Internal Audit Role in Enterprise Risk Management (ERM)

Presented by:
Dr. Abdelgadir Bannaga, PhD/FCCA

February 2010
Index

Details

Introduction

COSO

Risk

Internal Audit

Audit Process Evolution

Key Considerations for IA Leaders

Developing IA ‘s New Skill Set

Enterprise Risk Management

IA Roles within the Spectrum of ERM Activities

Conclusion
Introduction

- 1987 - issued its initial report.
- As a result of this initial report the Committee of Sponsoring Organizations (COSO) was formed.
COSO is sponsored and funded by 5 main professional accounting associations and institutes: 

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors
Risk

Risk is the possibility that an event will occur and adversely affect the achievement of an objective. It affects all parts of the organization and influences success and failure.
Examples of External Risk Factors

- Competitors
- Natural Hazards
- Customer Needs
- Capital Availability
- Industry
- Legal/political
- Supply Chain Efficiency & Relationship
- Technology
- Shareholders Relations
Examples of Internal Risk Factors

### Internal Risks

<table>
<thead>
<tr>
<th>Process</th>
<th>Examples of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Satisfaction</td>
<td>• Business Interruption • Product/Service Failure</td>
</tr>
<tr>
<td>Health &amp; Safety</td>
<td>• Environment • Contract Commitment</td>
</tr>
<tr>
<td>Product/Service Pricing</td>
<td>• Measurement • Alignment • Delivery Channels</td>
</tr>
<tr>
<td>Knowledge Management</td>
<td>• Physical Security • Product Liability</td>
</tr>
<tr>
<td>Product Development</td>
<td>• Compliance • Change Response • Transaction Processing</td>
</tr>
<tr>
<td>Efficiency</td>
<td>• Strategy • Implementation</td>
</tr>
<tr>
<td>Capacity</td>
<td>• Supply Chain • Partnering</td>
</tr>
<tr>
<td>Performance Gap</td>
<td>• Cycle Time • Sourcing • Relationship Management</td>
</tr>
<tr>
<td>Cycle Time</td>
<td>• Management Fraud • Employee Fraud • Third-Party Fraud</td>
</tr>
<tr>
<td>Sourcing</td>
<td>• Illegal Acts • Unauthorized Acts • Reputation • Ethical Decision Making</td>
</tr>
<tr>
<td>Relationship Management</td>
<td>• Conflict of Interest</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>• Relevance • Data Integrity • Access</td>
</tr>
<tr>
<td>Partnering</td>
<td>• Availability • Infrastructure • Capacity • Reliability • E-Commerce</td>
</tr>
<tr>
<td>Business Interruption</td>
<td>• Leadership • Outsourcing • Hiring/Retention</td>
</tr>
<tr>
<td>Product/Service Failure</td>
<td>• Performance Incentives • Communications • Training/Development</td>
</tr>
<tr>
<td>Environment</td>
<td>• Competencies/Skills • Accountability • Change Readiness • Empowerment • Succession Planning</td>
</tr>
<tr>
<td>Contract Commitment</td>
<td></td>
</tr>
<tr>
<td>Measurement</td>
<td></td>
</tr>
<tr>
<td>Alignment</td>
<td></td>
</tr>
<tr>
<td>Delivery Channels</td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
</tr>
<tr>
<td>Product Liability</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
</tr>
<tr>
<td>Change Response</td>
<td></td>
</tr>
<tr>
<td>Transaction Processing</td>
<td></td>
</tr>
<tr>
<td>Strategy</td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
</tr>
</tbody>
</table>

### Financial

- Interest Rate
- Currency
- Equity
- Commodities
- Financial Instruments
- Cash Flow
- Opportunity Cost
- Concentration
- Default
- Counterparty
- Collateral
- Credit
- Debt Rating
- Liquidity
- Foreign Exchange
- Modeling

### Management Information

- Budgeting & Forecasting
- Regulatory Reporting
- Accounting Information
- Investment Evaluation
- Taxation
- Financial Reporting
- Pension Fund
- Competence/Accuracy

### Integrity

- Management Fraud
- Employee Fraud
- Third-Party Fraud
- Illegal Acts
- Unauthorized Acts
- Reputation
- Ethical Decision Making
- Conflict of Interest

### Technology

- Relevance
- Data Integrity
- Access
- Availability
- Infrastructure
- Capacity
- Reliability
- E-Commerce

### Human Capital

- Leadership
- Outsourcing
- Hiring/Retention
- Performance Incentives
- Communications
- Training/Development
- Competencies/Skills
- Accountability
- Change Readiness
- Empowerment
- Succession Planning
Corporate Scandals

A strong corporate governance of managing risks becomes a necessity. To do that you need to have effective and efficient Internal Audit which identifies all the business risks in the organization.
What is Internal Audit?

