# Operational Risk Management in Insurance Companies

John Thirlwell

Director, Operational Risk Research Forum

City & Financial, London, 2 November 2004

- The context: What does operational risk really mean?
- Regulatory expectations
- The operational risk framework

# The regulatory "definition" - a reminder

- Operational risk [*has been described as* (SYSC 3A.1.1G)][*refers to* (PRU 2.3.29G)] "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."
- Basel II repeats this, with provisos for legal risk, strategic risk and reputational risk.
- CP190, CP195 and CP04/7 were silent.

# What do *you* mean by operational risk?

- Issues of definition
  - Legal risk. Includes regulatory fines.
  - Strategic and business risk.
  - Reputational risk. Almost always a consequence of events *caused by other risk types*, but OR is probably the main source. Takes years/decades to build and moments to lose.

- What is your firm's definition?

# Risk identification and classification

- Sources for classification:
  - Basel II
  - FSA: PSB, Policy Statements, CPs, Arrow framework
  - Lloyd's
  - British Bankers' Association
  - ABI (to come?)

# Scope of operational risk (1)

Internal fraud

– unauthorised activity; theft (assets/IP), embezzlement, fraud, insider trading (not on firm's account)

External fraud

– theft and fraud; systems security

Employment practices and workplace safety

– employee relations; safe environment; discrimination

Damage to physical assets

– including natural disasters

Business disruption and system failure

– hardware, software, telecom, utility outage

# Scope of operational risk (2)

Clients, products & business practices

– product suitability (incl. KYC); fiduciary breaches; privacy breaches; lender liability; improper trade/market practices; money laundering insider trading (firm's account); product defects; model flaws; disputes over advisory activities; exceeding client exposure limits

Execution, delivery & process management

– transaction capture, execution and maintenance; data entry; delivery failure; collateral management failure; monitoring and reporting (incl. external); documentation failures; customer/client account management; trade counterparties' disputes, non-performance; vendors and suppliers outsourcing and disputes

*[Full details available from BIS (www.bis.org) and/or BBA (www.bba.org.uk) websites]*

# Operational risk systems and controls (SYSC3A3)

Should cover, amongst other things:

- Employees
- IT and manual systems
- Direct *and indirect* losses arising from OR
- Tangible, immediate, quantifiable and intangible, delayed, difficult to quantify (e.g. reputational damage)
- Outsourcing risks
- External events

# More SYSC headings – all operational risk

- People
  - Employee responsibilities
- Processes and systems
  - Internal documentation
  - External documentation
  - IT systems
  - Information security
  - Geographical location
- External events and other changes
  - Expected changes
  - Unexpected changes and business continuity management
- Outsourcing
- Insurance

# Examples of OR for stress and scenario tests (PRU2.3.31G)

- Fraud
- Pension under-funding
- Technology
- Reputation risk
- Marketing and distribution risks
- Legal risks
- HR – management; strikes; resourcing of key functions; adequacy of resources

# A few they forgot from CP 04/7

- Adequacy of policies and procedures – risk of non-application
- Internal audit
- Business continuity / disaster recovery
- Political interference; taxation; confiscation of assets

# What is different about operational risk?

- Often difficult to identify from management information and reporting systems:
  - P&L – explicit, e.g. fraud
  - P&L – implicit, e.g. OR amounts mixed with other expenses such as consultancy fees (indirect losses); OR in trading or credit losses
  - Not in P&L – lost future revenues; project failure or delay
  - A lot of OR events are *hidden*
- Much of OR is difficult to identify and assess because it's a 'soft' risk which goes beyond transactions or process, especially the loss events which really bite.
- Much of OR is difficult to control - people and external events (e.g. fire, flood, pestilence, business environment)
- It is risk-based, rather than control-based – compare and contrast Sarbanes-Oxley.

# Regulatory expectations - ECR, ICAs and flying pigs

- ECR – minimum risk-based capital requirement (cf Basel Basic and Standardised formulaic approaches)
- ECR – the heroic assumption:

  "a BBB rating . . .[which equates to] a 99.5% confidence level that a firm will survive for a one-year period."

  NB no similar *explicit* assumption in CP195 or CP04/7, but
- "We envisage that, for intervention purposes, ICG will be set taking into consideration capital consistent with a 99.5% confidence level over a one year period . . ." (PS 04/16 5.3, and similar in PRU 2.3.14)

# Confidence level

- Cf. Basel II, Advanced Measurement Approach: "comparable to that of the internal ratings-based approach for credit risk (i.e. comparable to a one year holding period and a 99.9% confidence interval)" [but note 669 (f)]
- Was 2001 a year in a 100?
- How confident are we with insurance risk to 100, 200 year time horizons, especially where data is sparse and/or heterogeneous? 4 x Florida windstorms = 500 year event
- Institute of Actuaries GIRO report 'Quantifying operational risk in general insurance companies' (March 2004) – statistical curve-fitting; probability distribution; EVT; stochastic differential equations; Bayesian networks; expert (fuzzy logic etc). Causal modelling probably the answer but a lot of work to do.

