THE BOARD’S ROLE IN AUDIT, CONTROL, & RISK OVERSIGHT

Key Functions Of The Board

• Reviewing and guiding corporate strategy and risk policy
• Monitoring effectiveness of the company’s governance
• Monitoring and managing potential conflicts of interest
• Ensuring the integrity of the firm’s accounting and financial reporting systems, including the independent audit and that appropriate controls are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.
• Overseeing disclosure and communications

OECD Corporate Governance Principles Section VI
Board’s Role In Audit, Control, & Risk Oversight

SURVEY QUESTIONS
Internal Audit Reporting

Polling Question: How frequently does your internal audit committee interact with the board of directors?

A: Monthly
B: Quarterly
C: Annually
D: I don’t know

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

AUDIT COMMITTEE OVERVIEW
Audit Committee Roles & Responsibilities

- 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
- 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
- Ensure 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

Key Oversight Areas Of The Audit Committee

<table>
<thead>
<tr>
<th>Oversight area</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key areas of business and financial risk</td>
<td>Assess risk management</td>
</tr>
<tr>
<td></td>
<td>Investigate deficiencies of risk management</td>
</tr>
<tr>
<td>Tone at the top/code of ethics</td>
<td>Assist establishing code of ethics</td>
</tr>
<tr>
<td>Internal controls and systems</td>
<td>Review/test internal control system</td>
</tr>
<tr>
<td></td>
<td>Investigate deficiencies of internal controls</td>
</tr>
<tr>
<td></td>
<td>Review management information system etc.</td>
</tr>
<tr>
<td>External audit activities and relationships</td>
<td>Appoint external auditor</td>
</tr>
<tr>
<td></td>
<td>Monitor independence of external auditor</td>
</tr>
<tr>
<td></td>
<td>Change external auditor if necessary</td>
</tr>
<tr>
<td>Periodic financial reporting, including finance and</td>
<td>Review of financial results and of financial</td>
</tr>
<tr>
<td>accounting policies</td>
<td>reporting</td>
</tr>
<tr>
<td></td>
<td>Review and approve of material changes in</td>
</tr>
<tr>
<td></td>
<td>finance/accounting policies</td>
</tr>
<tr>
<td>Internal audit activities</td>
<td>Review internal audit activities</td>
</tr>
<tr>
<td></td>
<td>Monitor independence of the internal audit</td>
</tr>
<tr>
<td>Key personnel selection for critical financial/</td>
<td>Assist CEO in selecting candidates</td>
</tr>
<tr>
<td>control positions</td>
<td>Oversee selection process</td>
</tr>
</tbody>
</table>
Organization Of The Audit Committee

Establishment
- The board should form a committee of independent directors to perform the role of the Audit Committee (AC)
- The board should establish written terms of reference for AC that should provide clear understanding of the AC's role

Composition and qualification
- The AC will typically consist of a minimum three members appointed by the board
- All/most members should have financial/accounting expertise. Legal and other skills as needed
- Should have sound judgment, objectivity, management experience

Term, meeting frequency and other
- Term of AC members must be co-terminous with that of Board members
- AC should meet at least on a quarterly basis
- AC should also meet at least once in absence of management
- Quorum should be 50% of the members, subject to a minimum of 2 members

Independence of AC members
- All should be non-executives, ideally a majority independent.
- Chairman ideally independent with finance/accounting background.
- Members should not be directly responsible for or part of any committee involved in the management functions of the company

Audit Committee Meeting Agenda

Evaluate the internal and independent audit processes
- Coordination of internal and independent audit effort and definition of responsibilities
- Independent auditors
- Internal audit department

Risk Management & Compliance
- Risk management policy document
- Effectiveness of risk management systems
- Oversee work of Compliance function

Assess Processes relating to control environment
- Compliance with code of ethical conduct
- Control policies and procedures
- Internal and independent auditor control observations and recommendations

Audit committee structure
- Update charter
- Assess audit committee performance

Oversee financial reporting
- Financial statements and earnings releases
- Periodic reports and findings
- Management overview of financial results for quarter/year
- Accounting policies

Assess current trends
- Industry and market updates
- Review financial community expectations
- Information technology changes
Audit Committee – Possible Agenda Topics For External/Internal Audit Oversight

