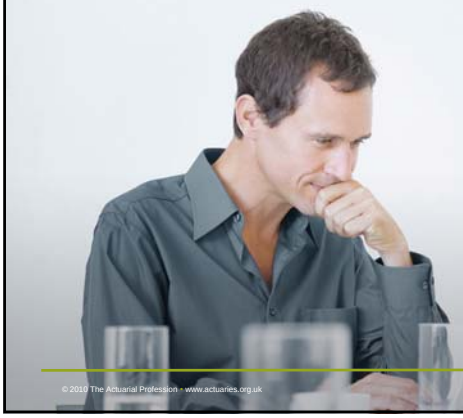
The Actuarial Profession
making financial sense of the future

Life conference and exhibition 2010
Andrew Shiels, avantage (UK) Ltd and Sandy Trust, KPMG LLP



# An Introduction to Operational Risk

7-9 November 2010



## Introductions and what we're going to talk about …

- What is operational risk ?
- Operational risk framework
- Governance and oversight
- Operational risk lifecycle:
  - Identification
  - Assessment
  - Control
  - Monitoring and reporting
  - Risk appetite
  - Stress testing and scenario analysis
- Operational risk capital modelling

1

The Actuarial Profession
making financial sense of the future

# What is Operational Risk?



## Before defining 'Operational Risk' what do we mean by 'Risk'?

- The British Standard on Risk Management defines "risk" as, *"something that might happen and its effect(s) on the achievement of objectives."*
- This echoes a Standard which had been used in Australia and New Zealand, AS/NZS 4360:2004, which spoke of "risk" as being, *"the chance of something happening that will impact objectives."*

## Before defining 'Operational Risk' what do we mean by 'Risk'?

- In Chinese, the concept of risk is represented by two characters, which 'translate' as **danger** and **opportunity**. The characters for 'crisis' (rather than danger) are ***wei ji*** and the characters for 'opportunity' are ***ji hui*** – so, the character ***ji*** forms part of the concepts for crisis and opportunity.
- Conceptually, the Chinese understood the twin sides of risk many centuries ago!

4

## How do we define 'Operational Risk'?

The most widely used definition of 'operational risk' used in the financial services industry is the one published by the Basel Committee on Banking Supervision :

**Operational Risk**

The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

**Sub-categories of operational risk**

| | |
|---|---|
| People | Includes: fraud; breaches of employment law; unauthorised activity; loss or lack of key personnel; inadequate training; inadequate supervision. |
| Process | Includes: payment or settlement failures; documentation which is not fit for purpose; errors in valuation/pricing models and processes; project management failures; internal/external reporting; (mis)selling. |
| Systems | Includes: failures during the development and systems implementation process, as well as failures of the system itself; inadequate resources. |
| External events | Includes: external crime; outsourcing (and insourcing) risk; natural and other disasters; regulatory risk; political risk; utilities failures; competition. |

5

## Operational Risk – the "New Kid on the Block"?

Although Operational Risk is still considered to be the "new kid on the block" by many people, it's still the category of risk most likely to impact your organisation unexpectedly and often in a major way …

6

The Actuarial Profession
making financial sense of the future

## Examples of High Profile Operational Risk Events

7

## People Risk - Example

### Trader Pleaded Guilty to Fraud

Nick Leeson was a former derivatives trader whose unauthorised and unsupervised trading on the Singapore International Money Exchange caused the collapse of what was at the time the United Kingdom's oldest investment bank, Baring's Bank.

An audit in February 1995 uncovered losses that amounted to more than GBP 800 million, almost the entire assets of the bank. Dozens of executives who were implicated in the failure to control Leeson resigned or were sacked. Leeson pleaded guilty to fraud and was sentenced to six and a half years in prison.

A similar incident happened at Société Générale where an unsupervised trading loss incident in January 2008 caused the bank to lose approximately EUR 4.9 billion.

8

## Process Risk - Example

### Westpac's Costly Mistake

According to the Herald Sun, in June 2009, Westpac had mistakenly sent a fax authorising a transfer of NZD 3.47 million into a computer firm's account, even though the actual amount owed was only NZD 34,680.

A Westpac spokesperson put the mistake down to a "simple typing error" when sending the fax. Westpac made a very similar but costlier data processing error only one month earlier when an NZD 8 million transfer was made instead of NZD 80,645. In that case, the account holders fled with the money and Westpac wasn't able to recover all of its losses.

9

## Systems Risk - Example

### Barclays Technology Crash

In June 2009, UK-based Barclays PLC experienced a technology breakdown that left millions of customers, primarily in the South of England, unable to withdraw money from ATMs for most of the afternoon. Barclay's internet and telephone banking services were also impacted and a small number of customers experienced difficulty using their cards to make payments at retailers.

10

## External Events Risk - Example

### Squirrel Brings Down the NASDAQ

In August of 1994, the NASDAQ market had to close for more than half an hour, losing valuable trading time, as an energetic squirrel had gnawed through the power lines supplying the stock market's computer centre in Trumbull, Connecticut. The system failed to perform the automatic switchover to the temporary backup power supply and consequently the market was down for 34 minutes.

