DASHBOARD CONTROLS – CHECK ENGINE!

CONTROLS, AUDIT AND RISK MANAGEMENT
SESSION 7

Objectives

- Understand the board’s role in control environment
- Learn about audit committee and internal controls
- Understand the internal and external audit function
- Learn about risk management oversight
- What’s the role of the board in compliance?

Refer to book chapters:
- 4.3 - Audit and Risk Committee
- 5.4 - Risk Management
- 6.2 - Conflicts of Interest, RPT, compliance
The Board’s Role in Control Environment

<table>
<thead>
<tr>
<th>Oversight</th>
<th>Value Creation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy</td>
<td></td>
</tr>
<tr>
<td>Risk Oversight</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Financial/controls</td>
<td>Strategy Development</td>
</tr>
<tr>
<td>Control/monitor performance</td>
<td>Internal/external audit policies</td>
</tr>
<tr>
<td>Approval of investments, M&amp;A</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td></td>
</tr>
<tr>
<td>Create code of conduct (e.g. values, behavior, conflict resolution)</td>
<td>Protection of shareholder rights</td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
</tr>
<tr>
<td>Evaluation of management performance</td>
<td>Compensation guidelines</td>
</tr>
<tr>
<td>Approval of HR policies</td>
<td>Succession planning</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Basic organizational design (e.g. dominant axis of management, relation HQ-subsidiaries)</td>
<td></td>
</tr>
<tr>
<td>Board Organization</td>
<td></td>
</tr>
<tr>
<td>Board evaluation</td>
<td>Defining Board proceedings</td>
</tr>
<tr>
<td>Defining information needs</td>
<td>Defining Board calendar</td>
</tr>
</tbody>
</table>

Governance Structure of Control Environment

Shareholders
Board of Directors
Achievement of strategic objectives and value creation
Full duties and responsibilities in law and prescribed functions

Board Operations
- Strategy
- Corporate Policies & Procedures
- Board Governance Instruments
- Monitoring and Evaluation

Information Communication

CEO & Management
- Internal Controls & Assurance
- Combined Assurance Model
  - Internal Audit
  - External Audit
  - Other Assurance Providers
  - Management

Board Committees
- Audit Committee
- Remuneration Committee
- Other Committee
- Executive Committee
“Ensuring the integrity of the corporation’s accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards”

OECD – Principles of Corporate Governance

### Division of Responsibilities

<table>
<thead>
<tr>
<th>Board of Directors</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversee the development and implementation of an adequate internal control systems</td>
<td>Establish and maintain an adequate and effective system of internal controls</td>
</tr>
<tr>
<td>Monitor the independent assurance function</td>
<td>Develop a system to monitor and control risks</td>
</tr>
</tbody>
</table>
Internal Control Definition

- A process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
- Operating objectives
- Reporting objectives
- Compliance objectives

Key Questions to Ask about Internal Controls

- What is the role of the audit committee and the board in ensuring that proper internal controls are maintained, risks are managed and that the company is in compliance with all relevant laws and regulations?
- Describe how the company’s internal controls (operational, financial and compliance, including IT systems) are designed and maintained?
- Are internal controls risk based?
- Were there any significant problems in internal controls in the past 5 years? Please describe.
- Does the board monitor that management responds to the deficiencies identified in Management Letters?
- Are internal controls designed in accordance with a relevant framework, e.g., COSO, COBIT, Basel?
Internal Audit Helps to Monitor the Internal Controls

Board, in particular, the Audit Committee oversees

Internal audit function evaluates

Monitoring the Internal Control Process

Managers have primary task to design and maintain controls

External auditors assess and opines on

Internal Auditor

- Evaluate and monitor on daily basis the company's risk management, reporting, and control practices, operations and systems and make suggestions for improvement
- Shall be independent of the management – reports to audit committee (the board)
- Can be hired and fired only by AC/board
- Annual internal audit plan approved by AC/board
- Is in charge of following up on the internal controls deficiencies identified by external auditors, compliance function and regulators
- Evaluates the company's corporate governance structures and processes
Future of Internal Audit Function: Trusted Advisor

