

An introduction to Operational Risk

John Thirlwell

Finance Dublin, 29 March 2006

- Setting the scene
 - What is operational risk?
 - Why are we here?
- The operational risk management framework
- Basel and the Capital Requirements Directive

Setting the scene -
what do we mean by
operational risk?

Basel II definition of operational risk

“The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk” (Basel II, para 644)

Originated from the BBA/ISDA/RMA 1999 Survey

- Attempt to be positive, i.e. not to say “everything except credit and market risk”
- Not intended as a bounded definition but to indicate the **scope** of OR
- A definition for regulatory capital rather than risk management purposes.

Other issues of definition

- Strategic (or business) risk – should they be included within operational risk?
- Where does reputation risk fit in?
- Where does reputation risk fit in to

CAUSE → EVENT → EFFECT ?

Credit risk	Market risk	Liquidity risk	Insurance risk	Group risk	Operational risk
-------------	-------------	----------------	----------------	------------	------------------

Credit risk	Market risk	Liquidity risk	Insurance risk	Group risk	Operational risk
Operational controls	Operational controls	Operational controls	Operational controls	Operational controls	

Is operational risk different
from other risks?

Is operational risk different from other risks?

	Credit risk/ Market risk	Operational risk
Is the risk transaction-based?		
Is the risk assumed proactively ?		
Can it be identified from accounting information eg the P&L?		
Can occurrence of the risk (all risk events) be audited?		
Can its financial impact be bounded or limited?		
Can you hold a position in the risk, i.e. can you close out or sell the risk?		

Another way of looking at it – What keeps you awake at night?