<table>
<thead>
<tr>
<th>Topic</th>
<th>External auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recommend appointment and review performance</td>
</tr>
<tr>
<td></td>
<td>Approve audit fees and terms of engagement</td>
</tr>
<tr>
<td></td>
<td>Consider policy in relation to non-audit services</td>
</tr>
<tr>
<td></td>
<td>Consider objectivity/independence and obtain confirmation from auditor</td>
</tr>
<tr>
<td></td>
<td>Review audit plan, scope of work, and receive update</td>
</tr>
<tr>
<td></td>
<td>Review external audit findings</td>
</tr>
<tr>
<td></td>
<td>Discuss appropriateness of accounting policies, estimates and judgments</td>
</tr>
<tr>
<td></td>
<td>Discuss external auditors views on control environment including fraud and risk management</td>
</tr>
<tr>
<td></td>
<td>Discuss with auditor in absence of executives and management</td>
</tr>
<tr>
<td></td>
<td>Ongoing communication (written/oral) of external auditor with audit committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve appointment of Head of Internal Audit (on recruitment)</td>
</tr>
<tr>
<td>Review internal audit plan</td>
</tr>
<tr>
<td>Review significant internal audit reports and findings</td>
</tr>
<tr>
<td>Discuss with auditor in absence of executives and management</td>
</tr>
</tbody>
</table>

Source: Audit Committee Institute – Practical Guide

Key Role Of The Audit Committee – Financial Reporting
Ensure That Processes To Verify Financials Are Systematized

Feedback to next review cycle

- Assess procedures
- Focus on hot spots
- Discuss with key stakeholders

Financial controls
- Numbers accurate?
- Controls sufficient?
- Previous problems corrected

Generation of reports
- What’s the process and who is involved?
- Is process workable – e.g. sufficient time?
- Any concerns of those involved?

Disclosure of hot spots
- Reporting errors?
- Previous problems?

Key difficulties
- Auditor concerns?
- Accounting adjustments?
- Investor/analyst concerns?

Key accounting assumptions
- Revenue, expenses, capital?
- Variances from norms?
- Management/auditor disagreements?

External auditors
- Would they have prepared statement differently?
- Any concerns, e.g. aggressive accounting?
- Qualified statements?

Internal auditors
- Auditor concerns?

Compliance
- Any concerns?
- Complete compliance?
**Key Audit Committee Role - Integrity Of Financial Statements**

With support from the CFO, the committee:

» Reviews significant financial reporting issues and judgments
» Satisfies itself of the clarity/completeness of financial disclosures
» Considers significance of accounting policies, changes, estimates and judgments, unusual transactions and special purpose vehicles
» Determines whether the company has appropriate accounting policies and is making appropriate estimates and judgments
» Reviews financial reporting, accuracy and context of disclosures
» Reports to the board unsatisfactory aspects of the company’s proposed financial reporting
» Reviews related information presented with the financial statements:
  • Operating and financial review
  • Corporate governance
  • Statements relating to audit and risk management

**Whistle-blowing: What The Audit Committee Needs To Know**

» Does the company have whistle blowing procedures?
» Are employees aware of them?
» Can employees raise concerns without risk of censure?
» Does the company act promptly on concerns?
» Are genuine whistle-blowers protected?
» Is there a senior manager responsible?
» Do all managers understand the policy and accept the principle?
» Are all reports advised to the audit committee?
### Audit Committee
#### Leading practices and trends

