Institute of Actuaries of India

ERM: Adding value to business, stakeholder perspectives

… a view from the Board of a life insurance company

2013 Risk Management Seminar

11th December, 2013 | Gurgaon, India

Topics for discussion

- What is happening in the financial markets
- The risk landscape is changing, so is its management
- An ERM framework should be clear, solid and crisp
- International trends for insurers
- Lessons learned by Boards from past experience
- Conclusion

What is happening in the financial markets …

- Increase in the number of significant risk events, such as:
  - Banks' financial losses through "rogue traders" e.g. Bruno Iksil "London whale" (JP Morgan, USD5.8 bn), Kweku Adoboli, (UBS, USD2 bn)
  - Price rigging scandals e.g. Libor, gold, oil markets, foreign exchange, industrial commodities
  - Data theft and reputational damage e.g. JPMorgan Chase (465,000 clients, May 2013), Standard Chartered, Singapore (647 top clients, Dec 2013)

- Deeper analysis shows some common themes:
  - "In fact, to a large extent, the current crisis can be understood as the product of a profound <u>failure in private risk management</u>" *(the US Congressional Oversight Panel, COP 2009)*
  - "The HBOS story is one of catastrophic <u>failures of management, governance and regulatory oversight</u>." *(Chairman, Parliamentary Commission on Banking Standards, Andrew Tyrie MP, 2013)*
  - "<u>Top management was too complacent</u>, wrongly believing that everything was under control, given that numerous risk reports, internal audits and external reviews always ended in a positive conclusion" (*Prof Straumann, reviewing UBS in 2010)*
  - "UBS does not strike me as a corrupt or fraudulent bank so much as a <u>naive and careless</u> one. It cut too many corners to compete in an industry in which extreme caution was required." *(Gapper, FT Journalist on UBS, Dec 2012)*

The risk landscape is changing, so is its management

1. Complexity is driving organisations to rethink the way they manage risk.
   - "Forecasting the future is risky, but businesses that fail to look forward will almost certainly be left behind in an increasingly competitive and globalized world" (E&Y).
   - Society has increasingly high expectations of corporate behaviour and a sharply increased ability to find and broadcast embarrassing information.

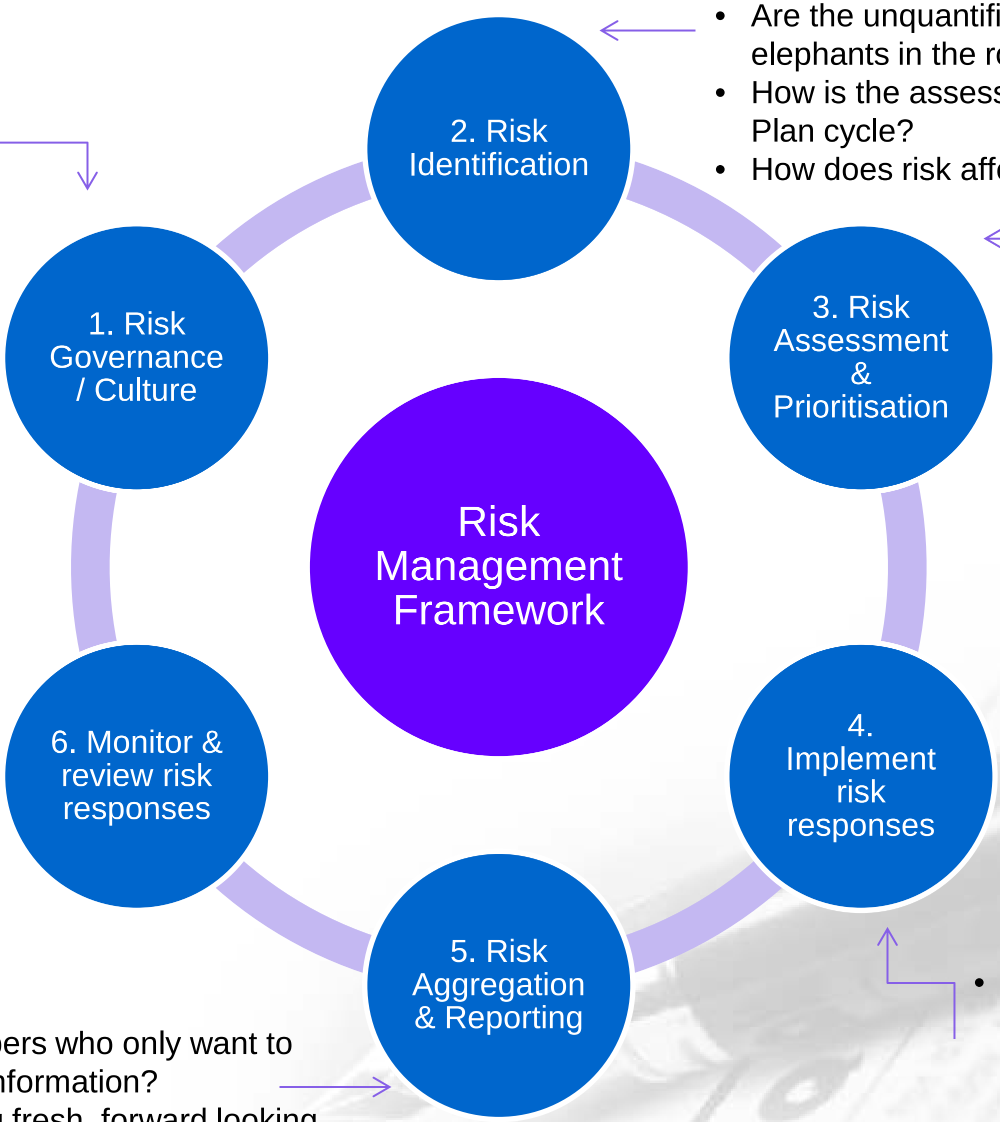
2. With increased Board accountability, they have increased their risk oversight:
   - Less absolute control by the CEO, more transparency to the Board
   - Increased role of independent directors
   - Increased focus on managing and pre-empting, not only assessing, risks
   - Increased focus on balancing interests of all stakeholders, not only those of shareholders