# What do regulators want?

- Capital
- Risk management
- Regulatory compliance

# Regulatory expectations of capital - ICA, ICG et al

- Identify the major sources of risk
- Consider the extent to which capital is an appropriate mitigant for the risks identified and assess the amount and quality of capital required.
- Stress tests; scenario analyses; aggregation; confidence level.
- ICGuidance and Pillar 2/Arrow. NB for banks, Pillar 2 can only be additive.

# ICAs and operational risk

- Data limitations and lack of high powered analysis tools acknowledged, so limitations to quantitative analysis.
- Combination of quantitative and qualitative tools accepted. But management must make a judgement of capital adequacy.
- "A firm may consider that investigation of operational weaknesses and corrective action is a better response than holding capital and may consider that a certain degree of risk is within its pre-defined risk tolerance." (Draft PRU 2.4.33G)

# Regulatory expectations of risk management - cf banks

- Board and senior management involved in oversight of the OR framework
- An OR system that is conceptually sound and implemented with integrity
- Sufficient resources in major business lines, control and audit areas
- Policies documented
- OR management function – codify policies and procedures; design and implement OR assessment and reporting (to unit, senior management, Board)
- Systematically track internal loss data
- Validation and independent review

# The operational risk framework

- Risk identification and classification
  – generic or business based?
- Risk assessment
  – Internal and external loss data
  – Scenario analysis
  – (Control) risk self-assessment
  – Key Risk Indicators
  – Risk appetite and tolerance

# Internal loss event data – some health warnings and issues

- Completeness – most loss data of any interest does not flow from the General Ledger. It has to be manually identified and reported, whatever threshold is chosen. Its completeness cannot be audited.
- Consistency – common understanding of the loss categories
- Near misses (happened, but something prevented the loss being realised), profits etc
- What's so interesting about losses? Causes are what matter.
- But losses validate self-assessment, KRIs, stress tests etc

# External loss data – more health warnings

- External data pools – health warnings
  - The pool must have a common purpose, e.g. benchmarking; raw data; causal; modelling; informing scenario analysis
  - Completeness – different internal structures, reporting thresholds, exclusions (e.g. legal, insurance settlements)
  - Control cultures
  - Scaling – a spurious accuracy
  - Validation
- Pooled versus public data (e.g. Aon, Willis, FitchRisk)
- The use of external data
  - provide *information,* rather than data
  - enhance OR management rather than measure "severe" losses
  - "External data is in the realm of *scenario analysis*" - Roger Cole, Chairman Basel Risk Management Group, Nice, 22 June 2004

# (Control) risk self-assessment

- Identification of risks and their assessment of frequency/severity through questionnaires, workshops etc, i.e. bottom-up
- Assessment should be validated by peers, audit, risk management etc
- Involves some degree of scoring - from traffic lights (or H,M,L, but should be 4 minimum) to larger number of grades and mathematical extrapolation
- Gross (assuming controls fail) and net (assuming they work)
- May lead to overall assess risk assessment but will filter into league table of highest risks for management action.
- Validated by loss event data (internal and external)

# Key risk indicators

- KRIs provide leading indicators
- Again should be bottom-up, for knowledge and buy-in – they should be meaningful drivers of risk, based on experience and involve the expert assessment of business areas.
- Whenever possible should be capable of being measured quantitatively and open to verification
  - some classics: staff turnover; errors; downtime; training objectives achieved
  - but can be softer: staff satisfaction; external views e.g. headhunters
- Reported to management/Board and tested against triggers, i.e. against a target range, which will be amber, so that better = green, and worse = red = ACTION

# Risk appetite and risk tolerance

- Quantitative or qualitative? Should be about management first, not measurement.
- Relationship to WTL?
- % of capital resources?
- Zero?
- Front page of the *Sun*
- Cf KRIs – is there an appropriate escalation process?

# 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, and manages it.
- OR management tools should be part of the business lines' lives.
- OR should be part of any business decision in providing a basis for risk assessment, including changes in strategy, new products/classes, re-engineering.
- An OR culture should create shareholder value through loss reduction increased revenues and lower regulatory capital.
- Senior management buy-in is critical.

# The biggest obstacles

- Lack of data – volume and quality
- Scale of project
- Difficulty in modelling OR
- Lack of awareness among staff; lack of communication
- Lack of senior management support

# Thank you, and good luck!

John Thirlwell

Tel: 020 8386 8019
E-mail: info@johnthirlwell.co.uk