<table>
<thead>
<tr>
<th>Committee Dynamics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>» Focus on committee composition, including independence, financial expertise, broad business or leadership experience and succession planning</td>
<td></td>
</tr>
<tr>
<td>» Having four or five audit committee members is usually considered most effective, depending on need</td>
<td></td>
</tr>
<tr>
<td>» Conduct an annual committee self-evaluation</td>
<td></td>
</tr>
<tr>
<td>» Consider periodically rotating audit committee members</td>
<td></td>
</tr>
<tr>
<td>» Participate in audit committee training/education activities</td>
<td></td>
</tr>
<tr>
<td>» Engage independent advisors, as necessary</td>
<td></td>
</tr>
<tr>
<td>» Encourage discussion not presentation at meetings</td>
<td></td>
</tr>
<tr>
<td>» Consider providing routine compliance items in advance materials</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Oversight</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>» Increase focus on risk culture and assessment</td>
<td></td>
</tr>
<tr>
<td>» Avoid becoming overly dependent on forms or tools for risk monitoring</td>
<td></td>
</tr>
<tr>
<td>» Periodically re-assess the list of top risks</td>
<td></td>
</tr>
<tr>
<td>» Focus on IT milestones and reporting against them especially in IT transformation</td>
<td></td>
</tr>
<tr>
<td>» Review on acquisitions, including risks, relevant integration milestones and ROI analysis. Also consider post-acquisition reviews to evaluate the reliability of initial acquisition assumptions</td>
<td></td>
</tr>
</tbody>
</table>

Source: Deloitte – Audit Committee Leading Practices and Trends (May 2010)

---

### Audit Committee
#### Leading practices and trends

<table>
<thead>
<tr>
<th>Self-assessment and Evaluation of Effectiveness</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>» Perform a self-assessment in a thorough manner rather as a compliance exercise</td>
<td></td>
</tr>
<tr>
<td>» Consider using self assessment results as a catalyst to re-engineer processes, procedures and agendas</td>
<td></td>
</tr>
<tr>
<td>» Communicate with the board on activities and recommendations</td>
<td></td>
</tr>
<tr>
<td>» Audit committee meeting materials and agendas should be aligned with priority areas:</td>
<td></td>
</tr>
<tr>
<td>• Put significant areas first in advance materials and on the agenda</td>
<td></td>
</tr>
<tr>
<td>• Include and discuss matters for review and comment</td>
<td></td>
</tr>
<tr>
<td>• Present compliance matters for review and comment</td>
<td></td>
</tr>
<tr>
<td>• Meetings should be followed by private and executive sessions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oversight of Internal Controls and Financial Reporting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>» Understand key controls and reporting risk areas as necessary</td>
<td></td>
</tr>
<tr>
<td>» Increase oversight for corporate taxes, an area where high-risk and high dollar decisions are made</td>
<td></td>
</tr>
<tr>
<td>» Leverage the value of internal controls beyond compliance with the assessment and reporting requirements</td>
<td></td>
</tr>
<tr>
<td>» Understand complex accounting and reporting areas</td>
<td></td>
</tr>
<tr>
<td>» Anticipate and understand how pending financial reporting and regulatory developments may affect the company and its talents needs</td>
<td></td>
</tr>
</tbody>
</table>
### Audit Committee

#### Leading practices and trends

<table>
<thead>
<tr>
<th>Relationship with the Independent Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Exercise ownership of the relationship with the independent auditor and get to know the lead partners and meet periodically</td>
</tr>
<tr>
<td>» Establish expectations regarding the nature and method of communication</td>
</tr>
<tr>
<td>» Engage in regular dialogue outside the scheduled meetings</td>
</tr>
<tr>
<td>» Set an annual agenda with the independent auditor and focus on independence, including pre-approval process</td>
</tr>
<tr>
<td>» Provide formal evaluations and regular feedback</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Partnership with the CFO and other Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Focus on the tone at the top, culture, ethics and hotline monitoring</td>
</tr>
<tr>
<td>» Conduct annual evaluations and engage in the forward looking identification of issues</td>
</tr>
<tr>
<td>» Understand plans to address new accounting and reporting requirements</td>
</tr>
<tr>
<td>» Provide input to management’s goal setting</td>
</tr>
<tr>
<td>» Discuss succession planning for the CFO and staff, conduct pipeline and staff reviews including identification of high potential personnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Executive (Private) Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Schedule regular sessions with the internal auditors, independent auditors and management</td>
</tr>
<tr>
<td>» Provide clear objectives and expectations for each meeting and prepare specific topics and questions</td>
</tr>
<tr>
<td>» Understand the response and resolution for each issue raised</td>
</tr>
</tbody>
</table>

