Operational risk and corporate governance

John Thirlwell

Director, Operational Risk Research Forum

Said Business School, University of Oxford, 22 July 2004

- The development of operational risk in banks and financial institutions
- Regulatory drivers
- The scope and nature of operational risk
- The regulatory approach and the operational risk management framework
- Some thoughts on operational risk and governance

Evolution of OR in the financial sector?

- Year dot.
- Oil, engineering, manufacturing – process management and controls; business continuity
- 1988 – Piper Alpha, Lockerbie
- Some financial sector events – Daiwa (1995), Barings (1995), Sumitomo Corp (1996), NatWest (1997), Y2K, WTC (2001), AllFirst (2001), SARS (2003), Nat Australia Bank (2004)
- Banks – 1995 +; BBA survey (1997)
- BBA, ISDA, RMA survey, 'Operational Risk: The Next Frontier' (1999)
- Bank regulators, the new Basel Capital Accord and the 'plug' factor (1998 – 2008)
- Insurance – the next frontier; investment management?

Regulatory definitions and drivers

- Operational risk "*has been defined as* the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." (FSA CP142 – OR systems and controls)
- Basel II repeats this definition, with provisos for:
  - legal risk
  - strategic and business risk
  - reputational risk
- Regulatory drivers:
  - systemic risk
  - capital
  - management
- Regulation: Basel Capital Accord (Basel II); EU Risk Based Capital Directive (CAD3); FSA PSB

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

Operational risk is different from other risks

- Market, liquidity, credit/counterparty, insurance, group
- Often difficult to identify from audited or management accounts:
  - P&L – explicit, e.g. fraud
  - P&L – implicit, e.g. OR amounts mixed with other expenses such as consultancy fees; 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 and goes beyond transactions or process.
- Much of OR is difficult to control or limit, e.g. people and external events
- It is risk-based, rather than control-based – compare and contrast Sarbanes-Oxley.

Sound Practices for the Management and Supervision of OR (BIS, Dec 2001)

1. Board awareness and responsibility for major aspects of OR; approve OR strategy and "tolerance" for OR.
2. Senior management – consistent implementation.
3. Consistent OR management culture through communication.
4. Identify, including for new products and activities.
5. Measure/assess
6. Monitor exposure and losses
7. Processes to control or mitigate

8/9. Supervisors to ensure compliance

10. Public disclosure

Regulatory expectations of banks
(Basel II)

- Board and senior management involved in oversight of the OR framework
- An OR system that is conceptually sound and implemented with *integrity* i.e. integral to bank's management process
- OR management function – codify policies and procedures; design and implement OR assessment and reporting (including escalation to senior management, Board)
- Sufficient resources in major business lines, control and audit areas
- Policies documented (i.e. transparency, disclosure, audit trails); but understanding?
- Systematically track internal loss data
- Validation and independent review

***

The interests of the Board, given their responsibilities to shareholders, are aligned with regulators' interests

The operational risk management framework

- Risk identification and classification
- Internal and external loss data
- Scenario analysis
- (Control) risk self-assessment
- Key Risk Indicators

Issues of (internal) loss event data collection

- 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.

  [The heroic assumption]
- Consistency – lack of 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

Issues of external loss event data

- External data pools
  - 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 (e.g. BBA GOLD; ORX) versus public (e.g. Aon; FitchRisk) data
- External loss event data
  - provide *information,* not quantifiable data
  - enhance OR management rather than measure "severe" losses
  - "[are] 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,
- 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)
- Produces overall risk assessment and may 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, rather than reporting of past problems
- Should be bottom-up, for knowledge and buy-in, and meaningful drivers of risk, based on experience and 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
  - cf Balanced business scorecards, 6 sigma etc
- 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

Some thoughts on OR and governance

- Sarbanes-Oxley is an OR issue (CEO Wachovia)
- OR management teaches you that you cannot
  - identify all the risks and losses you have
  - anticipate all the risks you may have
  - measure many of the above
- The culture of financial institutions generally is founded on their ability to identify, document, control and report risks. It is often said that OR today is no more than the centralisation of historic risk management, but it goes beyond controls and the process or transaction food-chain. Internal audit should ensure that policies are appropriate and implemented, which is also a wider remit than historically.
- UK financial institutions' Boards accept responsibility for risk management, even if driven to it by the FSA or Turnbull and the Combined Code.
- The age-old US/UK divide – prescription and rules vs guidance and principles (c.f. Basel, PSB). "Mutual recognition is not in the lexicon of the US."

John Thirlwell

e-mail: info@johnthirlwell.co.uk

Tel: 020 8386 8019

www.johnthirlwell.co.uk