An operational risk management framework for managing agencies

John Thirlwell

Director, Operational Risk Research Forum

Lloyd's Risk Forum, 28 May 2004

- Operational risk and its evolution
- Regulators and OR
- The banking experience
- Building blocks

What is operational risk?

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

(BBA/RMA/ISDA survey, 1999)

[Adopted by Basel Committee, with provisos that it includes legal (e.g. documentation) but not business or strategic risk *for minimum regulatory capital purposes*.]

What's different about operational risk?

- It's difficult to identify from standard accounts:
  - P&L – explicit, e.g. fraud
  - P&L – implicit, e.g. OR amounts mixed with other expenses such as consultancy fees
  - 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 is 'soft' risk, not always linked to transactions
- Much of OR is difficult to control, e.g. people and external events

How did it evolve?

- Year dot.
- Oil, engineering, manufacturing – process management
- 1988 – Piper Alpha, Lockerbie
- Financial sector events – Daiwa, Sumitomo, NatWest, Barings, AllFirst, Y2K, WTC
- Banks – 1995 +
- BBA, ISDA, RMA – 1997+
- Bank regulators, the new Basel Capital Accord and the ‘plug’ factor (1998 – 2008)
- Insurance – the next frontier

Regulators and banks – the Standardised Approach (1)

- OR system with clear responsibilities assigned to an OR management function.
- OR function responsible for: developing strategies to identify, assess, monitor and control/mitigate OR; codify firm-level policies and procedures; design and implement assessment methodology; design and implement OR reporting system.

Regulators and banks – the Standardised Approach (2)

- ". . must systematically track relevant OR data including material losses . ."
- OR assessment system must play a prominent role in risk reporting, management reporting and risk analysis.
- Regular reporting of OR exposures to business units, senior management, the Board.
- System subject to regular independent review and validation by internal and external auditors.
- Document, document, document.

Regulators and banks – the Standardised Approach (EU)

- No specific reference to a function, but similar requirements are there (policies, procedures, relevant data, losses etc), together with

- Costs and benefits of alternative OR management strategies to be undertaken
- Requirement for OR strategies to be implemented consistently throughout the whole organisation
- BCP

Individual Capital Assessments

- "a firm should consider the extent to which capital is an appropriate mitigant for the risks identified and assess the amount and quality of capital required." (CP 04/7)
- Stress tests; scenario analyses; aggregation; confidence level.

ICAs and operational risk (CP 04/7)

- 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)

Confidence level

- Basel – 99.9% for AMA, but could become 'target'
- CP 190 – 99.5% (= BBB?)
- Was 2001 a year in a 100?
- How confident are we with insurance risk to 100, 200 year time horizons?
- Insurance risk (by class) is relatively homogenous as to cause and effect. Operational risk (of large, infrequent events) involves sparse, heterogeneous data.
- 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.

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*

Reputation risk

- Almost always a consequence of events *caused by other risk types*, but OR is probably the main source.

Banks and OR

No programme	19%
< 12 months	16%
1 - 2 years	22%
> 2 years	43%

(Source: SAS/*Operational Risk* survey May 2004)

Tools	Implemented (%)	Implemented and/or implementing (%)
Internal loss database	59	83
Self-assessment	54	83
Internal reporting	43	77
Key Risk Indicators	24	69
Statistical modelling	19	48
External loss database	33	46

(Source: SAS/*Operational Risk* magazine survey May 2004)

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, telecomms, 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]

Examples of OR (CP 04/7)

- Fraud
- Technology
- Marketing and distribution risks
- Legal risks
- Outsourcing
- HR – management; strikes; resources - key functions, adequacy
- Adequacy of policies and procedures – risk of non-application
- Internal audit
- Business continuity / disaster recovery
- Political interference; taxation; confiscation of assets

‘Headings’ to consider in assessing OR (CP 04/7)

- Organisation
- Compliance
- Risk assessment
- Management information
- Employee and agents
- Internal audit
- Business continuity
- Processes and systems
- Group structure
- Policies, procedures and controls
- Human resources

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. Its completeness cannot be audited.
- Consistency – common understanding of the loss categories
- Near misses, profits etc
- What's so interesting about losses? Causes are what matter.
- But losses validate self-assessment, KRIs, stress tests etc

External loss event information – more health warnings

- External data pools
  - Common purpose – 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
- External data pools
  - provide *information,* rather than data
  - enhance OR management rather than measure "severe" losses.
- Pooled versus public data (e.g. Aon, Willis, FitchRisk, OpRisk Analytics (SAS)

(Control) risk self-assessment

- Identification of risks and their assessment of frequency/severity through questionnaires, workshops etc, i.e. bottom-up
- 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.
- What keeps you awake at night? What lets you sleep at night? What should keep you awake?