### Audit Committee

#### Leading practices and trends

<table>
<thead>
<tr>
<th>Interaction with the Internal Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Assess whether the internal auditors have a direct functional reporting line to the audit committee and an indirect lien to management for administrative activities</td>
</tr>
<tr>
<td>» Be involved with the internal audit risk assessment and audit plans</td>
</tr>
<tr>
<td>» Conduct annual evaluations of Internal audit function</td>
</tr>
<tr>
<td>» Understand internal audit staffing, resources, and succession planning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Executive Compensation</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Periodically conduct meetings with the compensation committee regarding management incentives and related topics</td>
</tr>
<tr>
<td>» Consider in conjunction with the compensation committee the appropriateness of the incentive structure and whether it contributes to increase fraud risk</td>
</tr>
<tr>
<td>» Increase focus on the compensation of officers and directors, including the appropriate use of corporate assets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Orientation and Continuing Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>» Address board education in the company’s corporate governance guidelines to be consistent with regulatory standards</td>
</tr>
<tr>
<td>» Provide orientation of new members involving both company executives and the independent auditor</td>
</tr>
<tr>
<td>» Consider offering continuing education in specialized or regulated industry matters</td>
</tr>
<tr>
<td>» Offer one-on-one and committee-level education</td>
</tr>
</tbody>
</table>
### Expanding Role And Expertise Of The Audit Committee

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management</td>
<td>61%</td>
<td>Technology</td>
<td>26%</td>
</tr>
<tr>
<td>Industry</td>
<td>59%</td>
<td>Other</td>
<td>6%</td>
</tr>
<tr>
<td>Legislative compliance</td>
<td>58%</td>
<td>No additional expertise on</td>
<td>4%</td>
</tr>
<tr>
<td>M&amp;A</td>
<td>39%</td>
<td>the audit committee</td>
<td></td>
</tr>
<tr>
<td>International</td>
<td>32%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tax</td>
<td>27%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit committee’s role in</td>
<td>30%</td>
<td>Significant financial</td>
<td>22%</td>
</tr>
<tr>
<td>risk governance</td>
<td></td>
<td>statements/audit issues and</td>
<td></td>
</tr>
<tr>
<td>Oversight/evaluation of</td>
<td></td>
<td>how they were addressed</td>
<td></td>
</tr>
<tr>
<td>external auditor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(including independence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and objectivity, services,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resource for</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reappointment, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Effectiveness of audit</td>
<td>25%</td>
<td>Oversight of the CFO/finance</td>
<td>15%</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td>team</td>
<td></td>
</tr>
<tr>
<td>Audit committee’s</td>
<td>24%</td>
<td>Oversight of evaluation of</td>
<td>14%</td>
</tr>
<tr>
<td>effectiveness</td>
<td></td>
<td>internal auditor</td>
<td></td>
</tr>
<tr>
<td>(qualification of members,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>performance evaluation, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit committee meetings</td>
<td>23%</td>
<td>None of the above</td>
<td>40%</td>
</tr>
<tr>
<td>(number, attendance, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>22%</td>
<td></td>
<td>1%</td>
</tr>
</tbody>
</table>

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

### INTERNAL AUDIT OVERVIEW
Key Questions: 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?

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 enterprises 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 well.

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 Audit Objective And Tasks

OBJECTIVE: To provide the board and management with reasonable assurance that the organization has a sound system of internal control to protect against loss

- Evaluate the system of internal controls, risk management and CG
- Assess risks / component of risk management
- Test operations of systems (including IT)
- Communication, recommendations for improvement and follow up
Internal Audit Assessment of Risk Management Function

In your opinion, how mature is your organization's risk management function?

- 41% Robust and embedded framework and resources in place
- 20% Implemented, but requires additional work and resources
- 19% In the development stage
- 11% Immature
- 9% We do not have a formal program or resources


Key Features of 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>

**Internal Audit Helps to Monitor the Internal Controls**

- Board, in particular, the Audit Committee oversees
- Internal audit function evaluates
- Managers have primary task to design and maintain controls
- External auditors assess and opines on

- **Monitoring the Internal Control Process**
Outsourcing: Where Internal Audit Gets the Talent they Need


Internal Audit Reporting

Future Of Internal Audit Function: Trusted Advisor

Unrealized value

- Trusted advisor
  - Providing value-added services and proactive strategic advice to the business well beyond the effective and efficient execution of the audit plan.
- Insight generator
  - Taking a more proactive role in suggesting meaningful improvements and providing assurance around risk.
- Problem solver
  - Bringing analysis and perspective on root causes of issues identified in audit findings, to help business units take corrective action.
- Assurance provider
  - Delivering objective assurance on the effectiveness of an organization’s internal controls.