Loss of reputation

Product liability

Physical damage

General liability

Failure to change/adapt

Terrorism

Business interruption

Failure of key
strategic alliance

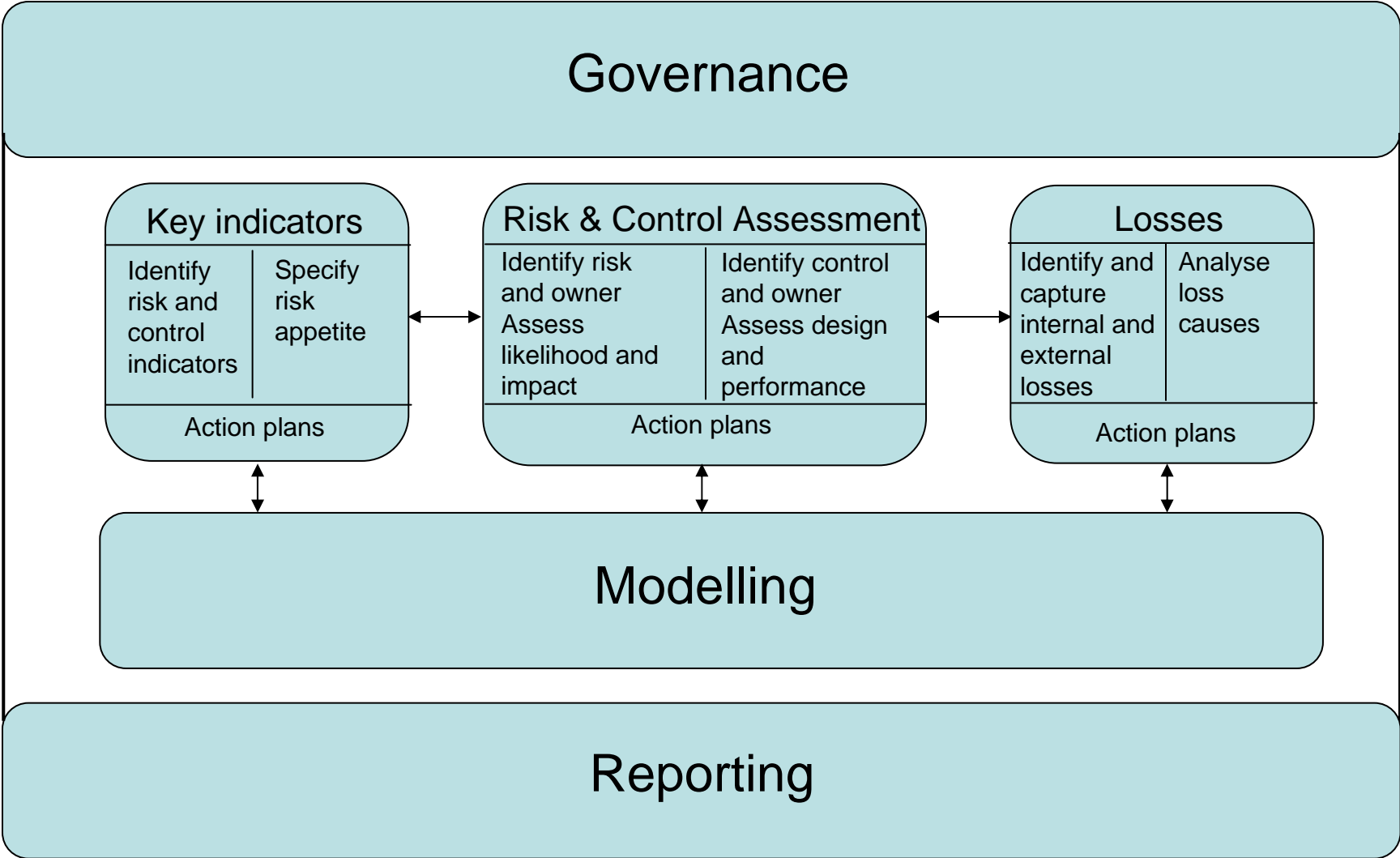
Employee retention

Computer crime

Political risk

... 75% not transferable – but
manageable

ORM Framework



Loss event data

Attributes of loss event data

- **Loss category**
- **Amount – the basis of severity**
- **Date – the basis of frequency**
- Business activity, business unit
- Geographical location
- **Cause - narrative**
- **Effect/impact**

Issues and decisions concerning loss data

- **Reporting threshold**
- **Near misses**
- **Indirect costs and costs to fix**
- Business interruption
- Foregone income
- **Offsets and gains**
- **“Boundary” losses**

Realities of loss event data

- It will be incomplete, be scarce and patchy
- It will be inconsistently reported although, once reported, it *is* auditable.
- It is historic and backward looking. Major events will probably have led to tighter controls, change of policy etc.
- It does not, of itself, tell you about **causes**.

But it can . . .

- Focus management attention on areas of activity that are giving rise to losses
- Validate risk self-assessments, scenario analysis, key risk indicators and capital allocation.
- It is therefore extremely useful as *information*.

External data is similar – only more so . . .

Realities of external loss data

- Pooled, e.g. BBA GOLD, ORX, ABI and national data pools
 - All the concerns of internal data
 - As with internal data, its construction and nature will depend on the purpose for which it is gathered (e.g. benchmarking; raw data; causal; modelling; informing scenario analysis)
 - Different risk, control and reporting cultures
 - Exclusions (e.g. legal, insurance settlements)
 - Scaling?
- Public data (e.g. FitchRisk, Aon (insurance claims), Willis)
- The use of external data
 - provide *information*
 - enhance OR management rather than measure “severe” losses
 - “External data is in the realm of *scenario analysis*” - Roger Cole, Chairman Basel Risk Management Group.

Risk self-assessment

Risk self-assessment

- Essentially a matrix to assess the frequency/probability and severity/impact of the risks which have been identified.
- Involves some degree of scoring - from traffic lights (red, amber, green) or H,M,L to larger number of grades and mathematical extrapolation. Ideally, should be minimum of 4 grades.

Assuming some metrics are used, these will be “logarithmic” . . .

Matrix parameters - example 1

Frequency	
<i>Definition</i>	<i>Expected frequency</i>
Almost impossible	< 1 x 10 years
Rare	Between 1 x 1 yr and 1 x 10 years
Very unlikely	Between 1 x 1 month and 1 x 1
Unlikely	year Between 1- 5 x 1 month
Likely	Between 5 – 9 x 1 month
Very likely	> 9 x 1 month
Severity	
<i>Definition</i>	<i>Loss range</i>
Very severe	> 1000k
Severe	100k – 1000k
Moderate	10k – 100k
Small	1k – 10k

What should impact relate to?

- assets?
- income?
- sales?
- capital?

But there's a missing ingredient . . .