11

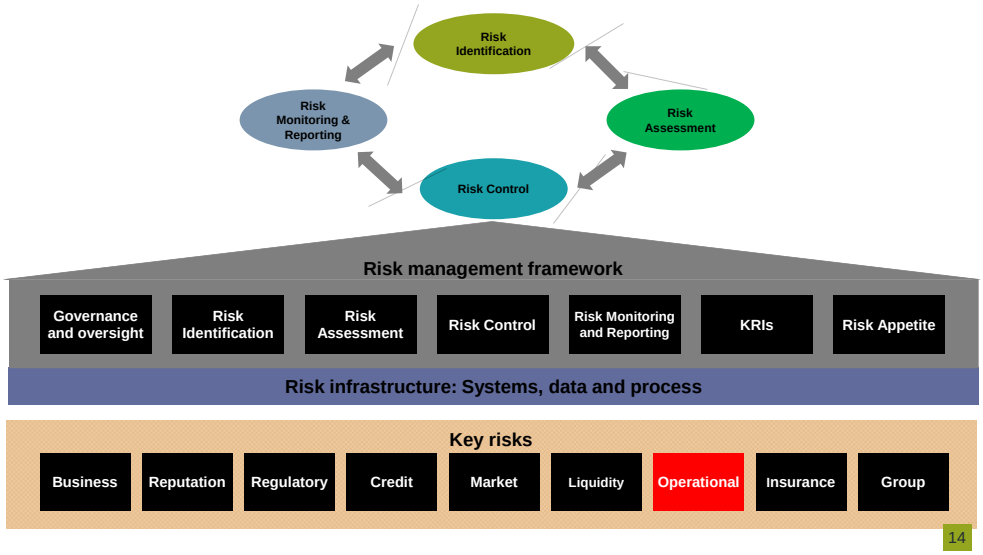
The Actuarial Profession
making financial sense of the future

# Operational Risk Framework



## Operational Risk – Key Building Blocks

## Operational Risk Lifecycle




14

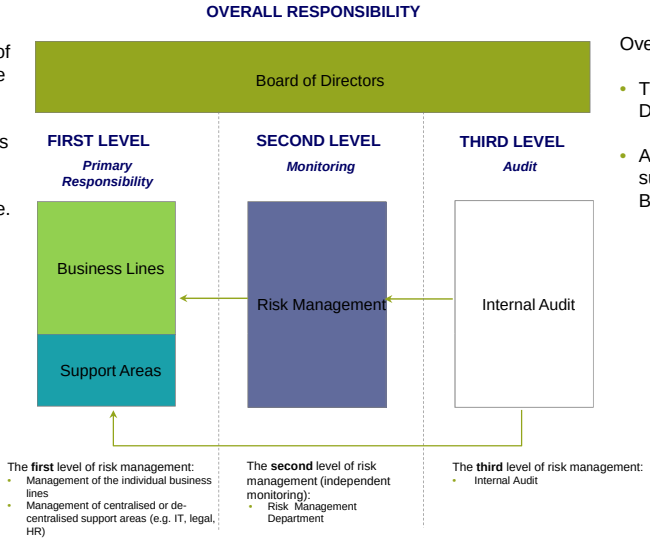
The Actuarial Profession
making financial sense of the future

## Governance and Oversight

15

# The Traditional 'Three Lines of Defence Model

- In the three lines of defence model the primary responsibility for managing the risks in the business is devolved to the business unit / line.



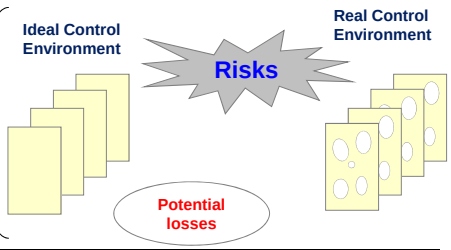

Overall responsibility:

- The Board of Directors
- A committee supporting the Board of Directors

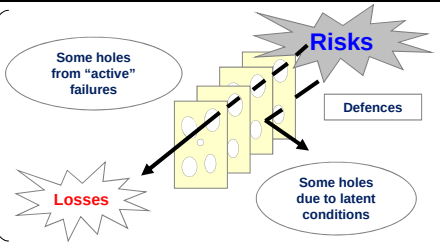
16

# "Swiss cheese model" – Major Op Risk events

- "Swiss cheese" analogy – holes exist in all systems
- Risk of accidents can be mitigated by developing effective "defences-in-depth"
  - Successive layers of protection each designed to protect against the possible breakdown of the one in front
- Defensive control layers try to minimise occurrence of large organisational accidents




- "Major" OpRisk events more unlikely as they require alignment of holes in successive control layers
  - e.g. bad person; flawed systems; poor management; weak controls, on a bad day . . .




17

## Specific Challenges of Operational Risk Management

Operational risk is a young discipline. It is the softest of risks, difficult to grasp, yet only too familiar. Establishing an effective operational risk management framework in a firm is not easy and open to many challenges, including:

- Getting the Board on Board
- Achieving buy-in throughout the firm
- Why colours and not numbers ?
- Why model operational risk ?
- How can you set a risk appetite for operational risk ?
- Reporting challenges …



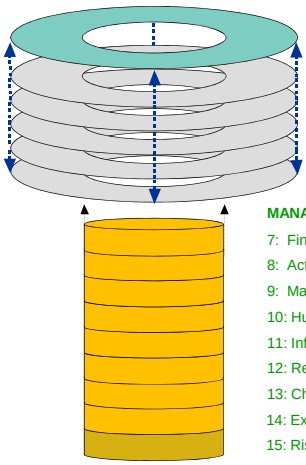


The Actuarial Profession
making financial sense of the future

## Operational Risk Identification

# Identification of Strategic and Objective Core Processes

**Level 1 Processes**



**OPERATING PROCESSES**

1: Develop Vision and Strategy
2: Develop and Market Products
3: Distribute Products and Services
4: Process New Business
5: Service Policies
6: Settle Claims

