Actuaries and Operational Risk

Malcolm Kemp, Nematrian

EUROPEAN ACTUARIAL
DAY 2025
www.ead2025.org

About the speaker

Malcolm Kemp

Malcolm is the vice-chairperson of the Actuarial Association of Europe and Managing Director of Nematrian. 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
- Selected topics covered in recently published AAE paper

Presentation based mainly on Actuarial Association of Europe Discussion Paper "*Actuaries and Operational Risk Management (2025 Edition)*" (published July 2025) written by Sinéad Cronin, Malcolm Kemp, Christoph Krischanitz, Daphné de Leval, Karina Schreiber and Eddy Van den Borre

The presenter would like to thank his co-authors for their efforts in preparing this updated paper

Introduction

Available at: https://actuary.eu/paper/aae-discussion-paper-actuaries-and-operational-risk-management-updated-2025-edition/

Part of a wider selection of AAE publications available at: https://actuary.eu/papers/

Summarised in European Actuary Magazine Sept 2025 edition: https://actuary.eu/wp-content/uploads/2025/08/TEA-43-full-issue.pdf

First edition (2021) presented to EAD 2021

AAE

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

Paper contents

- Majority of paper relates to insurers or IORPs
- Also, some broader content

Paper Appendices

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

Operational risk

- Outside financial sector most risks might be deemed “operational”
- Narrower definition used within financial sector
  - E.g. as “*the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events*” in Solvency II texts and in EIOPA-BoS-19-247 “Opinion on the supervision of the management of operational risks faced by IORPs”
- Near identical definitions used elsewhere in financial sector, e.g. Basel Committee on Banking Supervision
- 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)

Paper provides

- Overview of roles, skills and techniques actuaries can bring to operational risk management
  - Arguing that actuaries are well placed to assist in this area
  - Alongside merits of multi-disciplinary approaches
- Appendices covering a wide range of topics including:

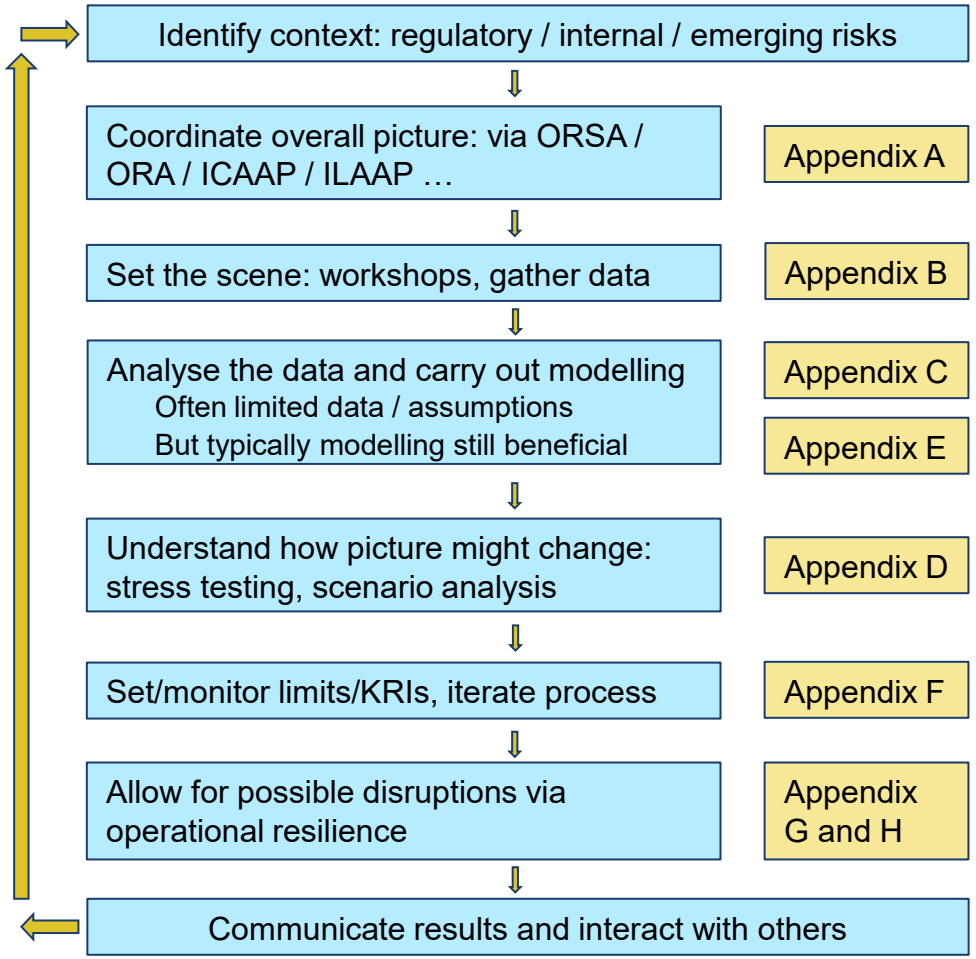
	Main updates
A. ORSA versus ORA (Insurers versus IORPs)	
B. Operational risk workshops	
C. Quantifying operational risk	Expanded
D. Stress testing and scenario analysis	
E. Coping with limited data	
F. Operational risk appetite, limits and Key Risk Indicators	
G and H. Operational resilience, including Digital Operational Resilience Act	NEW
I. Risk culture	NEW

