

# Operational Risk and Corporate Governance

John Thirlwell

Director, Operational Risk Research Forum

Unicom, 24 November 2004, London

- Context
  - what is corporate governance and why does it matter?
  - the scope of operational risk
- The relationship between operational risk and corporate governance
- Using the operational risk management framework to improve corporate governance

- Context
  - **what is corporate governance and why does it matter?**
  - the scope of operational risk
- The relationship between operational risk and corporate governance
- Using the operational risk management framework to improve corporate governance

# Why corporate governance matters

- Investments in companies with highest quality of governance structures and behaviour significantly outperform those with the lowest
- Companies with the top 20% of governance scores are more profitable (avge ROE - 15.9%) than those in the bottom 20% (avge ROE – 1.5%)
- The higher the corporate governance score, the lower the equity-price volatility.

*Deutsche Bank analysis of FTSE 350 (2004)*

# Specialist analysts

- Governance Metrics International
- ISS - Corporate Governance Quotient

Work on the principle that better corporate governance will produce better results, and better returns for investors.

# What does corporate governance cover? – the Codes (ICAEW)

- Cadbury (1992)
- Greenbury (1995)
- Hampel – combined code (1998)
- Turnbull – internal controls (1999)
- Smith – audit committees (2003)
- Higgs (2003)
- The new Combined Code (effective end 2003)

# What do the Codes cover?

- Directors (exec, non-exec, Chairman)
- Remuneration (including dividend policy)
- Relations with shareholders/investors
- Relations with external auditors, consultants, regulators, media
- Risk management
- Assurance and control
- Supply and flow of information
- Ethical culture
- Disclosure of corporate governance arrangements

- Context
  - what is corporate governance and why does it matter?
  - **the scope of operational risk**
- The relationship between operational risk and corporate governance
- Using the operational risk management framework to improve corporate governance

# 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.”

*(PS Not intended as definition other than to be positive and to show scope)*

# Some issues of definition

- Legal risk. Includes regulatory fines
- Strategic and business risk. Excluded from the Basel regulatory capital definition – but the biggest, and what Op Risk management's about.
- 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. Management's response to a crisis will probably affect reputation more than the nature of the crisis itself.

# Scope of operational risk (Basel II)

Internal fraud

External fraud

Employment practices and workplace safety

Damage to physical assets (including natural disasters)

Business disruption and system failure

Clients, products & business practices

Execution, delivery & process management

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

# Operational risk systems and controls (SYSC3A3)

- Employees
- IT and manual systems
- Direct *and indirect* losses arising from OR
- Tangible, immediate, quantifiable *and/or* 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*
- Insurance

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

- Fraud
- *Pension under-funding*
- Technology
- *Reputation risk*
- Marketing and distribution risks
- *Legal risks*
- *HR* – management; strikes; resourcing of key functions; adequacy of resources
- Adequacy of policies and procedures – risk of non-application
- Internal audit
- *Change (management)*
- *Political interference; taxation; confiscation of assets*

- Context
  - what is corporate governance and why does it matter?
  - the scope of operational risk
- **The relationship between operational risk and corporate governance**
- Using the operational risk management framework to improve corporate governance

- In sum, the full scope of Operational Risk = business risk
- If corporate governance is a vital component of business management, it is also the starting point for Op Risk management
- Without the culture and control embodied by good corporate governance in the Boardroom, there will be no effective Op Risk management.
- “Maintaining a culture that values integrity and creates adequate controls is crucial . . . And the effort must start at the top.” *Governor Roger Ferguson, FRB Vice-Chairman, March 2002*

- Context
  - what is corporate governance and why does it matter?
  - the scope of operational risk
- The relationship between operational risk and corporate governance
- **Using the operational risk management framework to improve corporate governance**

# The operational risk *management* framework

- 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

*(Basel II - Standardised Approach and AMA)*

# The *practical* operational risk framework – building the dashboard

- Risk identification and classification – the scope (your choice; generic or business line; boundary issues)
- Risk assessment
  - Internal and external loss data
  - (Control) risk self-assessment
  - Scenario analysis
  - Key Risk Indicators
  - Risk appetite and tolerance

## Loss event data – some health warnings and Board issues

- Completeness – most data of any interest is not transaction-based and has to be manually identified and reported. Its completeness cannot be audited. Will the compensation policy militate against reporting?
- Data consistency – probably poorly reported, but at least internal audit can work on this.
- Near misses (i.e. it happened, but something prevented the loss being realised eg financial penalties waived), including non-financial eg health and safety – would have been electrocuted but); profits etc are all valuable
- Thresholds – all losses and Board reported losses?
- What's so interesting about losses? **Causes** are what matter. How are these identified and reported?

# (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.
- Peer review (including internal audit) plus validation by loss experience.
- Gross (assuming controls fail) and net (assuming they work)
- May lead to overall assess risk exposure assessment, but will filter into league table of highest risks for management/Board action.

# Scenario analysis and business strategy

- Similar approach to self-assessment but moves outside the box.
- Scenario analysis involves looking at uncertainties and extending the range of unexpecteds – classic strategic process
- Rumsfeld – wwk; wwkwk; wwdkwk – largest slice + wwdkwk – poor reporting system [cf Nassim Nicholas Taleb – black swans; why don't we learn that we don't learn; [www.fooledbyrandomness.com](http://www.fooledbyrandomness.com)]
- Scenarios are often multiple simultaneous loss events (ie beyond single risks)
- Always remember the difficulties of people – poor, poor mgt, poor decisions; inappropriate incentivisation, so system not pre-disposed to report (at bottom) or acknowledge issues (at top)
- Adds value if it drives management action

# Key risk indicators

- KRIs provide leading indicators *warning lights, not predictors of future*
- 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.
- 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 (as with all dashboard/reports)

# Risk appetite and risk tolerance

- Quantitative or qualitative? Should be about management first, not measurement.
- % of capital resources?
- Zero?
- Front page of the *Sun*
- Cf KRIs – is there an appropriate escalation process and/or early warning?
- Remember, you can't prevent many events which exceed your risk tolerance, but you can manage the consequences.

# 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. It's in the corporate bloodstream.
- 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. It will provide competitive advantage – you will cope; you will react well.
- Senior management buy-in is critical.

# Corporate governance checklist

- Directors (exec, non-exec, Chairman)
- Remuneration (including dividend policy)
- Relations with shareholders/investors
- Relations with external auditors, consultants, regulators, media
- Risk management
- Assurance and control
- Supply and flow of information
- Ethical culture
- Disclosure of corporate governance arrangements

# John Thirlwell

Tel: 020 8386 8019

E-mail: [info@johnthirlwell.co.uk](mailto:info@johnthirlwell.co.uk)

Web: [www.johnthirlwell.co.uk](http://www.johnthirlwell.co.uk)

[www.orr.org](http://www.orr.org)