**MANAGEMENT AND RESOURCE PROCESSES**

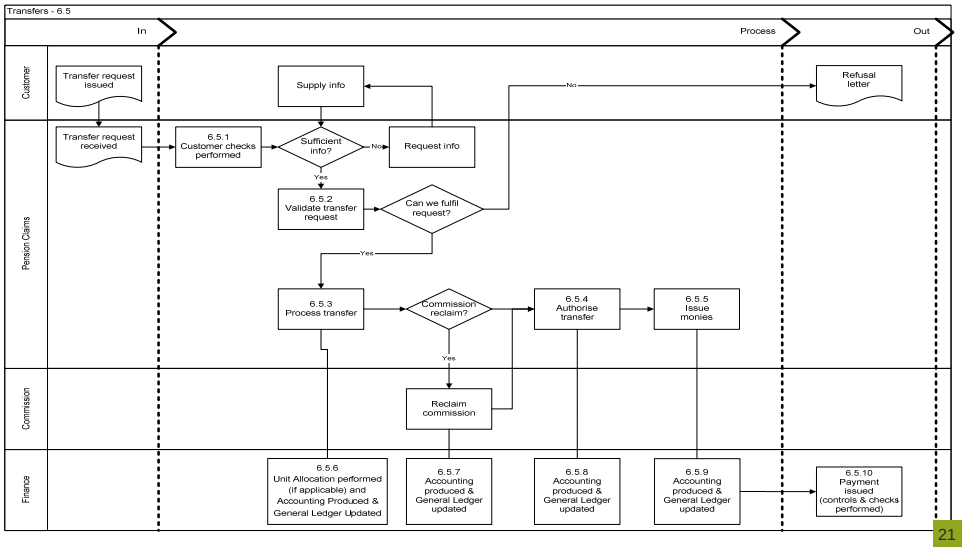
7: Financial Management and Reporting
8: Actuarial Reporting
9: Management Information
10: Human Resources
11: Info Technology/Info Systems
12: Regulatory and Complaints Management
13: Change Management
14: External Relationship Management
15: Risk Management (including IS and BC)

**Level 2 Sub-Processes Example: 'Settle Claims'**

6.1 Medical claims, including CI / WPB / CPB / PHI
6.2 Surrenders/Withdrawals – Deal with customer request to cash in all or part of the current value of their policy
6.3 Deaths – Deal with the notification of customer death, updating all records and paying out benefits where applicable according to the terms of the contract
6.4 Maturities/Retirals – Pay out the relevant benefits at the relevant time to the entitled person and terminate all records
6.5 **Transfers – Deal with customer requests to transfer all or part of their benefits to another provider within PSO guidelines**
6.6 Annuities – Ensure payments are made for the correct amount at the correct time

20

# Typical Process Map




21

# The Cause and Effect Relationship of Risk

CAUSE → EVENT → EFFECT (OR CONSEQUENCE)

| Year | Cause | Event | Effect/consequence |
|---|---|---|---|
| **1986** | Dangerous design of reactor and control rods; unauthorised changes to procedures; inadequate safety culture. | **Chernobyl nuclear reactor disaster.** | Severe release of radioactivity (4 times Hiroshima bomb) across Russia and Europe (60% in Belarus) ; evacuation and resettlement of 336,000 people; probable 4,000 additional deaths from cancer. |
| **2001** | Illegal meat imports; failure to comply with regulations by one farmer; lack of resources for cull; failure to appreciate changes in patterns of movements of animals around the UK. | **Foot and mouth crisis (UK).** | 4 million sheep and cattle slaughtered and burnt; world-wide ban on exports of British livestock and meat; UK tourism suffered an £8-£9bn loss in 2001 as countryside and tourist attractions involving animals were closed; UK government suffered £3bn cost in tax lost and compensation paid. |
| **2003** | New and contagious form of atypical pneumonia. | **SARS near-pandemic in 37 countries.** | Air travel restricted; quarantine; disinfectant arrangements. |

22

# Typical Operational Risk Matrix

| | |
|---|---|
| Level 1 Process | Settle Claims |
| Level 2 Sub process | Transfers (Ref 6.5) |
| Process Objectives | Deal with customer requests to transfer all or part of their benefits to another provider with PSO guidelines |
| Associated Policy(ies) | CSD Policies (tbc)<br>Finance Policies (tbc) |

| Key steps | Func. | Risk cat. | Key risk events | Key controls | Ref. sources | Freq | Control type | Control cat. | Resp. | Delegated to | Evidence | CSA | | Action plan ref |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | Design | Perf. | |
| 6.5.1 Customer Checks | | | | ?? | Procedures | Ad-hoc<br>Daily<br>Weekly<br>Twice per month<br>Monthly<br>Etc... | Prevent<br>Detect<br>Automated<br>Manual | Oper.<br>Fin<br>Compl. | | | | S | S | |
| | | | | ?? | Procedures | Ongoing | Prevent<br>Detect<br>Automated<br>Manual | | | | | S | S | |
| 6.5.2 Validate transfer request | | | | | | Ongoing | Prevent<br>Detect<br>Automated<br>Manual | | | | | | | |
| 6.5.3 Process Transfer<br>(Hand-off to 6.5.6) | CSD | | | ?? | Procedures | Ongoing | Prevent<br>Detect<br>Automated<br>Manual | | | | | S | S | |
| | | | | ?? | Procedures | Ongoing | Prevent<br>Detect<br>Automated<br>Manual | | | | | S | S | |
| | | | | ?? | Procedures | Ongoing | Prevent<br>Detect<br>Automated<br>Manual | | | | | S | S | |
| 6.5.4 Authorise Transfer<br>(Hand-off to 6.5.7) | | | | ?? | | | | | | | | S | S | |
| | | | | ?? | | | | | | | | S | S | |
| | | | | | | | | | | | | S | S | |
| | | | | ?? | | | | | | | | | | |

23

The Actuarial Profession
making financial sense of the future

# Operational Risk Assessment

## Operational Risk Assessment

- Often undertaken in a 'Workshop' environment, involving relevant management and staff
- More sophisticated organisations may score likelihood and impact using electronic voting software
- Scoring of likelihood usually expressed simply (e.g. high / medium / low) or using probability percentage (%) score
- The scoring of risk impact may be undertaken on different levels – e.g. impact on business plan achievement; reputational damage; financial impact; regulatory impact (e.g. fines/censure); impact on customers etc.

## Operational Risk Assessment

- Many organisations multiply probability by impact to produce overall rating, which is used to rank risks
- Scores are often assigned for both gross (inherent) and residual (net) risk exposure
- Risks showing a sharp decline in probability between gross and net scores usually indicate that heavy reliance is placed on the associated controls – these controls are of particular interest during Internal Audit testing and whilst performing Control Self Assessment (CSA).