Key Questions to Ask about Internal Audit

- To whom does the Chief Internal Auditor report? How is the IA chief hired/fired and does the CIA privately meet with the board or the audit committee?
- What is the relationship between IA, the Chair, CEO, CFO, CRO, CIO and external auditor?
- Are the IA work plans reviewed by the audit committee or the board?
- Does the board monitor management’s response to deficiencies and weaknesses identified by the IA function?
- Are internal audits risk based?
- Were there any significant problems with internal audit in the past five years? Please describe.
- Is corrective action taken, followed-up on?
- What are the audit standards applied by IA, e.g., IIA Standards?
- Does the external auditor rely on the work of internal audit in conduct of the annual financial statement audit?
- How are conflicts of interest with internal auditors handled?
Audit Committee Functions

- **External audit**
  - Appoints the external auditor and key contact point
  - Recommends the audit fee to the Board and approves any non-audit services provided by the external auditor
  - Discusses with the external auditor, the nature and scope of the audit and reviews the auditors quality control mechanisms
- **Internal audit**
  - Monitors and reviews the activities of internal audit
  - Ensures that the internal audit is adequately resourced and has sufficient standing within the company
  - Maintains the independence of IA and provides necessary resources
  - Considers management response to IA recommendations
- **Controls and risk management**
  - Ensures that a comprehensive internal controls framework in place
  - Ensures the presence of a risk management policy document
  - Reviews significant reporting issues and accounting policies
  - Reviews company’s semi-annual and annual financial statements
  - Reviews formal announcements made to the shareholders
  - Reviews relevant regulatory returns filed and disclosures made by the company
  - Reviews the going concern assumption of the company
  - Monitors and approves material related-party transactions
- **Reporting and disclosure**

Expanding Role and Expertise of the Audit Committee

In addition to “financial expertise,” what other in-depth experience or expertise currently resides on your AC? | In what areas would you favor additional reporting/communication from AC to investors? |
---|---|
- Technology | Audit committee’s role in risk governance |
- Industry | Oversight/evaluation of internal auditor (including independence and effectiveness, responsiveness, etc.) |
- Legal/regulatory companies | Effectiveness of audit process |
- MBA | Audit committee’s effectiveness (qualification of members, performance evaluation, etc.) |
- International | Audit committee meetings (number, attendance, etc.) |
- Tax | Significant financial statement audit issues and how they were addressed |

Source: KPMG ACI Global Audit Committee Survey, (2014)
External Audit

- Audit committee/board in charge of selecting an auditor
- Auditor independence (attention to non-audit services)
- Regular contact with the auditor (through audit committee/board)
- Evaluation by the audit committee/board of the auditor’s quality
- Invite representatives of the auditor to the shareholders meetings
- Follow up on management letters issued by the auditor
- Disclosure of the audit report (annual report, web-site)
- Auditor/lead partner rotation

Key Questions to Ask about External Audit

- Who, formally and in practice, selects the external auditors and to whom are they accountable?
- What is the relationship between EA, the Chair, CEO, CFO, CRO, and CIA?
- Is there the policy to rotate the external auditors or the lead audit partners?
- Has the Audit Opinion ever been a Qualified, Disclaimer or Adverse Opinion? Why?
- Does the board monitor management’s response to accounting and reporting control deficiencies and weaknesses identified by Management Letters and IA?
- Is there the policy to rotate the external auditors or the lead audit partners?
- What are the accounting standards used to report results (IFRS, GAAP)? What are the audit standards used by the external auditor (ISA, GAAS)? Any disparities with local standards and international standards?
- Does the external auditor rely on the work of internal audit in conduct of the annual financial statement audit?
- Does the external auditor provide any other services besides the external audit?
Compliance and Whistleblowing:
How Is Compliance Related to Corporate Governance?

Key Questions to Ask about Compliance

• Is there a compliance function? Is it separate department/unit (centralized or decentralized)? Independence?
• What is the relationship between CCO, the Chair, CEO, CFO, CRO, and CIA?
• Is there a code of ethics?
• Please describe the company’s compliance program or procedures including training of employees, auditing and monitoring systems, company “hotline” for reporting violations?
• Is there a Compliance Register?
• Are instances of non-compliance followed up on with corrective action?

