known expert in risk and quantitative finance, with over 35 years' experience in the financial services industry including senior roles in insurance and investment management.

AGENDA

- Introduction
- Operational risk management disciplines and techniques
- Potential opportunities for actuaries
- Selected topics

Presentation based mainly on Actuarial Association of Europe Discussion Paper “Actuaries and Operational Risk Management” (published January 2021) written by Malcolm Kemp, Christoph Krischanitz, Daphné de Leval and Eddy Van den Borre

INTRODUCTION



Available at: https://actuary.eu/memos/actuaries-and-operational-risk-management/
Part of a wider selection of AAE publications available at:
https://actuary.eu/publications/positions-discussion-papers/

AAE

- Risk Management Committee
- Keen to promote actuarial involvement in risk management

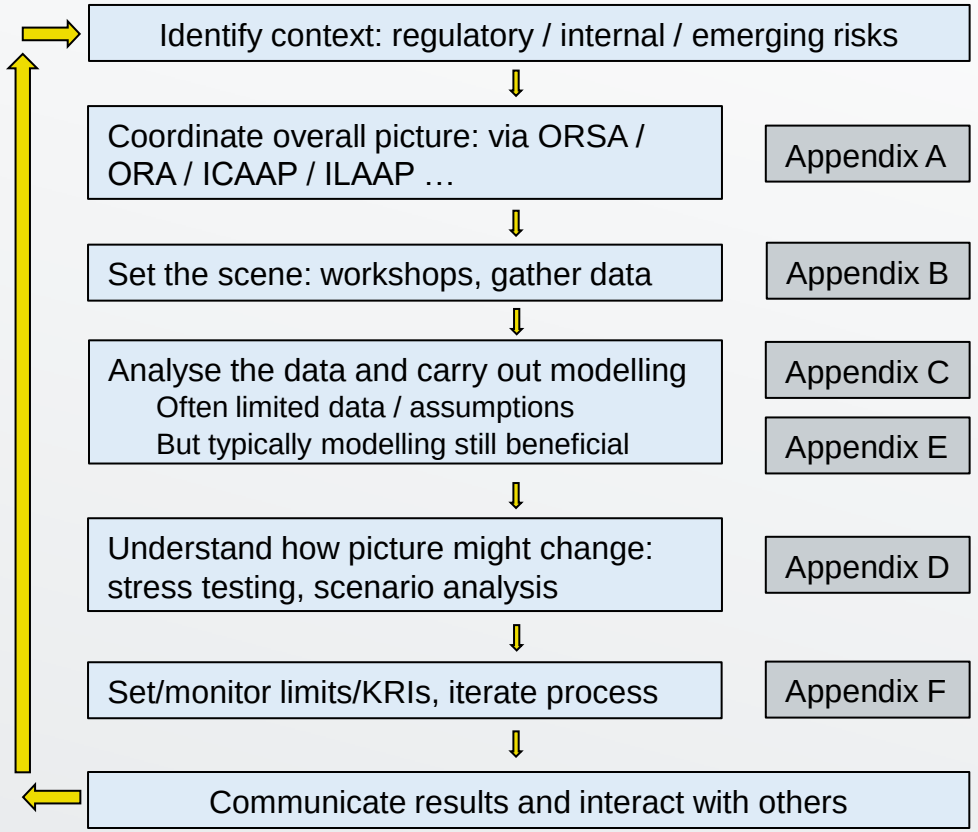
Paper contents

- Majority of paper relates to insurers or pension funds
- With some broader content

Paper Appendices

- Explore in more detail some common roles / activities relating to operational risk

Main roles of an operational risk manager



OPERATIONAL RISK: DISCIPLINES AND TECHNIQUES

- Operational risk:
  - Outside financial sector most risks might be deemed “operational”
  - Narrower definition used within financial sector
- Typically defined in financial sector regulatory texts along the lines of:

  “*the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events*”
- Usually seen as an unrewarded risk
  - Except for e.g. outsourcers or non-life insurers providing coverage against such risks (e.g. cyber insurance risk)

Typical responsibilities of operational risk managers

- Formulating and implementing a coherent and effective risk management process
- Championing risk management with senior executives and board
- Challenging from a risk management perspective the activities and decision-making of others within the organisation
- Drafting / updating risk policies including ones on operational risk
- Developing and implementing ways to measure and manage operational risk
- Formulating and implementing controls
- Capturing loss and other relevant business risk management information and preparing and presenting relevant management information and proposals
- 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)
- Contingency planning and crisis management