## Scoring Operational Risk Impacts – Example Metrics

| Impact | Financial | Customer | Reputation |
|---|---|---|---|
| | *Potential or actual loss which affects either the Profit & Loss Account or Balance Sheet (i.e. loss of profit or loss of asset).* | *Actual or potential impact arising from either operational failure or management failure which leads to an inability to:*<br>•Provide a quality service to our customers; OR<br>•*Execute our business; OR*<br>•*Comply with laws, regulations or policies and procedures.* | *Actual or potential impact to the reputation of 'Bank X' in the external environments, UK and Overseas. This includes the views held by all the regulatory bodies that regulate any element of our Group's businesses or activities.* |
| **Discloseable** | Discloseable Internal (to Group Audit Committee): Above £80m, below £400m<br>Discloseable External (to Shareholders): Above £400m<br>All Discloseable Risks are assessed for financial impact only. | | |
| **Major** | Between £10m and £80m | 1. Affecting more than 25% or more of a business's customers or staff.<br>2. Total failure of major third party supplier.<br>3. Loss of key system for a trading day or failure to meet a business critical process deadline e.g. CHAPS.<br>4. Management failure at an Executive level. | 1. High likelihood of (or actual) **formal censure** by any of our Regulators.<br>2. Concerted, widespread or recurrent critical coverage of the Group or of the specific Event in the national media. |
| **Significant** | Between £1m and £10m | 1. Affecting between 5% and 25% of a business's customers or staff.<br>2. Partial failure of a third party supplier.<br>3. Loss of key system which causes a significant operational or customer impact.<br>4. Management failure at an operational level. | 1. Any event which may affect our standing with any of our Regulators.<br>2. An Event that may (or has) damage (d) relations with consumer bodies, trade associations.<br>3. Individual press reports in national media that Group Communications consider to be of material concern to the Group. |
| **Important** | Between £100k and £1m | 1. Affecting up to 5 % of a business' customers or staff.<br>2. Deteriorating performance of a 3rd party supplier.<br>3. Loss of key system which causes a minor operational or customer impact.<br>4. Management failure at a unit or supervisory level. | 1. An Event that may (or has) tarnish(ed) our reputation with any significant customer group, 3rd party or our Regulators.<br>2. Actual adverse comment in local press or the equivalent that Group Communications consider to be of material concern to the Group. |
| **Minor** | Between £10k and £100k | 1. Affecting a small number of users of a single product or service.<br>2. Deteriorating performance of a non-critical 3rd party supplier.<br>3. Loss of a non-key system which causes a minor operational or customer impact.<br>4. Management failure at a unit or supervisory level. | 1. An Event that may tarnish our reputation with any significant customer group, 3rd party or our Regulators.<br>2. Threat of adverse comment in local press or the equivalent that Group Communications consider to be of material concern to the Group. |

The Actuarial Profession
making financial sense of the future

# Operational Risk Control

## Control Self Assessment

- Regular process
- Performed by risk owners
- Focus on control design and control performance
- Different types of controls, e.g.: preventive and detective
- Control design may suddenly become ineffective between quarters, due to changes in business structure, personnel, products or services offered
- Fully documented audit trail (ideally electronic document storage)
- It is vital to follow-up on any control weaknesses highlighted and also to incorporate the results in management reporting
- Results should feed in to Internal Audit Programme

29

## Dealing with Residual Operational Risk Exposure – The "4 T's"

- **Transfer** – e.g. insure the risk via a third party, instead of carrying the burden
- **Treat** – enhance controls / introduce new controls
- **Tolerate** – accept the risk exposure as part of the risk appetite
- **Terminate** – stop undertaking the activity which gives rise to that risk

30

The Actuarial Profession
making financial sense of the future

## Operational Risk Monitoring & Reporting

# Development Operational Risk Appetite

## Risk Appetite

*The risk of loss that a firm is willing to accept for a given risk-reward ratio [over a specified time horizon at a given level of confidence]*

The clause in brackets gives more precision and is often included in definitions of risk appetite by more sophisticated firms which are further down the road of risk modelling

**Operational risk appetite** may be expressed in a number of ways :

- Qualitative statements of appetite (often linked to policy documents)
- Articulation of accepted levels of risk against existing thresholds
- Expression of acceptance of £x losses per annum, or over a rolling period
- One of the most common approaches is to establish limits / thresholds against key operational risk categories and monitor via a suite of Key Risk Indicators (KRIs)
- NB – Historical loss data can be of great use in helping an organisation to calibrate its risk appetite limits and thresholds

32

# Risk Appetite v Risk Position at Individual Risk Level

**DESCRIPTION OF RISK – Security – Physical & Logical**
Failure to hold data securely, leading to unauthorised use of customer data to harm 'Bank X' customers or 'Bank X' through fraudulent activity.

| Risk Description | Customer | Reputation | Financial | Ability to Operate |
|---|---|---|---|---|
| | Personal data security compromised leading to potential fraud against customer | Loss of customer data likely to be highly publicised | Risk of loss through litigation and direct costs of reimbursing customers | Risk that privileged users could impact systems and risk of closure whilst responding to incidents. |
| **External Inputs** | **Customer** | **Reputation** | **Financial** | **Ability to Operate** |
| Peer group-Good practice | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| Regulatory Compliance | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| External Incidents | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| **Internal Inputs** | **Customer** | **Reputation** | **Financial** | **Ability to Operate** |
| Control testing | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| Managed Security | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| Policy Standards | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| SARBOX testing | Accept Important | Accept Important | Accept Minor | Accept Important |
| Internal Audit & Risk Issues | Accept Important | Accept Important | Accept Important/Significant | Accept Important |
| | **Customer** | **Reputation** | **Financial** | **Ability to Operate** |
| Risk Appetite | Accept Important | Accept Important | Accept Important/Significant (Individual/Aggregate) Incident) | Accept Important |
| Risk Position | Risk of SIGNIFICANT incidents | Risk of SIGNIFICANT incidents | Risk of SIGNIFICANT/MAJOR incidents | Risk of SIGNIFICANT incidents |
| GAP Analysis | Risk position outside appetite | Risk position outside appetite | Risk position outside appetite | Risk position outside appetite |