Source: Frame of reference for integrated GRC; Razz, Weippl, Seufert, 2010
Comprehensive Risk Approach

Board of Directors (directly or through a Committee) | Management
---|---
• Approval of RM or elements thereof | • Development of RM system
• Review and control over RM system efficiency | • Implementation and maintenance

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.
Enterprise Risk Management Implementation

### Success Factors

1. Assess the full risk situation (e.g. financial risk, operational risks, industry risk,...)
2. Evaluate the potential risks according to their likelihood of appearance and their potential consequences/cost
3. Identify possible direct and indirect consequences of the risks
4. Evaluate the cost of dealing with the risk
   - Avoiding the risk (e.g. pursue other alternatives)
   - Limit the risk (e.g. quick reaction in case risk materializes)
   - Hedge the risk (e.g. counterbalancing the risk)
   - Share the risk (e.g. insurance)
   - Control the risk (e.g. early red flags)
   - Understand the risk (e.g. evaluation by outside experts)
5. Get the top management support
6. Make sure there is close relation between ERM and strategic objectives setting and business planning process

### Hidden Obstacles

1. Risk is not managed but monitored
2. Insufficient awareness of ERM importance, its functions and objectives
3. Excessive emphasis on technical aspects, neglect of personnel’s behavior peculiarities

---

### Red Flags

- Is cash-flow from successful operations or from non-recurring transactions?
- Did the company shift its funding to riskier sources?
- Is the company experiencing unusual employee/management turnover?
- Inadequate explanations for variances of actual to budget
- Irregular or no contact with executive staff
- Resistance to abandonment of a marginally profitable venture
- Disruption in supply chain affecting operations
- Auditors identifying significant control problems and disagreeing with management on material issues
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

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)
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
E. B, C and D
Organization: Three Lines of Defense:

1. **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

2. **Board of Directors**
   - Risk Management and objectives, risk appetite & ultimate level of responsibility

3. **Board Audit Committee**
   - Independent review focus:
     - Reviews effectiveness of risk management practices
     - Confirms level of compliance
     - Recommends improvements and enforces corrective actions where necessary

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
- **Senior Management**
- **Business Units**
- **Chief Risk Officer**
  - Risk Management Department
- **Internal Audit**
- **Performance**
- **Governance**
Risk Related Roles: Non-FI

- **Board of Directors**
  - CEO on BOD Possibly CFO, COO
  - Audit Committee
  - External Auditor
- **Other Committees**
- **Business line Head**
- **COO**
- **CFO**
- **Internal Audit**

Risk Governance Responsibilities

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

- **Key board/risk management committee attributes**
  - 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

<table>
<thead>
<tr>
<th>Risk Management Committee</th>
<th>Audit Committee</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td><strong>Focus</strong></td>
</tr>
<tr>
<td>Future performance</td>
<td>Historical performance</td>
</tr>
<tr>
<td>Broader risks (strategic, managerial and operational)</td>
<td>Effectiveness and efficiency of operations, financial reporting &amp; compliance</td>
</tr>
<tr>
<td>Risks with financial and non-financial consequences</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TOR</th>
<th>TOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment (ensure management assesses risks and updates risk register &amp; risk assessment is part of the decision-making process &amp; risks are within board-set risk appetite)</td>
<td>Audit (ensure external and internal audit functions are adequate to address business risks)</td>
</tr>
<tr>
<td>Risk management (ensure effective RM system in place to assess, control &amp; monitor risks)</td>
<td>Internal control (ensure management has established adequate IC to address business risks &amp; effective implementation of IC)</td>
</tr>
<tr>
<td>Risk reporting (review information and report to board on major risks and exposures and their management)</td>
<td>Financial Reporting (review financial reports &amp; ensure duties of directors regarding financial disclosure are discharged)</td>
</tr>
</tbody>
</table>

Source: Aon Risk Solutions, White Paper on RMC, 2011
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?

The Board’s Value-Added in the Control Environment

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
Key Messages

- The board should create an environment of trusting the management with completeness and accuracy of information and controls and verify it independently.
- Internal controls are implemented by people (with use of certain technology) but mistakes and omissions are possible.
- The external audit of the financial statements does not relieve management of any of its responsibilities.