The Institute of Internal Auditors (IIA) defines internal auditing as:

“Internal Auditing is an independent objective assurance and consulting activity designed to add value and improve on 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”.

This definition recognizes two roles for internal audit:

a) Independent assurance role (board and audit committee)
b) Consulting role (Management)
What is Internal Audit? Contd.

The internal audit is performed by professionals with an in depth understanding of the business culture systems and processes, the internal audit activity provides assurance that internal controls in place are adequate to mitigate the risks, governance processed are affective and efficient, and organizations goals and objectives are met.

The internal audit activity evaluates risk exposures relating to the organizations’ governance, operations and information systems in relation to:

- Effectiveness and efficiency of operations
- Reliability and integrity of financial and operational information
- Safeguarding of assets.
- Compliance with Laws, regulations and controls.
Audit Process Evolution

Control Based Auditing
- Compliance with Laws and regulations
- Financial accuracy of account balances
- Operation of specific controls procedures

Process Based Auditing
- to determine the efficiency and effectiveness of key operational processes.

Risk Based Auditing
- Identification of Risks and controls in place to mitigate those risks (On a risk by risk basis)

Enterprise Risk Management
- Take a portfolio view of risk across the enterprise at every level and unit.
- Aim to protect and enhance enterprise value.
Key Considerations for IA Leaders

- Focus on the future
- Integrate ERM
- Augment skill sets and leverage resources
- Focus on fraud
- Establish an adviser role
- Build continuous audit capability and influence continuous monitoring techniques
- Maintain independence and objectivity
- Provide value-added assurance services
- Leverage access to management
Developing Internal Audit’s New Skill Set

- Industry knowledge and functional expertise (strategic operational knowledge)
- Cross-culture training for global IA functions
- Improved interpersonal skills to allow for effective communication with process owners/line managers
- ERM – risk management and evaluation
- Fraud skills
- IT – automation of internal control environment
- Specific certifications, CFE, CFA, CIA, CFSA, CGAP, CCSA, CISA, and others should be considered in
- Augmenting internal audit staff
What is Enterprise Risk Management (ERM)?

COSO defined ERM as follows:

“Enterprise Risk Management (ERM) is a process effected by an entity’s board of directors, management, and other personnel, applied in strategic setting and across the enterprise, designed to identify potential events that may affect the entity and manage risks to be within its risk appetite to provide reasonable assurance regarding the achievement of an entity objectives”.

13
What is Enterprise Risk Management (ERM)? Contd.

Effective ERM

- Helps achieve objectives
- Is an ongoing entity wide process to identify, evaluate, analyze, respond, monitor, and communicate on risks.
- Is effected by people at all levels
- Occurs in a strategic setting
- Applies to every unit
- Provide reasonable assurance
- Enable continuous improvement in decision making
- Provides reasonable assurance
- Helps achieve objectives
- Is an ongoing entity wide process to identify, evaluate, analyze, respond, monitor, and communicate on risks.
- Is effected by people at all levels
- Occurs in a strategic setting
- Applies to every unit
- Provide reasonable assurance
- Enable continuous improvement in decision making
COSO ERM Integrated Framework

- ERM Principle Processes
  - Internal Environment
  - Objective Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
  - Control Activities
  - Information and Communication
  - Monitoring

- Four Types of Management Objectives:
  - Strategic
  - Operations
  - Reporting
  - Compliance

- Encompasses the Entire Enterprise
  - Enterprise-Level
  - Subsidiary
  - Business Unit
  - Division

- Enterprise risk management requires an entity to take a portfolio view of risk.
- Management considers how individual risks interrelated in the eight components of the framework
- Management develops a portfolio view from each perspective
# ERM Principle Processes