Control risk self-assessment

- Two assessments are required
 - Assuming controls work (net)
 - Assuming controls fail (gross)
- The final result will provide
 - A league table of risk exposures, which will drive management action and provide the basis for cost-benefit evaluations of new controls
 - A risk map for senior management
 - The basis for Sarbanes-Oxley sign-off
 - Feeds to internal and external auditors regarding the effectiveness or weaknesses in controls

Frequency and severity – Traditional ORM

High (3) Frequency	3	6	9
Med (2)	2	4	6
Low (1)	1	2	3
	Low (1) Severity	Med (2)	High (3)

Frequency and severity - modern ORM

High (3) Frequency		n/a	n/a
Med (2)			n/a
Low (1)			
	Low (1) Severity	Med (2)	High (3)

Practical challenges

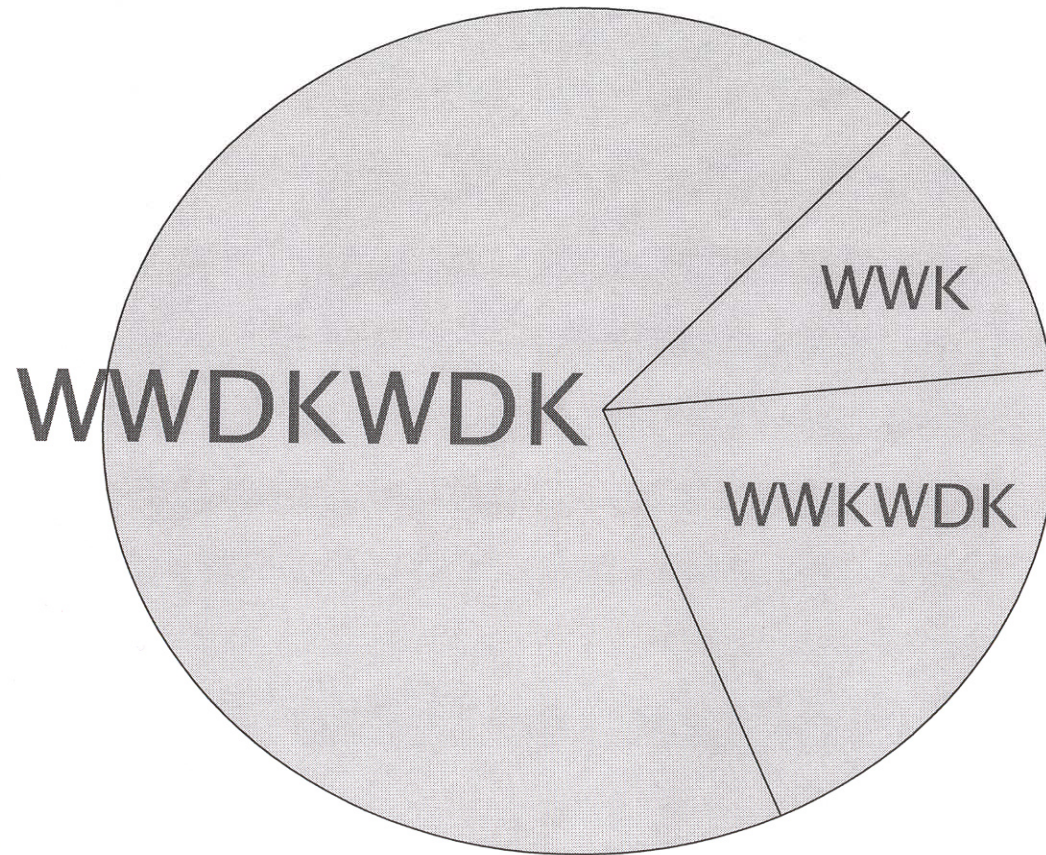
	Losses	Control risk self assessment
Objective (past)	Y	N?
Subjective (forward looking)	N	Y
Quality analysis by:	Finance	Management
Quantity available	Low?	Tailored
Collection time	Long	Short
Source	Accounts, but . . .	Management

Scenario analysis

Scenario analysis

- Uses the same process but attempts to move outside the box.
- Involves looking at uncertainties and extending the range of unexpected.
- Is intended to:
 - Derive reasoned assessments of plausible severe losses
 - Evaluate potential losses arising from multiple simultaneous loss events
- Rumsfeld territory