# Monitoring Operational Risk Appetite against Current Risk Position

**The table below shows a summary of the risk appetite and risk position for Technology Division for each major activity undertaken.**

| Components | Customer | Reputation | Financial* | Ability to Operate |
|---|---|---|---|---|
| CONTINUITY | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min |
| SECURITY: PHYSICAL & LOGICAL | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min |
| PROJECTS & CHANGE | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min |
| MANAGING OPERATIONS | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min |
| MANAGING PEOPLE | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min | RA / RP — Maj Sig Imp Min |

*** Financial Risk Appetites and Positions shown are aggregate positions (over 12 months) – not individual incidents**

**Key**

Risk position is within risk appetite

Risk position exceeds risk appetite

34

# Process Risk: Trade Instruction Error

RA / RP — MINOR | MODERATE | SERIOUS

**KEY RISK**: With regard to investment decision and transaction processing : the risk of incorrect/missing trade instructions and/or trade instructions not properly executed and/or allocated.

**ACTION REQUIRED**: None.

**QUALITATIVE STATEMENTS OF RISK APPETITE:**

- The Partners have a low tolerance for trade instruction errors that result in a material detrimental financial or reputational impact for the firm.

**DETAILED RISK APPETITE**

| | Appetite | Position | RAG |
|---|---|---|---|
| IMPACT | MINOR | MINOR | |
| LIKELIHOOD | LOW | LOW | |

**MOVEMENTS IN RISK POSITION**

| | |
|---|---|
| LAST YEAR | MINOR |
| LAST QUARTER | MINOR |
| CURRENT | MINOR |
| TREND | ⟷ |

**KRIs**

| | Actual | T'hold | Limit | RAG |
|---|---|---|---|---|
| No of trade errors | x | 0 | 1 | |
| No of near misses *(TBC)* | x | x | x | |
| No of incorrect allocations | x | 1 | 2 | |
| No of trade instruction losses funded by the Firm | x | 1 | 2 | |

## Monitoring Op Risk Appetite against Current Risk Position : Establishing Limits and Thresholds

| Indicators | Units | Actual | Threshold | Limit | Risk Position Score | Previous Quarter |
|---|---|---|---|---|---|---|
| **People Risk : Inadvertent Employee Activity** | | | | | | |
| No of material breaches / errors | # | 0 | 3 | 6 | | |
| No of significant breaches / errors | # | 0 | 0 | 1 | | |
| No of complaints (specify topic) | # | 0 | 1 | 2 | | |
| No of complaints outstanding | # | 0 | 1 | 2 | | |
| No of client SLA / agreement breaches | # | 0 | 1 | 2 | | |
| **People Risk : Loss of Key Personnel** | | | | | | |
| No of staff resignations / departures | # | 0 | 2 | 3 | | |
| **Process Risk : Pricing / Valuation Error** | | | | | | |
| No of pricing errors | # | 0 | 2 | 4 | | |
| No of FSA reportable pricing errors | # | 0 | 0 | 1 | | |
| No of other material Unit Trust related errors | # | 0 | 1 | 3 | | |
| **Process Risk : Trade Instruction Error** | | | | | | |
| No of trade errors | # | 0 | 0 | 1 | | |
| No of near misses (TBC) | # | 0 | x | x | | |
| No of incorrect allocations | # | 0 | 1 | 2 | | |
| No of trade instruction losses funded by the Firm | # | 0 | 1 | 2 | | |
| **Process Risk : Corporate Action Error** | | | | | | |
| No of corporate action errors | # | 0 | 1 | 2 | | |
| No of losses funded by Firm | # | 0 | 0 | 1 | | |

## Examples of Regular Operational Risk Report Contents

| Section | Contents |
|---|---|
| Executive Summary | Allows for any summary analysis including, but not limited to: key themes: major issues; risk analyses; and actions for the reports included in the pack |
| Risk Profiles | A result of the risk and control assessment process. As a minimum includes: risk identified by the business mapped on a chart of financial impacts against likelihood of occurrence; the control effectiveness for those risks; movements from the previous report |
| Control Improvement Plans | A result of the risk and control self assessment process. Required for all risks that: have a 'Qualified' or 'Requires Improvement' rating; or have moved significantly since the previous report |
| Key Risk Indicators (KRIs) | Reports the performance of the KRIs for the given period. As a minimum includes: KRIs for the top risks grouped by risk category and identified as predictive or lagging current period data and movement from the previous period scoring or rating. |
| Aged Actions | Reports on all actions captured from the various risk processes (e.g. risk maps, incident reports, internal audit reports etc.) that are overdue. As a minimum captures: actions that are overdue from their original due date; accountability for the actions |
| Incidents | Reports on the incidents and their respective loses for the period. As a minimum, includes: a summary of the major incidents for the period |
| Emerging issues | Captures emerging issues and potential events that require action. The purpose of this section is to highlight future events that are not captured as part of the risk profile but which cannot be ignored. |

37

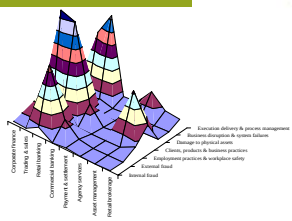
## Examples of Operational Risk Reporting Formats

**Risk Plotting Charts**

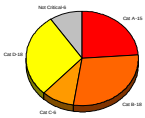
**RAG Status Reports – 'Top 10' Risks**


**CRSA Action Plans**

**Risk Surfaces**



**Risk Exposure Pie Charts**



**Functional Risk Hot Spots**

38

## Operational Risk Stress Testing and Scenario Analysis

- **Stress testing** and **scenario analysis** are essential tools for a firm's planning and operational risk management processes
- **Stress testing** is generally described as the **shifting of a single parameter**. In an operational risk context, this can be taken to refer to either the occurrence of a single risk, such as internal fraud or a system failure, or to the movement of a factor which may affect or does affect the firm as a whole, such as a significant increase in interest rates or a significant equity market downturn

39

## Operational Risk Stress Testing and Scenario Analysis

- By contrast, **scenario analysis** is about simultaneously **moving a number of parameters** by a predetermined amount, based on statistical results, expert knowledge and/or historically observed events
- Stress tests and scenarios are not forecasts of what is likely to happen ; they are deliberately designed to provide **severe, but plausible, possible outcomes**. They are necessarily forward looking and therefore involve an element of judgement
- They are invaluable techniques, particularly during periods of expansion, by providing a useful basis for decisions, when none is available from other sources.

