Governance, Risk and Compliance
-
an NED's perspective

John Thirlwell

Guernsey FSC, 14 May 2009

Governance

- What do we mean by governance?
- Whose responsibility is it?
- Does it add value?

Governance principles

- Strategic objectives
- Set of corporate values
- Clear lines of responsibility and accountability
- Board members appropriately qualified
- Appropriate oversight by Board and senior management
- Internal and external audit and other control functions
- Appropriate compensation policies
- Transparency

[Source: Enhancing corporate governance in banks, BIS, 2005]

UK corporate governance – the path to the Combined Code

1992 Cadbury – corporate governance

1995 Greenbury – remuneration

1998 Hampel – review of Cadbury and Greenbury

1998 Combined Code of corporate governance

1998 Turnbull – internal controls

1999 Higgs - NEDs

2003 Smith – Audit Committees

2005 Revised Code of corporate governance

Corporate governance

(Higgs Report 2003)

- Board
  - role
  - effectiveness
  - committees
- Role of the Chairman
  - independence
  - Audit Committee
- Independent NEDs
  - more than 50% of Board to be *independent* NEDs
  - training
  - outside advice
  - remuneration
  - pre-appointment due diligence
- Comply or explain

Governance

- What do we mean by governance?
- Whose responsibility is it?
- Does it add value?

Governance and the Board/NEDs

- Oversight
- Fiduciary duty – to whom?
- Conflicts of interest
- Board effectiveness
- Strategy, objectives, policies
- Monitor and, if necessary replace, key executives
- Culture and tone; ethical values

Governance risk indicators

[*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

Governance

- What do we mean by governance?
- Whose responsibility is it?
- Does it add value?

What do we mean by risk?

Some definitions of risk

- . . .something that might happen and its effect(s) on the achievement of objectives. *BS31100 Code of Practice for Risk Management*
- . . . the chance of something happening that will impact objectives . . . *AS/NZS 4360:2004 (Australian/New Zealand Standard from ASI)*
- ‘an uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives . . . A risk consists of a combination of the probability of a perceived threat *or opportunity* occurring and the impact of its magnitude on objectives.’ *(UK Office of Government Commerce, Management of Risk framework)*

What is Enterprise-wide Risk Management (ERM)?

- “A process, effected by an entity’s board of directors,. . . applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of its entity objectives.” [COSO]
- “A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.” [Sumitomo Mitsui Banking Corp]

Risk policy

- Purpose and scope of policy – overall objectives
- Definitions
  - different risk groups (e.g. credit; insurance/underwriting; market; liquidity; operational)
  - ‘boundary’ issues
  - other definitions i.e. establishing a common risk language
- Risk structure and responsibilities
  - clear and unambiguous ownership of risk and risk policy
- Risk management process
  - principal sources of risk
  - deviation from policy: authorised and unauthorised
  - measurement, management and reporting
- Risk appetite and risk tolerance
- Ethical and behavioural guidelines

Is operational risk different from other risks?

	Credit/Insurance/Market/Liquidity 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?		

Dealing with some other risks

- Strategic risks
- Reputation risk
- 3rd party dependencies (= outsourcing?)
- Legal risk
- Regulatory risk

Reputation risk

- Reputation risk
  - is almost always a *consequence* of events caused by other risk types, but OR is probably the main source
  - can result from competitors' activity
- Reputation
  - takes years/decades to build and moments to lose
  - is the largest asset in value and is crystallised when a business is sold
  - is a valuable barrier to entry
- Reputation risk management = management. Good management will accrue reputation.
- Management's response to a crisis will probably affect reputation more than the nature of the crisis itself.

Where does Risk - and the Head of Risk/Chief Risk Officer – sit?

- Relationship to:
  - Board (and Audit Committee)
  - CEO/CFO
  - Audit/assurance
  - Business
    - Common view of risk
    - Bad news
    - Whistle-blowing
  - HR
  - Insurance buyer (i.e. risk transfer)

The role of the Chief Risk Officer

- Overall risk leadership, vision and direction
- Establishing an ERM framework for all risks
- Developing and reviewing risk management policies (including risk appetite)
- Implementing risk metrics, including early warning indicators
- Allocating risk-based economic capital
- Developing support infrastructure

The Chief Risk Officer function

Independent?

Implementer? Facilitator? Consultant?

Are Risk's roles clear to Risk and to the business?

Compliance

- What do we mean by compliance?
- Compliance with what?
- Who is responsible for compliance?

Bringing them all together - the 3 lines of defence?

1	Business operations	• Established risk and control environment • Ownership
2	Oversight functions: Finance, Quality, HR, Compliance and Risk	• Functional oversight • Strategic management • Policy and procedure setting
3	Independent assurance: Internal audit, external audit, other independent assurance providers	• Provide independent challenge and assurance

BOARD

NEDs are like a bidet – nobody knows what to do with them but they add a bit of class.

(attrib. Michael Grade)

Becoming and NED – the spec

The job spec

- **Strategy**. NEDs should constructively challenge and contribute to the development of strategy.
- **Performance**. NEDs should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance.
- **Risk**. NEDs should satisfy themselves that financial information is accurate and that financial controls and systems of risk management are robust and defensible.
- **People**. NEDs are responsible for determining appropriate levels of remuneration of executive directors and have a prime role in appointing, and where necessary removing, senior management and in succession planning. [Higgs report, 2003]

The person spec

Non-executives should

"be sound in judgement and have an enquiring mind. They should question intelligently, debate constructively, challenge rigorously and decide dispassionately. And they should listen sensitively to the views of others inside and outside the board." [Higgs report, 2003]

The job ad

Independent of mind, with honesty and integrity, curiosity and willingness to challenge results, even when they appear to be successful, willing to stand up to executive directors and, if appropriate, resign.’ [ICAEW response to Higgs]

Becoming an NED – the test

- Board
  - Colleagues
  - Terms of reference (Committees)
  - Reports of activities
  - Board evaluation
  - Shareholders – views and structure
  - Going concern
  - Auditor independence
  - Remuneration policy

- Company
  - Market
  - Financials and funding
  - Risks
- Senior management
- Chairman
  - Due diligence (see above)
  - Board preparation; meeting time etc
  - D&O cover
- References from industry, advisers, brokers

Being an NED

- Board
- Audit Committee
- Remuneration Committee

Audit (and Risk?) Committee

- Membership (and chair)
- Financial and other reporting
- Risk assessment and internal controls
- External auditors
  - Appointment
  - Quality
  - Scope and findings
  - Differences of opinion
- Internal audit
- Responding to management needs
- Reporting to the Board

Risk - the NED/Audit Committee perspective

- Is there a clear set of risk management objectives?
- Does the executive take risk management seriously?
- Where does ownership for risk management lie?
- Is there a structure for strong oversight and challenge?
- Is general risk awareness visible? i.e is there a strong risk culture?

Being an NED

- Board
- Audit Committee
- Remuneration Committee

Remuneration Committee

- Remuneration as a behavioural incentive.
- Remuneration in line with ethical values and company’s objectives

John Thirlwell

Tel: +44 (0)20 8386 8019

E-mail: info@johnthirlwell.co.uk