An Uncertain World



not forgetting **WWDKWK**

Context dependency – the past as a guide to the future

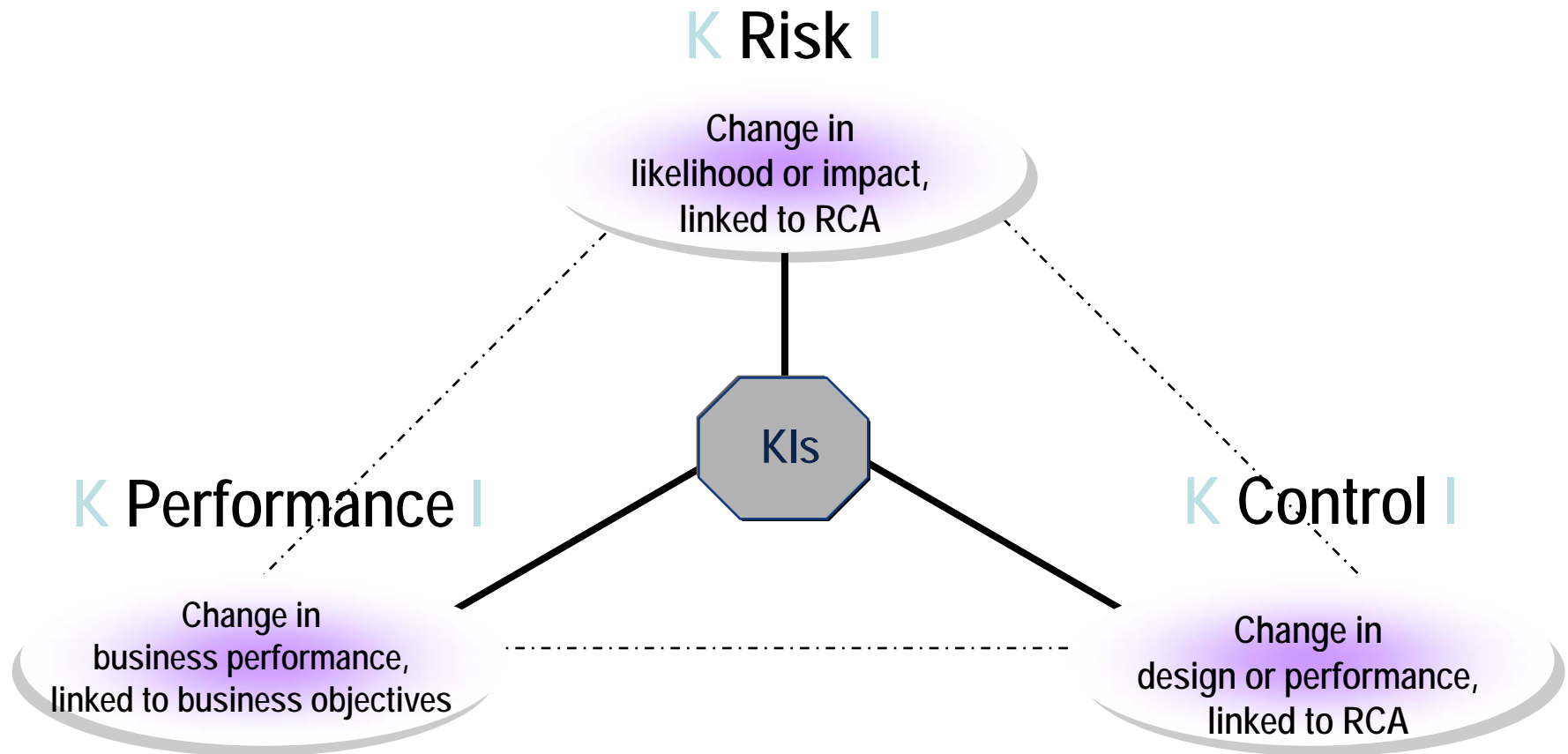
- There's always a tendency to look at the future as an extension of the past.
- Are your businesses, people or processing systems similar to 10 years ago?
- Are the threats to those systems similar to 10 years ago?
- How relevant, therefore, are your internal and especially external loss data in compiling scenarios?
- The higher the context dependency, the less the past will be a good predictor for the future.