40

## Stress Testing and Scenario Analysis – Live Case Study

Business Units, RMs, Credit, Strategy, Finance, Treasury, Risk

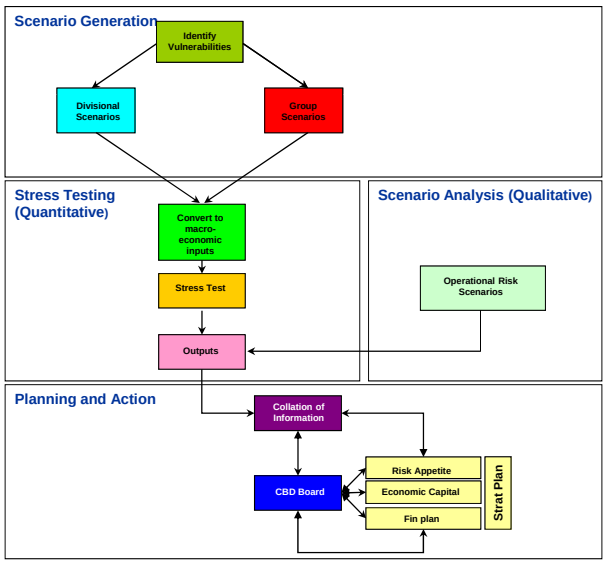
Group Economics

Risk Modelling Team to co-ordinate across Risk, Finance & Treasury

**Risk, Finance & Treasury**

Divisional Strategy

Divisional Board




41

## Some 'Top Tips' for Managing Operational Risk …

- Obtain full senior management support towards Operational Risk initiatives
- Demonstrate to the business some of the benefits of effectively managing Operational Risk (e.g. reduced losses, lower regulatory capital, increased risk awareness and the ability to price risk)
- Incentives should be built in to the system
- Ensure consistency in the system – e.g. in relation to the definition of operational risk, risk categorisation and key risk indicators

42

## Some 'Top Tips' for Managing Operational Risk …

- The right people should be involved in the process (e.g. in terms of training, motivation, attitude and cultural fit)
- The reporting process should be dynamic, rather than static ("cut and paste" approach), seeking improvement in measures and controls
- The results should be shared with all business areas
- Supplement your active management of Operational Risk through the use of insurance, business continuity planning and having a strong internal audit function.

43

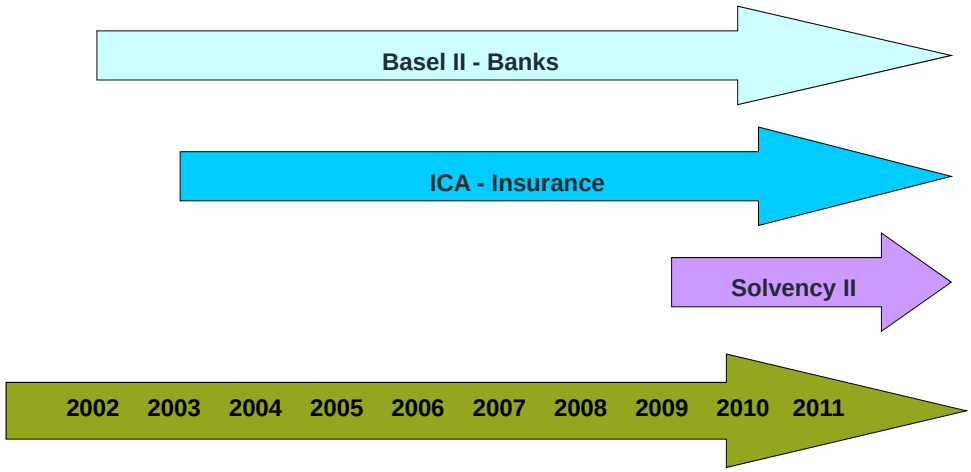
# Operational Risk Capital Modelling



## Operational Risk Capital Modelling
## Content

- Background
- Issues
- Potential Approaches
- Risk Identification
- Operational Risk Capital Modelling Techniques
  - Risk Event Scenarios
  - Modelling Loss Data
  - Stylised Scenario
- Operational Risk and Solvency II

## Operational Risk Capital Modelling
### Background



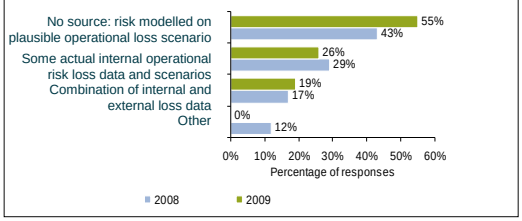

## Operational Risk Capital Modelling
### Issues

- Data
  - What is the data?
  - Low frequency/high severity – high frequency/low severity
  - Appropriateness of loss data
- Model Risk/Model Error
- Correlations
  - Validation
  - Symmetry
- Spurious Accuracy

# Operational Risk Capital Modelling
## Potential Approaches

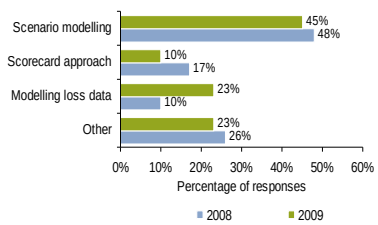
- Operational risk is still regarded as a key area for improvement in insurers ICA calculations
- Companies are looking to improve their operational risk model capabilities (i.e. moved to modelling loss data)
- More advanced Operational risk modelling capabilities is expected to lead to less capital