Many other (actuarial) resources

- E.g. from member associations of the AAE such as output from the IFoA Operational Risk Working Party

Date	Link to paper
2024	Operational Risk Working Party - Validating Operational Risk Models | British Actuarial Journal | Cambridge Core
2020	Operational risk dependencies | British Actuarial Journal | Cambridge Core
2016	Good practice guide to setting inputs for operational risk models | British Actuarial Journal | Cambridge Core

Main roles of an operational risk manager



Some more specific (insurance) roles

- 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
- 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, including operational resilience management

Desirable skills (can fit actuaries well!)

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

SELECTED TOPICS

A. ORSA versus ORA (Insurers versus IORPs)
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
G. Operational resilience
H. Digital Operational Resilience Act
I. Risk culture

A. ORSA versus 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
- Model risk: potentially a large contributor to operational risk

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 are examples of a **loss distribution approach** (LDA) but with different levels of **expert judgement**. Expert judgement sources include:
  - Professional expertise (another reason for using actuaries?), 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
  - Other firms’ experience. More information provided in second edition on how these might be accessed or inferred, including for IORPs

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, i.e. apply credibility theory

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

F. Operational risk appetite, limits and KRIs

- 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 …

G. Operational Resilience

NEW IN 2nd Ed.

- **Risk identification**. Both internal and external risks
- **Impact Analysis**. On firm's operations, services and stakeholders
- **Critical Business Services**. Adequate documentation and agreed impact tolerances on each one
- **Recovery and Response Plan**. Ensure critical functions can be maintained or rapidly recovered
- **Testing and Exercising**. Essential to validate effectiveness
- **Vendor and Third-Party Management**. Operational resilience extends beyond firm's internal operations
- **Continuous Monitoring and Improvement**. Ongoing process, establish 'lessons learnt' mechanisms, stay updated on industry best practices etc.

H. Digital Operational Resilience Act (DORA)

NEW IN 2nd Ed.

- **Adoption**. By European Union in 2022. Complex piece of legislation. Establishes European Cybersecurity Agency (ESCO)
- **Scope**. All financial institutions subject to EBA or EIOPA supervision
- **Risk assessment**. Institutions must conduct risk assessment to identify and assess risks of cyberattacks and other operational disruptions
- **Mitigation measures**. To include security controls protecting IT systems and networks, plans to respond to cyberattacks etc., testing / exercising
- **Response plan**. Should include procedures for identifying and responding to cyberattacks, recovering from cyberattacks, communication with customers and other stakeholders
- **Reporting**. Any significant cyberattacks or operational disruptions to authorities.

I. Risk Culture

Why is a good risk culture important?	Risk actuaries – a pillar of a robust risk culture	Steps to achieve a good risk culture	Power of a Speak-up culture	Harness cognitive diversity
Customer trust	Quantitative risk analysis, regulatory compliance	**Top-down commitment, incentivization**	Empowers employees	Broadens risk perspective
Regulatory compliance	Pricing and product development	**Continuous training, open communication**	Supports diverse perspectives	Challenges status quo
Operational efficiency	Scenario and stress testing	**Risk appetite definition**	Encourages accountability	Innovates in risk strategies
Reputation management	Capital management	**Periodic reviews**		Provides resilience in adversity
Employee moral and retention	Stakeholder communications	**Engage external stakeholders**		

NEW IN 2nd Ed.

N.B. Currently a particular regulatory emphasis on risk culture in banking

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
  - How to address limited data?
  - Importance of operational resilience and of having a good risk culture
- Actuarial skills very relevant
- Detailed topic coverage in nine appendices

Thank you!

- Contact details: malcolm.kemp@nematrian.com