Desirable skills

Desirable skills for a good (operational) risk manager		
Qualitative skills	Quantitative skills	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 (e.g. 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

POTENTIAL OPPORTUNITIES FOR ACTUARIES

- ORX and McKinsey (2017) thought operational risk was the “unloved child of risk management”
  - Too focused on **regulatory capital** and **compliance**
- They thought areas most needing improvement were typically:
  - Sub-optimal management information
  - Minimal integration of advanced analytics
  - Ineffective and inefficient controls
  - Risk culture not sufficiently embedded; and
  - Lack of business and specialist skills
- Actuaries with relevant expertise should be able to help

The business landscape

Insurers and pension funds

- Considerable variation
  - Firm size
  - Business focus
  - Importance of risk
  - Risk “maturity” level

Staff

- Employees have varied backgrounds
- Advantages of multidisciplinary teams

Actuaries

- Significant proportion of insurer CROs or equivalent are actuaries
- AAE analysis suggests c. 25% of European actuaries work in some form of risk management

SELECTED TOPICS

A. ORSA versus ORA (insurers versus pension funds)
B. Operational risk workshops
C. Quantifying operational risk
D. Stress testing and scenario analysis
E. Coping with limited data
F. Operational risk appetite, limits and Key Risk Indicators

A. ORSA versus ORA

- ORSA is Own Risk and Solvency Assessment (applies to EU insurers)
  - A requirement of the EU Solvency II Directive
- ORA is Own Risk Assessment (applies to EU Institutions for Occupational Retirement Provision, i.e. EU pension funds)
  - A requirement of the EU IORP II Directive
- ICAAP is Individual Capital Adequacy Assessment Process (applies to EU banks, asset managers, investment firms)
  - A requirement of the EU Capital Requirements Directive

ORSA and ORA

Solvency II

- Maximum harmonisation directive. Extensive role for EU COM and EIOPA
- Own Risk **and Solvency** Assessment

IORP II

- Minimum harmonisation directive. EIOPA opinions for Competent Authorities
- Own Risk Assessment

Comparison

- ORSA: EIOPA-BoS-14/259 includes 20 ORSA guidelines
- ORA: EIOPA-BoS-19-247 for competent authorities

- ORA Opinion includes coverage of:
  - Outsourcing and cyber risk
  - Governance documents and protocols: ORA, risk register, risk tolerance statement (or equivalent), monitoring and reporting of breaches, losses etc., external developments
- Note also recent regulatory focus on operational resilience: e.g. proposed EU Digital Operational Resilience Act (DORA)

ORA: Cyber Risk

- Highlighted in EIOPA IORP Opinion
- Kelliher and Jaeger (2020) *Pension scheme cyber risk* highlight e.g.:
  - Ransomware attacks (including the infecting of backups)
  - Data theft (and need to compensate members for frauds then committed on them)
  - Asset theft, e.g. hacking of systems to create fraudulent transfers of funds
- Mitigation includes
  - Improve personal cyber hygiene and follow regulator-specified cyber risk principles
  - Validate robustness of controls and resources of providers of outsourced operations (including sponsor)
  - Insurance?

B. Operational risk workshops

- Usually aiming to capture the wisdom of experts:
  - Target outcome: list of key risks, tool to help monitor changes, advance the firm's risk culture
  - Obtain different perspectives, replay conclusions, be on lookout for cultural failings, maybe use Delphi method or similar

Data being sought	Comment
Risk mapping	I.e. how the risk in question fits into the broader business context
Likelihood	Maybe expressed as a score from e.g. 1 to 5
Severity	Maybe expressed as a score from e.g. 1 to 5
Historical experience	Examples of past losses or near misses
Credible worst-case scenario	Expert judgement is key
Existing mitigations	What mitigations are in place, their likely effectiveness, person(s) responsible for them, documentation (and/or location of documentation
Planned mitigations	Likely influenced by workshop
Risk owner	E.g. relevant manager
Other	Any other relevant information

C. Quantifying operational risk

- Approaches explored in Discussion Paper include:
  - Frequency-severity / Monte Carlo / Advanced Measurement approach
  - Stress testing / scenario analysis approach and hybrids between this and (1)
  - Bayesian / causal approach (non-linear modelling)
- Most can be viewed as examples of a **loss distribution approach** (LDA) but making greater or lesser use of **expert judgement**