Appendix A. Correlation between frequency and severity

We suppose now that X_1, $X2$, ... are conditionally independent from N. We have $X|N \sim \mathcal{LN}(\mu(N), \sigma^2(N))$ with $\mu(N) = \mu + \alpha N$ and $\sigma^2(N) = \sigma^2 + \beta \times N$. We suppose that (N_1, N_2) have jointly a bivariate Poisson distribution (Johnson, Kotz & Balakrishnan, 1997). It means that $N_1 = N_{11} + N_{12}$ and $N_2 = N_{22} + N_{12}$ where N_{11}, N_{12} and N_{22} are mutually independent Poisson random variables with parameters λ_{11}, λ_{12} and λ_{22}. The correlation between N_1 and N_2 is:

$$\frac{\lambda_{12}}{\sqrt{(\lambda_{11}+\lambda_{12})(\lambda_{22}+\lambda_{12})}}$$

Given values for λ_1, λ_2 and $cor(N_1, N_2)$, then $\lambda_{11} = \lambda_1 - cor(N_1, N_2)\sqrt{\lambda_1,\lambda_2}$, $\lambda_{22} = \lambda_2 - cor(N_1, N_2)\sqrt{\lambda_1,\lambda_2}$ and $\lambda_{12} = cor(N_1, N_2)\sqrt{\lambda_1,\lambda_2}$. For the correlation between L_1 and L_2, we have:

$$cor(L_1, L_2) = e^{\lambda_1\left(e^{\alpha_1+\frac{\beta_1}{2}}-1\right)+\lambda_2\left(e^{\alpha_2+\frac{\beta_2}{2}}-1\right)}\left[e^{cor(N_1,N_2)\sqrt{\lambda_1\lambda_2}\left(e^{\alpha_1+\alpha_2+\frac{\beta_1+\beta_2}{2}}-e^{\alpha_1+\frac{\beta_1}{2}}-e^{\alpha_2+\frac{\beta_2}{2}}+1\right)}\right]\times$$

$$\left\{\sqrt{\lambda_1\lambda_2}+cor(N_1,N_2)\left(1+\lambda_1\left(e^{\alpha_1}+\frac{\beta_1}{2}-1\right)+\lambda_2\left(e^{\alpha_2}+\frac{\beta_2}{2}-1\right)\right)\right.$$

$$\left.\sqrt{\lambda_1\lambda_2}\,cor^2(N_1,N_2)\left(1-e^{\alpha_1+\frac{\beta_1}{2}}-e^{\alpha_2+\frac{\beta_2}{2}}+e^{\alpha_1+\alpha_2+\frac{\beta_1+\beta_2}{2}}\right)\right\}-\sqrt{\lambda_1\lambda_2}\Big]\times$$

$$\prod_{i=1}^{2}\left(\lambda_i e^{2\alpha_i+\beta_i}e^{\lambda_i\left(e^{2\alpha_i+\beta_i}-1\right)}+e^{\sigma_i^2+\beta_i}e^{\lambda_i\left(e^{2\alpha_i+2\beta_i}-1\right)}-\lambda_i e^{2\lambda_i\left(e^{\alpha_i+\frac{\beta_i}{2}}-1\right)}\right)^{\frac{1}{2}}$$

The correlations obtained with this framework are larger than the previous ones. However, they remain small. To give an idea of the level of correlations, we have computed the correlation (in per cent) with the Crédit Lyonnais risk measurement system. For that, we have introduced a parameter c that represents the proportion of the mean and the variance of the logarithm of X explained by the Poisson random variable.[4] Figure 3 represents the mean correlation. It is equal to 8% in the worst case ($c = 100\%$ and $cor(N_1, N_2) = 100\%$).

Key risk indicators

- Again should be bottom-up, for knowledge and buy-in
- Ideally will be measured quantitatively
  - the classics: staff turnover; errors; downtime
  - units should devise their own
- But could be softer – e.g. headhunter assessments
- KRIs provide leading indicators
- Risk (KRI) versus performance indicators (KPI)

Uses beyond risk assessment

- Mitigation
  - controls
  - policies
  - insurance (to be allowed for banks on AMA as a capital mitigant)
- Capital assessment and allocation
  - by syndicate?

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
- Lack of awareness among staff; lack of communication
- Scale of project
- Difficulty in modelling OR
- Lack of senior management support

Thank you, and good luck!

John Thirlwell

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