Graph: Source of Operation Risk Loss Data




*Source: KPMG Technical practices survey*

Graph: Approach used to quantify operational risk capital




*Source: KPMG Technical practices survey*

# Operational Risk Capital Modelling
## Identification of Risks

- Key to identify all the risks the firm is exposed to
- Internal workshops with key stakeholders/SMEs
- External databases
- Risk register
- Categorise by:
  - People, processes, systems & external events
  - By Business Division
  - By key process or function

# Operational Risk Capital Modelling
## Example Risk Register

| Operational Risk Scenarios |
|---|
| **Administration** |
| **Business continuity:**<br>- Failure or loss of key infrastructure<br>- Other |
| **Ineffective Claims Management:**<br>- Claims mishandling<br>- Delays in payment of claims |
| **Client retention** |
| **Company Specific risks** |
| **Credit rating drop** |
| **Failure to set appropriate strategy** |
| **Fraud** |
| **Inadequate Exposure Management** |
| **Inappropriate Underwriting** |
| **Incomplete data** |
| **Incomplete documentation** |
| **Investment mishandling/management:**<br>- Reluctance or Inability of investment counterparties to make payments |
| **IT (systems and control):**<br>- Breach of IT Systems licences/intellectual property/service contracts<br>- Failure of core processing system<br>- Loss of IT systems /infrastructure/ servers/ communication networks. |

| Operational Risk Scenarios |
|---|
| **Legal:**<br>- Failure to follow appropriate regulations<br>- Ineffective governance structure<br>- Other |
| **Mis-selling** |
| **Outsourcing** |
| **Pension scheme** |
| **People:**<br>- Failure of key service providers to deliver service levels to Franchisee<br>- Impact changes in Group on staff<br>- Other |
| **Project failures** |
| **Regulatory** |
| **Reinsurance:**<br>- Inappropriate reinsurance purchase<br>- Incorrect reinsurance recoveries |
| Reputational risk |
| Tangible asset damage |
| TCF (mis-pricing) |
| Unforeseen tax costs |

# Operational Risk Capital Modelling
## Risk Event Scenarios (1)

**STEP 1**

Develop a comprehensive operational risk register – may contain several hundred risks

**STEP 2**

Divide these individual granular risks into a smaller number of categories (say 6 or 8)

**STEP 3**

Develop adverse but plausible scenarios to provide coverage of the critical OR issues taking into account materiality and relevance

**STEP 4**

Estimation of financial impact of scenarios (both in terms of payments to policyholders and additional costs to company)

**STEP 5**

Diversification. Consideration of correlations between risk types.

**STEP 6**

Aggregated Operational Risk capital requirements. Potential additional capital?

| Description |
|---|
| People |
| Compliance, Legal, Health & Safety |
| Fraud |
| Operational Infrastructure |
| etc |

# Operational Risk Capital Modelling
## Risk Event Scenarios (2)

**STEP 3**

Develop adverse but plausible scenarios to provide coverage of the critical OR issues taking into account materiality and relevance.

Key to provide rationale for scenarios chosen and link to risk register.

| Operational Infrastructure Example Scenario |
|---|
| **A new product recently launched is received well in the market. This results in an unexpected increase in new business volumes at a level of five times over the projected sales plan. The business is unable to service the increased volumes within existing resource levels and systems capacity leading to a breach of the IFA charter (causing reputational damage), breach of the customer charter, increase in processing error rate, quality of service standards drop. The increase in people required to use the system also causes system failure. This causes Enhanced annuity and FIA annuity payments to be manually paid, leading to errors identified at a later date as overpayments of annuities to policy holders for two months.**<br><br>**In addition, an error in the unit pricing spreadsheets was not picked up in the quality control process as staff and management were overloaded. This error led to products being incorrectly priced, causing an increase in the number and amount of claims versus what we anticipated.** |

**STEP 4**

Estimation of financial impact of scenarios (both in terms of payments to policyholders and additional costs to company)

**Detailed consideration of impacts and costs to provide aggregate cost of this scenario**

# Operational Risk Capital Modelling
## Risk Event Scenarios (3)

**STEP 4**

Estimation of financial impact of scenarios (both in terms of payments to policyholders and additional costs to company)

| Mitigation – A possible approach |
|---|
| **- Each risk is allocated an exposure measure reflecting the level of mitigation for each risk given the level of control surrounding it.**<br><br>**- For example: allocate a mitigation reduction to the financial impact for each rating.** |

| Rating | Mitigation/ Reduction |
|---|---|
| 1 | 0.2 |
| 2 | 0.4 |
| 3 | 0.6 |
| 4 | 0.8 |
| 5 | 1.0 |

**STEP 5**

Diversification. Consideration of correlations between risk types.

**?**

- Can be difficult to ascertain correlations between scenarios so one approach to model between OR categories
- Should the correlation matrix be symmetrical
- Data for correlations must be collected
- Suitability of external data?

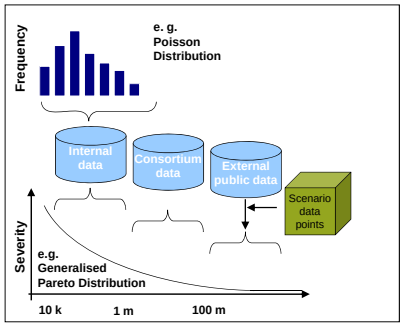
**STEP 6**

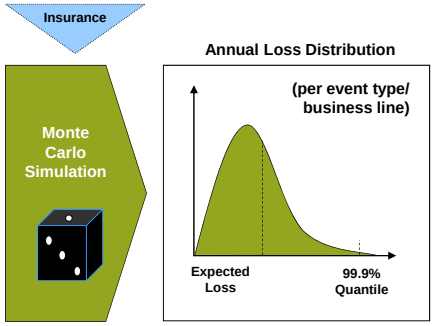
Aggregated Operational Risk capital requirements. Potential additional capital?