<table>
<thead>
<tr>
<th><strong>Internal Environment</strong></th>
<th>• The internal environment encompasses the tone of an organization</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective Setting</strong></td>
<td>• Objectives must exist before management can identify potential events affecting their achievement</td>
</tr>
<tr>
<td><strong>Event Identification</strong></td>
<td>• Internal and external events affecting achievement of an entity’s objectives, must be identified distinguishing between risks and opportunities</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>• Risks are analyzed considering likelihood and impact, as a basis for determining how they should be managed</td>
</tr>
<tr>
<td><strong>Risk Response</strong></td>
<td>• Management select risk responses to align risks with the entity’s risk tolerances and risk appetite</td>
</tr>
<tr>
<td><strong>Control Activities</strong></td>
<td>• Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out</td>
</tr>
<tr>
<td><strong>Information &amp; Communication</strong></td>
<td>• Relevant information is identified captured and communicated in a form and timeframe that enable people to carry out their responsibilities</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>• The entire process is monitored and modifications are made as needed.</td>
</tr>
</tbody>
</table>
## Benefits of ERM

- Greater likelihood of achieving those objectives;
- Consolidated reporting of disparate risks at board level;
- Improved understanding of the key risks and their wider implication.
- Identification and sharing of cross business risks;
- Greater management focus on the issues that really matter;
- Fewer surprises or crises;
- More focus internally on doing the right things in the right way;
- Increased likelihood of change initiatives being achieved;
- Capacity to take on greater risk for greater rewards and
- More informed risk-taking and decision making.
Strengthening ERM for Strategic Advantage

The recent financial crises is leading to renewed focus on how senior executives approach risk management and the role of their boards of directors in risk oversight. COSO issued a paper about ways to strengthen risk management in their organizations.

Review of the environment calls for organization to re-examine their risk management practices.

Highlight the following four specific areas where senior management can work with its board to enhance the board’s risk oversight capabilities.

1) Discuss Risk management Philosophy and Risk Appetite
2) Understand Risk management Practices
3) Review Portfolio Risks in Relation to Risk Appetite
4) Be apprised of the Most significant Risks and Related Responses
Elements of Risk Appetite

- **Existing Risk Profile**
  - The existing level and distribution of risk across risk categories (e.g., financial, market risk, operational risk, reputation risk, etc.)

- **Risk Capacity**
  - The maximum risk a firm may bear and remain solvent

- **Risk Tolerance**
  - Acceptable levels of variation any entity is willing to accept around specific objectives

- **Desired Level of Risk**
  - What is the desired risk/return level

**Determination of Risk Appetite**
Internal Audit Roles Within the Spectrum of ERM Activities
Internal Audit Roles Within the Spectrum of ERM Activities Contd.

Core internal audit roles:
- Give assurance on the risk management process
- Give assurance that risks are correctly evaluated
- Evaluate risk management processes
- Evaluate the reporting of key risks
- Review the management of key risks

Legitimate internal audit roles with safeguards:
- Facilitate identification and evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Consolidate reporting of risks
- Maintain and develop the ERM framework
- Championing establishment of ERM
- Developing ERM strategy for board approval

Roles internal audit should NOT undertake:
- Setting the risk appetite
- Imposing risk management process
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management’s behalf
- Accountability for risk management
Conclusion

COSO’s new chairman

David Landsittel gave his views on *What role does he think internal auditors play in the ERM process*

ERM is recognized to some extent outside the US. ERM is still in the early stage. People tend to view the role of internal auditor as providing assurance over the effectiveness of the process.

Although no single event caused the crisis, a myriad of failures—including breakdowns in governance, risk management, and internal control—brought the global financial system to a screeching halt. As organizations move from assigning blame toward a forward-looking, "lessons learned" era, they must take steps to make sure a breakdown of this magnitude doesn't happen again. "Changes in risk arising from changed business models were apparent in the crisis,"

He said in addition "I think there is an opportunity for internal auditors, particularly those in mid-market and smaller enterprises, to take more of a hands-on approach to ERM implementation and to play a key role that extends beyond the assurance process. That's because the skills of the internal audit group are consistent with the skills needed for those who oversee the ERM process, and the relationships that internal auditors build are consistent with what is needed in building an ERM process.."

He said in addition to the above, he would like to see that internal auditors take more of a hand on approach to ERM implementation and to play a key role that extends beyond the assurances process. Because internal auditors have training and experience in business process evaluation, they are well equipped to identify and assess risks, and that they are effective in formulating recommendations on how to mitigate risks. These skills are fundamental to ERM as well.

During the last financial crises many company’s’ were hit very hard by risks which they never expected. I believe it is important at all times to strengthen the approach to risk management. We hope that we learned a lot of lessons from the crises and put all the lessons into action plan. The management must ensure that internal audit professionals must lean the right capabilities to carry out the plan and achieve all its objectives.