Thank You!

Additional information is available in the Annex below.
Internal Control System | Internal Audit Function

Internal Control systems are the means by which:
• Operations are conducted in accord with prescribed policies and procedures.
• The enterprise is in compliance with applicable laws and regulations.
• The enterprise’s assets and information are protected from improper use.

Internal audit provides the board and management with reasonable assurance that these systems are adequate and functioning.

The Institute of Internal Auditors
Progress Through Sharing

Independent, objective assurance and consulting activity designed to add value and improve an organization’s operations.

It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal Control Processes

- Internal controls system
- Detects errors
- Prevents mistakes
- Identifies fraud
- Ensures integrity of all numbers
- Ensures the reliability of financial reports

Determine Business Objectives
Identify and Assess Risks
Identify Control Activities
Assess Residual Risk
Acceptable? If no...
1. Management oversight and the control culture.
2. Control activities and segregation of duties.
4. Information and communication.
5. Monitoring activities and correcting deficiencies.


**COSO Internal Control - Integrated Framework (2013)**

1. **Control Environment** - The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.
2. **Risk Assessment**
3. **Control Activities**
4. **Information and Communication**
5. **Monitoring Activities**

**Mandatory Elements**

---

**IT Controls and Emerging Trend of the Board Technology Committee**

**COBIT 5: Framework for IT Internal Controls**

- COBIT 5 (Control Objectives for Information and Related Technology), as published by ISACA in 2012, provides comprehensive framework to assist enterprises in the governance and management of IT.
- Recognizes the expanded role of IT as an integral part of the business.
- Used as the basis for the framework for managing operational and information risk in the context of Basel.

**Board Level Technology Committee**

- **Board of Directors**
- **CEO**
- **CIO**
- **COO**
- **CFO**
- **External Auditor**
- **Internal Audit**
- **Audit Committee**
- **Technology Committee**
- **Other Committees**
Key Features
The Internal Audit Function

- Continuity
- Independence
- Impartiality
- Professional competence
- Scope of activity
- Internal audit charter

Basel, The Internal Audit Function in Banks (2012)

CG Structure: Internal Audit Roles and Functions

<table>
<thead>
<tr>
<th>Board of Directors</th>
<th>Management</th>
<th>Internal Audit Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversee the development and implementation of an adequate internal control systems</td>
<td>Establish and maintain an adequate and effective system of internal controls</td>
<td>Assist management in the efficient and effective discharge of their responsibilities</td>
</tr>
<tr>
<td>Monitor the independent assurance function</td>
<td>Develop a system to monitor and control risks</td>
<td>Advise and make recommendations on internal control, risk management and corporate governance</td>
</tr>
</tbody>
</table>
Benefits of Audit Committee

- Board members improve their oversight of financial reporting, audit-related issues and key accounting processes
- Enables a small group of board members to focus on major topics in more detail
- Provides an opportunity, through meetings and discussions, for closer interface with senior company executives and the external auditor
- Allows external auditor to raise issues with the audit committee in a relatively structured environment

Audit Committee Organization

- Charter or bylaws
- Co-ordination with and information links to full board
- Composition
  - 3 members (board members vs. external)
  - Independence
  - Financial literacy vs. financial experience
- Meetings - no set frequency - but suggest 4 to go with quarterly reports
  - Frequency of audit committee meetings is expected to vary according to the stage of development of oversight activities in the company
  - “Normal” schedule of audit committee meetings that may be expanded when critical issues arise
Audit Committee - Detailed Duties (1)

Financial supervision
• Monitor the company’s financial position and its financial statements’ integrity
• Assess the appropriateness of accounting standards
• Monitor any formal announcements relating to the company’s financial performance, including the annual financial statements, the annual report, other reports, and interim reports and statements

Audit Committee - Detailed Duties (2)