EXTERNAL AUDIT OVERVIEW
KEY QUESTIONS: 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?

Changes In Audit Reporting – IAASB Exposure Draft

INDEPENDENT AUDITOR’S REPORT

To the Shareholders of ABC Company (or Other Appropriate Address)

Report on the Audit of the Consolidated Financial Statements

Opinion

In our opinion, the accompanying consolidated financial statements present fairly, in all material respects, (or give a true and fair view of the) consolidated financial position of ABC Company and its associates (the Group) as at December 31, 20X1, and the consolidated statement of comprehensive income, consolidated statement of changes in equity and consolidated statement of cash flows for the year then ended, and notes to the consolidated financial statements, including a summary of significant accounting policies.

Basis for Opinion

We conducted our audit in accordance with International Standards on Auditing (ISAs). Our responsibilities under those standards are further described in the Auditor’s Responsibilities for the Audit of the Consolidated Financial Statements section of our report. We are independent of the Group, within the meaning of (identify relevant ethical requirements or applicable law or regulation) and have fulfilled our other responsibilities under those ethical requirements.

Key Audit Matters (see ISA 500/11)

Key audit matters are those matters that, in our professional judgment, were of most significance in our audit of the consolidated financial statements. Key audit matters are selected from the matters communicated with (those charged with governance) but are not intended to represent all matters that were discussed with them. Our audit procedures relating to these matters were designed in the context of our audit of the consolidated financial statements as a whole. Our opinion on the consolidated financial statements is not modified with respect to any of the key audit matters described below, and we do not express an opinion on these individual matters.

The fair presentation of the financial statements and other matters are not affected by the facts and circumstances of the individual audit engagement and the entity. Nonetheless, the ISAs contain requirements that apply to any entity and may not be applicable to the individual audit engagement.
External Audit Leading Practices

- 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

INTERNAL CONTROLS OVERVIEW
**Key Questions: 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 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

*COSO – Integrated Framework, May 2013*
## Internal Control Frameworks

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Management oversight and the control culture.</td>
<td>1. Control Environment - The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.</td>
</tr>
<tr>
<td>2. Control activities and segregation of duties.</td>
<td>2. Risk Assessment</td>
</tr>
<tr>
<td>3. Risk recognition and assessment.</td>
<td>3. Control Activities</td>
</tr>
<tr>
<td>4. Information and communication.</td>
<td>4. Information and Communication</td>
</tr>
<tr>
<td>5. Monitoring activities and correcting deficiencies.</td>
<td>5. Monitoring Activities</td>
</tr>
</tbody>
</table>

## 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.
Key Questions: 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?
Compliance And Whistleblowing: How Is Compliance Related To Corporate Governance?

Source: Frame of reference for integrated GRC; Racz, Weiβpl., Seufert , 2010

Risk Governance Overview
Key Questions: 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?

CG Principles Revision Projects Include More Robust Risk Governance

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.

### Risk Culture: Definitions

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

*Institute of International Finance, Final Report of the IIF Committee on Market Best Practices, 2008*

“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

Risk Culture
Recommended best 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)

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. Tacitly 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 borrower(s)
- 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: Board & Management Roles In Risk Governance

- Implement
- Monitor
- Propose (adjustments)
- Review
- Approve

- Policies, high level limits and stress tests
- Senior management

- Executing and monitoring transactions
- Business Operations

- Board
- Audit/Risk committee

Organization: Three Lines of Defense:

- Board Risk Committee
- 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

- 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

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

- Board of Directors
- Board Audit Committee
- CEO and Executive Management

Governance “Above the Line”

Performance “Below the Line”

Embed risk management
Organization: Sample Risk Governance Structure for a Bank

- 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

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:
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

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>
<tr>
<td><strong>TOR</strong></td>
<td><strong>TOR</strong></td>
</tr>
<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
Thank you!