THE GOVERNANCE OF RISK MANAGEMENT
Polling Question: Who is primarily responsible for risk governance in any organization?

A. The board or board risk committee (if applicable)
B. The CRO
C. The business lines
D. The head of internal audit
What’s wrong with this picture?

Risk Committee
☑️ Only three members
☑️ Members of committee included:
  • Museum director, who was former director of a failed company
  • Grandson of a well known billionaire
  • CEO of a thermostat and work boot manufacturer
☑️ Only one with relevant bank experience - had not worked in the industry for 25 years
☑️ Same composition since 2008
☑️ None had worked as risk managers

Risk Committee
Museum director: accepted large donations from X for Museum, had personal loans from X, and was paid 250K for work on the board, resigned from compliance and governance committee of a failed institution

Son of billionaire: Was on committee that chose Mr. XY to lead X. Had not worked in the industry for 25 years

Thermostat manufacturer: CEO had received loans and advisory work from X, and X had purchased equipment and services from the thermostat manufacturer
JP Morgan Chase & Co.

- “Naive” - “poorly structured risk oversight” - “Nothing in their professional background...”
- JP Morgan is a complex financial institution
- Risk committee members unprepared to ask difficult questions
- lack depth of experience
- had questionable independence
All drafts include new elaborate sections on the governance of risk!
What’s Changed? Boards need to be Increasingly Focused on:

- Risk Appetite – A Risk Appetite Framework (RAF) encompassing all risks… and the resulting Risk Appetite Statement (RAS)

- Risk Compliance – Particularly “conduct risk”, adherence to P&P, ethical standards, fairness and disclosure

- Reputational Risk – Assessing the impact of potential reputational damage on returns, market share

- Capital Allocation – Measuring where capital is at risk and how risks are related

- Risk Culture – Shifting accountability to the front office and line (where conduct takes place)

- Stress Testing – Looking at the potential impact of possible events, inter-relationships, on the overall portfolio

- Risk Technology/Architecture/Cyber-security – improved risk information, reporting, data and analysis; and, stronger cyber security and anti-hacking measures

- Operational Risk – Fraud, Fines, Business Ethics, etc.
Overview

- Risk Culture and Risk Appetite
- Overview of the governance of risk management
- Board-level risk management committee
- Conclusion / Lessons
Risk Culture: Definitions

Principle I.i:
A robust and pervasive risk culture throughout the firm is essential.


“Risk culture” can be defined as the norms and traditions of behavior of individuals and groups within an organization that determine the way in which they identify, understand, discuss, and act on the risk the organization confronts and the risks it takes.”

Institute of International Finance, Implementing robust risk appetite frameworks to strengthen financial institutions, 2011
Risk Culture: Elements and Practices

- Principles, policies, procedures and controls
- An effective governance structure – management objectives linked to risk management objectives
- Senior management sets the correct “tone at the top”
- Adequate budget and support for the risk management units, with those working in risk management having an effective voice
- “Challenging and questioning” by employees, management, board - willingness and ability to ask the right questions
- A “top-down” view of risk in the form of a Risk Appetite Framework (RAF)
- “Stress testing” to understand the “portfolio effects”

Source: Risk Culture, Risk Governance, and Balanced Incentives (IFC Unpublished May 2014)
2. Culture…. Common Values? Returns versus Fairness…. 

1. A customer calls with an urgent need to deliver foreign exchange to a counterparty by end of day. Does your Bank
   a. Set an off-market FX rate so the bank makes lots of money?
   b. Set a competitive rate so the customer gets a fair deal?
   c. Charge a special processing fee?
   d. Inform the customer about these charges?

2. Consumer loans are currently in high demand. Does your bank:
   a. Increase rates and fees across the board without disclosing this? (Let them read the fine print...)?
   b. Maintain disclosed rates?
   c. Increase rates for more risky customers?
   d. Reduce rates to gain market share?

3. You overhear a trader in your bank get a call from a friend at another bank suggesting that they collude in setting the same price on a product. Do you:
   a. Openly praise the Trader for keeping returns high?
   b. Tactically approve of the Trader, and recommend his boss consider a bonus?
   c. Keep quite?
   d. Warn the Trader about ethical violations?
   e. Recommend the Trader be fired?
What is “Risk Appetite”?