- Full risk register
- Documentation of linkage between risk register and scenarios
- Adverse, plausible and specific scenarios
- Detailed analysis of costs
- Documentation of discussions, methodology, correlations etc

# Operational Risk Capital Modelling
## Modelling Loss Data (Frequency & Severity)

- Internal and external loss data is used as primary model input.

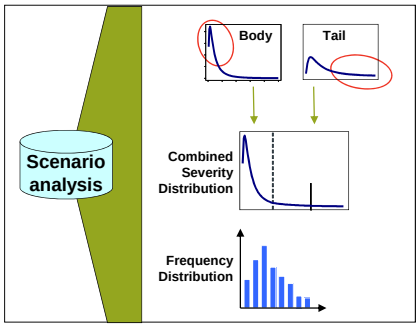


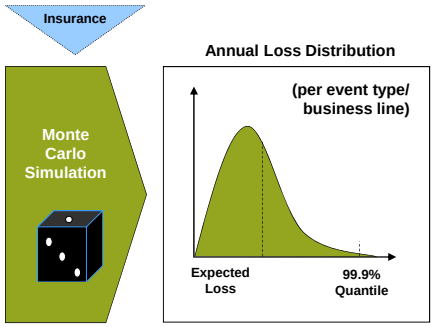




- Frequency and severity are modelled separately
- Different data sources cover different parts of the severity distribution
- From the aggregated loss distribution required risk figures are derived
  - expected loss
  - VaR (e.g. 99.9%)

# Operational Risk Capital Modelling
## Stylised scenario based approach

- Mainly data obtained from scenario analyses serves as model input.




- Frequency and severity are modelled separately
- Scenarios are described as ranges or average and worst case, including BE/IC* factors
- Body and tail of the severity distribution are modelled separately
- From the aggregated loss distribution required risk figures are derived
  - expected loss
  - VaR (e.g. 99.9%)

** Business Environment and Internal Control*

# Operational Risk and Solvency II
## Standard Formula

**Calculation**

| | |
|---|---|
| SCRop = | min{30%*BSCR; Oplnul} + 25%*Expul |
| Oplnul = | max{Oppremiumsl Opprovisions} |
| Oppremiums= | 4%*(Earned premiums for Life & SLT Health less earned premiums for UL business) |
| | + 3%*(Earned premiums for Non Life & Non SLT Health) |
| | + max{0, 4%*(change in Life (exc UL) earned premiums} |
| | + max{0, 3%*(change in Non Life earned premiums} |
| Opprovisions= | 0.45%*(Technical provisions for Life & SLT Health less technical provisions for UL business) |
| | + 3%*(Technical provisions for Non Life & Non SLT Health) |
| | + max{0, 4.5%*(change in Life (exc UL) technical provisions} |
| | + max{0, 3%*(change in Non Life technical provisions} |

| Risk | QIS4 | Final Advice | QIS5 |
|---|---|---|---|
| Technical Provisions – Life & SLT Health | 0.3% | 0.6% | 0.45% |
| Technical Provisions – Non-Life & Non SLT Health | 2.0% | 3.6% | 3.0% |
| Premiums - Life | 3.0% | 5.5% | 4.0% |
| Premiums – Non-Life | 2.0% | 3.8% | 3.0% |
| Unit Linked expense factor | 25% | 25% | 25% |
| BSCR cap – Life & Non-Life | 30% | 30% | 30% |

# Operational Risk and Solvency II
## Standard Formula - Comments

- **The current SF for operational risk is formulaic and linked to the level of technical provisions and premiums**
- **The SF calibration has been widely criticised for the following reasons:**
  - **It is too simplistic and is not risk sensitive**
  - **Rewards low pricing and reserving**
  - **Doesn't take into account the quality of the risk management framework**
  - **Doesn't reflect the wide spectrum of operation risks that can materialise**
  - **Doesn't allow for diversification against other risk components**
- **CEIOPS have indicated that the SF will not be appropriate for some companies' risk profiles and may lead to the situation of a company not holding enough capital**
- **A challenge for the regulator will be to explain to companies why an internal operational risk model is not adequate for their business given the weaknesses in the SF operational risk calibration – particularly in the case where the internal operational risk assessment leads to a higher SCR than the SF**

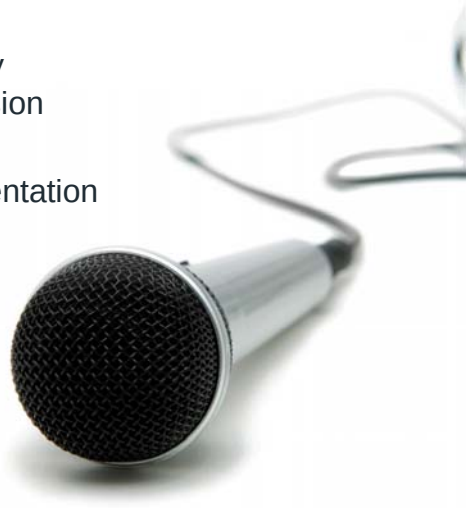
## Operational Risk and Solvency II
## Internal Model – some thoughts

- Meeting the Use test
- Validation
- Ensuring statistical quality standards are satisfied:
  - Choice of distribution (fat tailed – lognormal, gamma, weibull, pareto)
  - Choice of model – Lognormal and generalised pareto as part of extreme value theory are popular
  - ORIC recommends negative binomial for frequency but poisson most popular
  - Scaling to external data?
- Data quality standards
  - Internal, External, Op Risk Scenarios
- Expert Judgement
  - Has it been used?
  - How to validate?
  - Can it be back tested?
- Aggregation
- Allocation of capital to business lines
- Profit and Loss Attribution – split between risk types
  - Eg a lapse risk or an operational risk?

## Questions or comments?

Expressions of individual views by members of The Actuarial Profession and its staff are encouraged.

The views expressed in this presentation are those of the presenter.





59