Practical Approach towards Risk Based Internal Audit

Presented by CA Manoj Agarwal
Feb 10, 2016, Ernakulum, IASB, ICAI
Disclaimer

All the contents of the presentation constitute the opinion of the speaker, and the speaker alone; they do not represent the views and opinions of the speaker’s employers, supervisors, nor do they represent the view of organizations, businesses or institutions the speaker is, or has been a part of.
Agenda

• What is Risk?
• COSO ERM Framework
• 3 Lines of Defence Model
• Definition of Internal Audit
• Risk Based Internal Audit
• Tools
What is Risk?

Risk, in traditional terms, is viewed as a ‘negative’. The Chinese give a much better description of risk:

- The first is the symbol for “danger”, while
- the second is the symbol for “opportunity”, making risk a mix of danger and opportunity.

“Risk- let’s get this straight up front – is good. The point of Risk management is not to eliminate it; that would eliminate reward. The point is to manage it – that is, choose to place bets, where to hedge bets, and where to avoid betting together.” - Thomas A. Stewart
Risk & Risk Management

In economic terms, profit is the reward for entrepreneurship or “Risk Taking”

As a lay investor, our investment planning is based on risk perception – bank deposits, life insurance, debentures and GoI bonds, Mutual Funds, Shares, Private Equity...

Risk management is an attempt to identify, measure and monitor risks– so as to manage uncertainty.
Risk Management

1. Understand the nature and extent of risks facing the company

2. Understand the extent and categories of risks which it regards as acceptable for a company to bear

3. Understand the likelihood of risks concerned materializing

4. Company’s ability to reduce the incidence and impact on business of risks that do materialize

5. Costs of operating particular controls relative to benefits
Classification of Risks

Strategic
• A strategic risk is a risk that a company is exposed to when pursuing its business objectives, or likely loss arising from a poor strategic business decision. e.g. Too much dependence on one line of business; or a failed acquisition

Operational
• Operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. e.g. Frauds in Banking; Risk of poor planning e.g. Funds constraint

Compliance
• Risks a company is exposed to because of breach of law / regulatory requirement. e.g. Non compliance in foreign country due to ignorance.
The Need for Risk Management

- Complex, ever changing macro environment
- Sustainable, profitable growth to meet stakeholder expectation
- Trend towards greater transparency & enhanced levels of corporate governance

# Move from survival to competitive advantage
Eight Components of COSO ERM Model

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring
Eight Components of COSO ERM Model

**ERM Process**

**Objective Setting**

**Event Identification**
- Events – Factors Influencing Strategy and Objectives – Methodologies and Techniques
- Event Interdependencies
- Event Categories – Risks and Opportunities

**Risk Assessment**
- Inherent and Residual Risk – Likelihood and Impact
- Methodologies and Techniques – Correlation

**Risk Response**
- Identify Risk responses – Evaluate Possible Risk Responses – Select Responses – Portfolio View

**Control Activities**
- Integration with Risk Response – Types of Control Activities – General Controls
- Application Controls – Entity Specific

**Information & Communication**
- Information – Strategic and Integrated Systems – Communication

**Monitoring**
- Separate Evaluations – Ongoing Evaluations
Top Risks - Global Risk Report 2016-WEF

Figure 1: The Global Risks Landscape 2016
Three Lines of Defence Model

Three groups (or lines) involved in effective risk management:

- Functions that own and manage risks.
- Functions that oversee risks.
- Functions that provide independent assurance.

The Three Lines of Defense Model
1st LoD: Operational Management

- Own and manage risks.
- Responsible for implementing corrective actions to address process and control deficiencies.
2nd LoD: Risk Management & Compliance Functions

• Risk management function
  – Facilitates and monitors the implementation of effective risk management practices by operational management
  – Assists risk owners in defining the target risk exposure
  – Reporting adequate risk-related information throughout the organization.

• Compliance function
  – Monitor various specific risks such as noncompliance with applicable laws and regulations.
  – Multiple compliance functions for specific types of monitoring, such as health and safety, supply chain, environmental, or quality monitoring.

• Controllership function
  – Monitors financial risks and financial reporting issues.
3rd LoD: Internal Audit

• Comprehensive assurance based on the highest level of independence and Objectivity

• Provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve

• Risk management and control objectives.

• Reported to senior management and to the governing body, usually covers
  
  – A broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, procedures, and contracts.
  
  – All elements of the risk management and internal control framework, which includes: internal control environment
  
  – The overall entity, divisions, subsidiaries, operating units, and functions — including business processes as well as supporting functions.
External Auditors, Regulators, Other external Bodies

• Can have an important role in the organization’s overall governance and control structure.
• Regulators sometimes set requirements intended to strengthen the controls in an organization and on other occasions perform an independent and objective function to assess the whole or some part of the first, second, or third line of defense with regard to those requirements.
Coordinating The Three Lines Of Defense

- Role of each group in the risk management process

<table>
<thead>
<tr>
<th>FIRST LINE OF DEFENSE</th>
<th>SECOND LINE OF DEFENSE</th>
<th>THIRD LINE OF DEFENSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Owners/Managers</td>
<td>Risk Control and Compliance</td>
<td>Risk Assurance</td>
</tr>
<tr>
<td>• operating management</td>
<td>• limited independence</td>
<td>• internal audit</td>
</tr>
<tr>
<td></td>
<td>• reports primarily to management</td>
<td>• greater independence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• reports to governing body</td>
</tr>
</tbody>
</table>
“Internal audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control system. Internal audit, therefore, provides assurance that there is transparency in reporting, as a part of good governance.”