3. What is core to ERM?
   - An intelligent, proactive and systematic process to identify, assess, manage and monitor both upside and downside risks to the business.
   - Implementation of a clear intervention ladder if risks step out of pre-agreed boundaries.

"Success is clear POLICY, solid PROCESS and crisp REPORTING" **(by Nigel Masters)**

An ERM framework should be clear, solid and crisp

- Is it core to the CEO day-to-day walk or is it a paper policy?
- Is risk governance getting too heavy e.g. AA, CRO, Head of Internal Audit, Chief Compliance, Board Risk Committee? Can it be streamlined?
- Are the resources skilled, qualified and experienced enough to unearth the risks and challenge Management?



- Are the unquantifiable risks, emerging risks and elephants in the room captured?
- How is the assessment timed with the Business Plan cycle?
- How does risk affect our strategy?

- Does it answer … What can go wrong?
- Are the root causes of risks well understood?
- Does it include base case, scenarios, reverse stress tests?
- Does it provide an in-depth assessment of the options and recommendations?
- Is it too model driven vs required judgment to assess tail risks, correlations and potential extreme events?

- How reliable are the actions to curtail the risks or to mitigate risks under stressed conditions?

- How to report to Board members who only want to know solutions and minimal information?
- How to keep regular reporting fresh, forward looking and relevant? Frequent updates, annual refresh.

- How static vs dynamic is the monitoring of the risks given the changing risk landscape?

International trends for insurers

- IAIS with its 3 ICPs and 26 principles specify that each supervisory authority in each country requires insurance companies under its supervision to meet the following three requirements:
  - To establish a corporate governance which sufficiently acknowledge the protection of interests of policyholders (ICP 7)
  - To design a risk-based management and internal control framework (ICP 8)
  - To implement an integrated risk management (ICP 16)

- Europe - Solvency II with its core pillars of risk based capital, ORSA and greater disclosure to supervisors and public

- Australian with its 2 new standards on Risk Management (CPS 220) and Governance (CPS 550).
  - To be finalised by the start of 2014 with compliance by 1 January 2015.
  - Current draft requires a CRO to head the risk management function and not to be the CEO, CFO, Appointed Actuary or Head of Internal Audit (in other words, no “dual hatting”). The CRO is to have a direct reporting line to the CEO.

Lessons learned by Boards from past experience

1. Inadequate board skills and inability of NED members to exercise control
2. Blindness to inherent risks, such as risks to the business model or reputation
3. Inadequate leadership on ethos and culture
4. Defective communication and information flow within the organisation, including to board-equivalent levels
5. Organisational and business complexity and change
6. Inappropriate incentives, both implicit and explicit
7. Glass ceiling effects that prevent risk managers from addressing risks emanating from top echelons
8. A clear, overarching crisis strategy, defined in the calm of peacetime, to make better, more thoughtful decisions.

Source - Roads to Ruins : A study of major risk events, by Cass Business School based on twenty major corporate crises of the last decade.

Conclusion

- Board requires a sharp, concise and coherent articulation of a risk management strategy, risk map and an effective mitigation plan:
  - Risks are to be clearly identified, thought-through, weighted for materiality and managed in a controlled manner.
  - Increasing importance of preventive and detective actions.
  - Risk management culture is to be disseminated throughout the firm.
  - Risks are there for all players but the winners will be those who mitigate them judiciously.
- In today's highly competitive landscape, there is a need for 3 strong lines of defense for effective risk management and control:
  - Operational management functions is to *own and manage* the risks,
  - GRC (Governance, Risk and Compliance) and AA functions are to *oversee* the risks, and
  - Internal audit function is to provide independent *assurance* of the ERM effectiveness.
- Distinct roles between Appointed Actuary and CRO
  - CRO is a specialist risk manager, challenging material activities which affect the Company's risk profile and managing risk within its risk appetite. It is a full time job.
  - Nature of AA role is central to the overall financial soundness of the company and PRE.

Institute of Actuaries of India

ERM: Adding value to business, stakeholder perspectives

… a view from the Board of a life insurance company

2013 Risk Management Seminar

11th December, 2013 | Gurgaon, India