Key risk indicators

What is (and is not) a KRI

- Observed or calculated values used to show the state of a risk which is considered key
- A warning light of future risk exposure
- Identifies factors which have not yet become events
- Enables early detection and management of unacceptable risk in each function or process against predefined tolerance levels
- Should be a meaningful driver of risk (ie related to *causal* factors)
- NOT:
 - A predictor of future risk severity or frequency
 - An indicator of control or control failure
 - An indicator of business performance

Indicators



Working with the business

- Talk to the business about its risks and its current indicators. Which indicators are significant?
- Use workshops, the risk assessment process, audit reports, past incidents to unearth indicators
- Separate risk, control and performance indicators
- 60% to 70% of indicators for key risks are in the businesses already

NB Indicators must lead to behavioural *change* and/or force *action*.

Examples of indicators

Risk:
Client default on loan

Control:
Credit Scoring

RI:
Number of defaults

CI:
Number of clients with high credit scores

KPI:
Number of defaults by clients with high credit scores

Risk:
Loss of staff

Control:
Suite of training courses for staff to choose from

RI:
Number of staff leaving

CI:
No. of staff not attended a training course within last 6 months

KPI:
Number of staff leaving without attending a training course within last 6 months

Risk indicators - an Audit Committee perspective

NB almost all Y/N

[Audit Committee Institute (KPMG) – Shaping the Audit Committee agenda, May 2004]

Inappropriate tone at the top	Unusually rapid growth
Frequent organisational changes	Unusual results or trends
High turnover of senior mgt	Industry softness or downturns
Lack of succession plans	Interest rate or currency exposures
Inexperienced management	Exposure to rapid technological changes
Lack of management oversight	Late surprises
Management over-ride	Autocratic management
Overly complex organisational structures or transactions	Ongoing or prior investigations by regulators or others
Untimely reporting and responses to audit committee enquiries	Excessive or inappropriate performance-based compensation
Unrealistic earnings expectations (by firm or financial community)	Lack of transparency in business model and purposes of transactions

Quantification

Quantification and the 99% problem

- Under the AMA, banks should achieve “a soundness standard comparable to a *99.9% confidence interval over a one year period.*”
- Methodology to include *internal and external loss data, scenario analysis* and factors reflecting the *business environment and internal control systems.*

Advanced Measurement Approach - quantitative criteria (Basel)

Basel is the same as the CRD with one important difference:

- “. . . There may be cases where estimates of the 99.9th percentile confidence interval . . . would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases scenario analysis and business environment and control factors may play a more dominant role in the risk measurement system.” [para 669(f)]

Quantification and reporting

- Losses
 - incomplete
 - many high frequency, but low impact
 - few low frequency, high impact
 - not forward looking
- Risk self-assessment
 - subjective assessments
 - forward looking over capital time horizon and can assume confidence interval
 - Allowing for correlations (subjectively assessed) can form the basis of a capital assessment
- Indicators
 - forward looking but don't predict severity or frequency of risk exposure

Achieving the soundness standard – possible approaches

- Scaling
- Stress testing
- Scenario analysis
- Back testing
- Boot-strapping

Probably should have been Pillar 2 after all,
which is all about an assessment of . . .

Operational risk management

- Management issues
- Risk appetite
- Risk culture

OR Management issues

- Where does OR sit in the organisation?
 - Central or decentralised in the business lines?
 - Is it ‘independent’? Should it be?
- What is its relationship to
 - Board and senior management (do they understand OR?)
 - CEO (sign-off ICAAP)
 - Risk director
 - Compliance and/or internal audit
 - Insurance purchasing
 - Business continuity
- ‘Use test’ – is OR truly integrated with firm’s risk management system, including capital allocation?

Risk appetite and operational risk

- Can a cap/limit be put on OR?
- Is zero reasonable – or meaningful?
- Must an “appetite” be capable of measurement, i.e. be a metric?

- If or where the answer is NO to the above, what do we mean by risk appetite? How do we manage it?
- Risk indicators can form the basis for a practical expression of risk appetite.

Operational risk culture

- An OR culture is what you get after a successful implementation of a framework, where everybody in the organisation is aware about operational risk.
- OR management tools should be part of the business lines' lives – the true 'use test'.
- OR should be part of any business decision.
- An OR culture should create shareholder value through loss reduction, increased revenues and lower regulatory capital.
- The tone will come from the top.

If there is no culture of operational risk in the firm, there will be no meaningful operational risk management.

John Thirlwell

+44 (0)20 8386 8019

info@johnthirlwell.co.uk