Quantifying operational risk (2)

- Sources for the expert judgement include:
  - Professional expertise (another reason for using actuaries?)
  - External consultants
  - Other regulatory texts
    - E.g. Regulation (EU) 2019/2033 on prudential requirements for investment firms includes a Risk-to-Client element with “K-factors” relating to assets under management, client money held, assets safeguarded and administered, client orders handled, daily trading flow
    - N.B. Abandonment of Advanced Measurement Approach (AMA) in Basel III for banks
- Other firms’ experience
  - Partly via consultants
  - Partly via industry surveys
  - Partly via newsfeeds, regulatory notices, …

Quantifying operational risk (3)

- Model risk a potentially leading contributor to operational risk (see e.g. KPMG Technical Practices Survey 2020 and ORIC International Capital Benchmarking Survey 2020)
- Modelling of dependencies can significantly impact end answer. Kelliher et al. (2020) *Operational risk dependencies* suggest most common methods are:
  - **Correlation matrices**
    - Simplest approach, e.g. Solvency II Standard Formula aggregation. May overstate economic capital requirements if risk distributions are not elliptic.
  - **Copula aggregation**
    - Seems to be most common approach used by internal model firms (in UK)
    - Gaussian copula
      - Gaussian copula has zero coefficient of tail dependency. Maybe too optimistic for high severity risks?
    - T- and other copulas
      - Can include non-zero tail dependency, but more complicated
  - **Bayesian networks**
    - Rarer. Use conditional probabilities, can cope with asymmetries and may assist with a credible narrative
    - But potentially higher dependency on expert judgement?

D. Stress testing and scenario analysis

- Requires expert judgement
  - Capture and synthesise diverse opinions and concerns
  - Assist with risk mapping
  - Coping with ‘black swans’
- Many methodologies
  - Single risk factors, multiple risk factors in single scenario, multi-scenario, stochastic simulation
- Aim for:
  - Adequacy, objectivity, commitment, scenario identification, quantification, interpretation
- Standardised presentation

<table>
<tr><td colspan="2">Scenario Cyber attack</td><td>Risk owner XXX</td></tr>
<tr><td colspan="2">Scenario description
Hacker breaches XYZ’s information security controls, …
[narrative describing scenario]</td><td>RCSA / Workshop attendees
…
RCSA Score
[Numerical]</td></tr>
<tr><td>Financial impact
<table><tr><td>Description</td><td>EUR</td></tr><tr><td>System reviews</td><td></td></tr><tr><td>Legal costs</td><td></td></tr><tr><td>Total</td><td></td></tr></table></td><td>Rationale for impact
…
[Moderate severity and high severity scenarios might be developed separately</td><td>Directional assessment
…</td></tr>
<tr><td colspan="2">Risk tolerance
<table><tr><td></td><td>Current Date</td><td>Prior date</td></tr><tr><td>[Risk name]</td><td>GREEN</td><td>AMBER</td></tr></table></td><td>Key controls
… [Description]</td></tr>
<tr><td colspan="2">Internal loss / near loss events over past x years
[Details]</td><td>External loss events
[Hard and soft/reputational]</td></tr>
</table>

E. Coping with limited data

Stylised split

- Between
  - High frequency, low severity events
  - Low frequency, high severity events

What dominates?

- Low frequency high severity now seen to dominate in financial sector
- Reduced regulatory enthusiasm for internal models for operational risk in Basel III

Tackling the problem

- Need to supplement data with expert judgement
- Credibility theory

$$\alpha \times [\text{result derived from data}] + (1 - \alpha) \times [\text{result derived from expert judgement}]$$

F. Operational risk appetite, limits and Key Risk Indicators

- Risk appetite (tolerance) represents willingness and ability of organisation to take risk
  - Can be quantitative or qualitative or both
  - Strong link with franchise value and reputational risk
  - Difficult to cascade operational risk appetite into concrete limits that are meaningful for business units
- Key risk indicators (KRIs) may help with operationalization by focusing management attention
  - Examples include number of complaints, staff turnover ratio, number of employees attending training courses, average IT system down time, net promotor scores, business volumes …

SUMMARY

- Operational risk management involves mix of qualitative, quantitative and softer skills
  - "Unloved child of risk management": often too focused on regulatory capital and compliance and insufficient analytical rigour
  - A key issue: how to address limited data
- Actuarial skills very relevant
- Six specific topics covered in Discussion Paper appendices illustrate how actuaries can help