• “The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.” Financial Stability Board, Principles for an Effective Risk Appetite Framework (2013)

• “. . . the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.” COSO Enterprise Risk Management, Understanding and Communicating Risk Appetite (2012).

• “. . . is an expression of the amount of risk the firm is willing to take in pursuit of its strategic objectives, reflecting our capacity to sustain losses and continue to meet our obligations arising from a range of stress trading conditions” Standard Chartered Bank, 2010 Annual Report

• “The Board sets the Group’s financial volatility risk appetite in terms of broad financial objectives (i.e. “top down”) on through the cycle” Barclays Plc, 2010 20-F filing

• “…the actual risk appetite is assessed over time covering both banking and trading book exposures” Walker Report 2009
Risk Appetite – How Much Risk Concentration –
A Really Thorny Issue In Risk Governance

Concentration Risk: How do we measure risk concentrations; How much do we accept?

Easy:
• Single borrowers
• Single products, loans, cards, mortgages, etc.
• Single sectors, manufacturing, agri, etc.
• Type of collateral, land, houses, cars, equipment, etc.
• Tenor

Difficult:
• Group Borrowers – multi-industry, multi-company, multi-country
• Related products
• Related Sectors – covariance of losses in different industries
• Collateral valuations under stress
• Pre-payments and withdrawals under stress

The Board needs to exercise significant judgment about what kinds of information they need to be able to effectively monitor and limit the risks a Bank is actually taking . . . the trick is to think about what could happen and assess this in enough depth to inform the Risk Appetite Framework and Risk Limits and create data and reporting that capture these risks. This is related to stress testing and financial modeling…
Polling Question: An effective risk governance framework:

A. Identifies risky activities and prohibits the organization from engaging in them
B. Identifies risky activities and recommends strategies for managing and monitoring them
C. Is responsible for risk monitoring and crisis management
D. Is responsible for stress testing and scenario planning
Organization: Board & Management Roles in Risk Governance

- **Board**: Approve, Implement, Monitor, Review, Propose (adjustments)
- **Business Operations**: Executing and monitoring transactions
- **Audit/Risk committee**: Policies, high level limits and stress tests
- **Senior management, risk management Board/board committee**: Senior management
Organization: Three Lines of Defense:

1. **Board of Directors**
   - Board Risk Committee: Bank strategy and objectives, risk appetite & ultimate level of responsibility.
   - Board Audit Committee

2. **CEO and Executive Management**
   - **1st Line of Defence**
     - Business line operations: Real time operational focus:
     - Embeds risk management framework and sound risk management practices into standard operating procedures.
     - Monitors risk management performance in operation.
     - Accountable for effectiveness of risk management in operation.

3. **2nd Line of Defence**
   - Risk Management: Real time monitoring and review focus:
     - Develops and implements risk management framework – policies, systems, processes and tools.
     - Ensures framework covers risk:
       - Identification
       - Assessment / methods
       - Response
       - Controls / limits
       - Information / data
       - Monitoring
       - Reporting
     - Exercises approval authorities in accordance with delegated authorities.

4. **3rd Line of Defence**
   - Internal Audit: Independent review focus:
     - Reviews effectiveness of risk management practices.
     - Confirms level of compliance.
     - Recommends improvements and enforces corrective actions where necessary.

---

*Governance: Tone at the top*

*Performance: Embed risk management*
5. Organization: Risk Governance Structure for FI

Board of Directors

- Audit Committee
- Corporate Governance Committee
- Remuneration Committee
- Risk Management Committee
- Management Committee
- Executive level risk committees
  - Asset & Liability Management Committee
  - Credit Risk Committee
  - Operational Risk Committee
- Management
  - Senior Management
  - Business Units
- Chief Risk Officer
  - Risk Management Department

Governance

Performance

Internal Audit
Risk Related Roles: Non-FI

Board of Directors

- CEO on BOD Possibly CFO, COO
- COO
- CFO
- Business line Head
- Audit Committee
- Internal Audit
- Other Committees
- External Auditor
Risk Governance Responsibilities

- **Board**: Risk oversight, approve risk management framework
- **Senior Management**: Implement risk management Framework
- **Executive-Level Risk Committee(s)**: Setting risk limits within approved risk appetite levels and risk tolerance limits
- **CRO**: Identification, assessing, monitoring & mitigation of risks
- **Risk Management Department**: Day-to-day responsibility for risk management
- **Business Units**: Day-to-day responsibility for risk management
- **Audit Committee**: Review and ensure compliance with risk management policies

---

Risk Management Committee

- Risk management framework
- Setting risk limits
- Identification, assessing, monitoring & mitigation of risks
- Day-to-day responsibility for risk management
Organization: What Helps a Board be Effective Risk Governors?