Internal audit and control
• Evaluate the adequacy and appropriateness of internal control, internal audit, risk management
• Review internal audit plans, reports
• Safeguard the company’s assets by understanding the company’s risk environment and determine how to deal with those risks
• Evaluate compliance with laws, regulations
Auditor selection and monitoring
- Prepare the decision to appoint the external auditor
- Maintain contacts with the external auditor, examine the auditor’s reports
- Recommend the auditor to the board for shareholder approval
- Appoint, re-appoint, remove the external auditor
- Review, monitor the external auditor’s independence
- Evaluate the non-audit services supplied by the external auditor
- Develop, implement policy on engaging the external auditor to supply non-audit services
- Maintain communications on such matters between the board, management, the independent auditors, the internal auditors

Compliance
- Understand the ramifications of changes to the legal and regulatory framework on the company’s controls
- Ensure compliance with internal policies, procedures
- Monitor operation of the company’s whistleblower arrangement

Risk management
- Ensure that all business risks are identified, evaluated, suitably managed
- Decide on the company’s risk appetite
- For banks, analyze the current and future capital requirements in relation to its strategic objectives

Keep the full Board informed without repeating all the information
External Audit vs. Internal Audit

**External audit** means business activities involving an independent audit of accounting records and financial (accounting) reporting of companies and individual entrepreneurs.

**Internal audit** means an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Benefits of Risk Management

**Operational performance**
- Increases the likelihood of achieving business objectives
- Uses incidents to highlight the risk environment and helps management develop performance indicators or risk indicators to enhance business performance and processes
- Facilitates the management of the delivery of risk in key projects and initiatives

**Financial**
- Protects and enhances value by prioritizing and focusing attention on managing risk across the company
- Builds investor and stakeholder confidence, and shareholder value
- Reduces insurance premiums through demonstrating a structured risk-management approach

**Decision-making**
- Shares risk information across the company, contributing to informed decisions
- Facilitates assurance and transparency of risks at board level
- Enables decisions to be made against risk appetite
Typical Risk Indicators

Strategic
• Unfocused Strategy
• Strategy not Aligned with Capabilities
• Complacency Arising from Past Success
• Unsuccessful Acquisition/Abortive Bid
• Failure to Manage Major Changes
• Reputational Risk
• Loss of Investors’ Confidence
• Political/General Economic Risk

People
• Leadership/Mgt. Unable to Drive Company Forward
• Inadequate Succession Planning
• Loss of Key Players
• Poor Employee Motivation
• Internal Communication Weaknesses

Marketplace
• Not Responding to Market Trends/Failure to Motivate
• Missed Opportunities - New tech., Global Markets
• Weak Brands, Over-reliance on a Few Customers
• Poor Customer Satisfaction - Quality/Timeliness

Ethical
• Failure to Enact High Stds. of Ethics across Business
• Obtaining Contract Unethically
• Stakeholder Concerns on Products/Business

Suppliers/Outsourcers
• Over-dependence on Suppliers/Outsourcers
• Failure to Manage Cost/Quality of Outsourced Service
• Supply Chain Problems
• Joint Ventures, Strategic Alliances not Working

Financial
• Cash Flow/Going Concern Problems
• Treasury Operations Risk
• Susceptibility to Fraud/Accounting Irregularities

Legal/Compliance
• Failure to Protect Intellectual Property
• Health, Safety, Environmental Issues
• Litigation Risk
• Breach of Competition, Corporate, Employee, Tax Laws

Source: RSMi International, Building World-Class Boards, 2003

Example of a Risk Tool

There are three different radar tools:
• Financial risks
• Internal risks
• External risks

Risks are never stand-alone, so they are
• Influenced by other factors
• Influencing other risks and business relevant factors

Using the tool:
Evaluate the risks according to
• The possibility that they hit
• The severity if they hit
• The relevance to your company

Accordingly, give each risk a score:
1. Safety zone – no immediate danger for your company (monitoring)
2. Caution zone – company is at risk and prevention measures should be taken
3. Danger zone – immediate action is necessary to deal with the risk

• Be sure to write your personal comments to the risks in order for you to understand your reason for evaluation at a later time
• Let other members of your peer group do the same evaluation and discuss the results among your group
• Decide on appropriate measures to manage the risks

Source: RSMi International, Building World-Class Boards, 2003
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.**
- “Naïve” - “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
CG Principles Revision Projects Include More Robust Risk Governance

All drafts include new elaborate sections on the governance of risk!

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
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...
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 management’s 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