1. Avoid Concentration of Power - separate Chairman and CEO, have majority Independent Directors

2. Bring a balance of required risk expertise to the Board/committees - Credit, Market, Operational, IT, Reputational, Environmental and Social, Strategic, Successional, Incentives Structures -- with an understanding of the various roles of the front line units, the risk control units, and the audit functions within a bank

3. Set-out clear terms of reference and term limits for board members and committee members

4. Annually approves the bank’s strategy, capital plan, financial plan and Risk Appetite Framework

5. Actively oversee managements implementation of the Risk Appetite Framework, insist on stress testing

6. Ensure Audit and Risk Committees have overlap and communicate

7. Meets with Regulators and other authorities quarterly

8. Engage independent parties to review board performance every 3 years
A Separate Risk Management Committee

- Rationale
  - Risk management is a governance function
  - A prevailing best practice
  - Demonstrate the board’s commitment to risk management

- Functions
  - Ensure effective risk governance
  - Monitor risks
  - Oversee management actions to manage risks
A Separate Risk Management Committee

Key board/risk management committee attributes for good risk governance

- Top risks are identified and agreed throughout the organization
- Risks inherent in the corporate strategy are thoroughly understood
- Risk appetite is clearly defined
- Responsibility for managing each top risk is clearly defined at the board level
- There is vigilance of excessive risk-taking by management
Risk Management vs. Audit Committee Role

**Risk Management Committee**

**Focus**
- Future performance
- Broader risks (strategic, managerial and operational)
- Risks with financial and non-financial consequences

**TOR**
- Risk assessment (ensure management assesses risks and updates risk register & risk assessment is part of the decision-making process & risks are within board-set risk appetite)
- Risk management (ensure effective RM system in place to assess, control & monitor risks)
- Risk reporting (review information and report to board on major risks and exposures and their management)

**Audit Committee**

**Focus**
- Historical performance
- Effectiveness and efficiency of operations, financial reporting & compliance

**TOR**
- Audit (ensure external and internal audit functions are adequate to address business risks)
- Internal control (ensure management has established adequate IC to address business risks & effective implementation of IC)
- Financial Reporting (review financial reports & ensure duties of directors regarding financial disclosure are discharged)

*Source: Aon Risk Solutions, White Paper on RMC, 2011*
Good practices to implement

Some common sense practices must be in place:

• Board structured to add value and avoid conflict of interest
• Board has appropriate skills to review and challenge management actions
• Ethical and responsible decision-making
• Clearly defined and documented ToR for directors & executives
• Independent verification and validation of financial reporting and processes
• Disclosure to stakeholders of all material matters
• Structure and process to identify and manage risk
• Clearly documented key roles & responsibilities, policies & procedures throughout the company
Key Questions to Ask about Risk Governance

- Who is responsible for developing the risk management system?
- How are the risks identified and risk appetite set?
- Does the board periodically review the risk management systems?
- What is the role of IA unit in the management of risk?
- How often is management of risks compared to targets approved by the board?
- How is this reported to the board?
- Do the board and management appropriately assess risks when planning new strategies, activities and products?
Key Messages

Best practices and regulation has significantly changed recently and the Board clearly has responsibility for adequate risk governance:

1) Establish and Monitor Business Objectives and Strategy

2) Establish Corporate Culture and Values – including Risk Culture, Fairness and Disclosure standards, Environmental and Social Responsibilities, Code of Conduct

3) Oversee Implementation of Appropriate Governance Framework – including Risk Governance, levels of control

4) Establish the Bank’s Risk Appetite – Approve the Risk Appetite Statement (RAS) annually and monitor adherence at least quarterly, conduct stress tests

5) Establish Effective Risk Management Organization and Ensure Appropriate Staffing

6) Approve and Monitor Capital Adequacy, Liquidity, Compliance and internal controls

7) Select and Monitor Senior Management, Maintain Succession Plans, Staff Board Committees with Appropriate Experts

8) Design and Implement the Incentive Systems that reinforce good risk management
Thank you!