- The Internal Audit Standards Board of the ICAI

“Internal auditing is 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”

- Definition of Internal Auditing by Institute of Internal Auditors (IIA)
## Risk Based Audits

| Risk Based Audit | Risk based Internal Audit (RBIA) is an internal methodology which is primarily focused on the inherent risk involved in the activities or system and provide assurance that risk is being managed by the management within the defined risk appetite level.[1] It is the risk management framework of the management and seeks at every stage to reinforce the responsibility of management and BOD (Board of Directors) for managing risk |

Building a Risk aware enterprise

BOD
Oversight of
Risk Management

(1) Synthesizes issues for the Board
(2) Establish ERM Policies & Tolerances
(3) Reviews significant risk issues
(4) Ensures governance & Infrastructure for management of risk profile

Risk Management Committee

Functional Head

(1) Own Risk Management & Mitigation
(2) Perform Risk assessments on periodic basis
(3) Provide assertions on risk exposure for their business area.

Risk Governance

Risk Infrastructure and Management

Risk Ownership
Risk Based Auditing: Approach

1. Identification of Audit Universe
2. Breaking Audit universe into auditable units.
3. Risk Identification
4. Risk Assessment & evaluation
5. Risk Scoring/ Heat Map
6. RBIA Plan
7. Execution
8. Reporting
Risk Identification

**Analysis of processes:**
Will facilitate identification of the operational risk

**Brainstorming:**
A group of employees put forward their ideas or sensations of risk

**Interview:**
Interview with various management level members in order to elicit their concerns

**Workshops:**
Meeting the employees in order to identify the risks and assess impact

**Comparison with other organisations:**
Benchmarking is the technique used for comparing one’s own organisation with competitors
After identifying and analysing the risk, next step is the evaluate the risk.

**What is likelihood of the risk event occurring?**

*Probability*
- Almost certain
- Likely
- Moderate
- Unlikely
- Rare

**What is the consequence if the risk event occurs?**

*Impact*
- Extreme
- Very High
- Moderate
- Low
- Negligible
Components of Risk Evaluation

Legal Risk
- Legal Action by Counter – party
- Non enforcement of the Legal rights

Operational Risk
- Process complexity
- Volume
- Documentation
- Staffing
- Outsourcing
- Importance of MIS & safe-keeping
- Fraud control
- Auditors’ findings
- Budget variations

Financial Risk
- Size
- Industry Trends
- Credit risk
- Market risk
- Forex risk
- Settlement risk

Regulatory Risk
- Number of Regulators and Acts
- Complexity of Acts
- Applicability of international Laws

Information Technology Risk
- Dependence on IT systems
- Scalability / Up gradation
- Documentation
- Confidentiality of the data
- Number of interfaces
- Vendor support
- Skills / Training
- External agencies involvement

Reputation Risk
- Impact of Process
- Extent of customer interaction
- Effect on Future Business Plans
- Reputation risk wrt operations outsourcing
Example

Criticality Classification = Probability of Occurrence * Impact
Risk Scoring/ Heat Map

Plotting of Criticality score on a chart.
A Risk Based Plan will look like this

<table>
<thead>
<tr>
<th>Sr</th>
<th>Criticality</th>
<th>Criticality Score</th>
<th>Process Name</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High</td>
<td>25-30</td>
<td>• Revenue</td>
<td>Quarterly to Half Yearly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Human Resource</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
<td>20-25</td>
<td>• Accounts Payable</td>
<td>Half Yearly to Once in a year</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Fixed Assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Compliances</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>Below 25</td>
<td>• Admin Functions</td>
<td>Annual to Once in Two Year</td>
</tr>
</tbody>
</table>
Coverage of Key Financial Components in the Audit Plan
## Sample Criteria for Rating Observations

<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Critical</th>
<th>Major</th>
<th>Moderate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FINANCIAL</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Financial Exposure</td>
<td>&gt; Rs 5 Cr</td>
<td>Rs 1-5 Cr</td>
<td>Rs 1 Lakh to &lt; Rs 1 Cr</td>
</tr>
<tr>
<td><strong>COMPLIANCE</strong></td>
<td>AND/OR</td>
<td>AND/OR</td>
<td>AND/OR</td>
</tr>
<tr>
<td>Legal &amp; Regulatory</td>
<td>Prosecution or penalty exposure &gt; Rs 1 lakh</td>
<td>Penalty exposure &lt; Rs 1 Lakh</td>
<td>Any technical non-compliance (not resulting in penalty)</td>
</tr>
<tr>
<td>Fraud Vulnerability</td>
<td>Any observation on probability of fraud</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td><strong>OPERATIONAL</strong></td>
<td>AND/OR</td>
<td>AND/OR</td>
<td>AND/OR</td>
</tr>
<tr>
<td>Policy &amp; Procedures</td>
<td>Policy, procedures and practice doesn’t exist</td>
<td>Policy, procedures in place but not in practice</td>
<td>Policy, procedures not documented but practice exists</td>
</tr>
<tr>
<td>Transaction Error (incl SLA)</td>
<td>&gt; 20% of audit sample selected</td>
<td>5% to 20% of audit sample selected</td>
<td>&lt; 5% of audit sample selected</td>
</tr>
<tr>
<td>Repeat audit finding</td>
<td>Last rating Critical or Major</td>
<td>Last rating Moderate</td>
<td>NA</td>
</tr>
<tr>
<td>Customer Impact</td>
<td>Impacts &gt; 1% of customer base (complaints)</td>
<td>Impacts 0.5% to 1% of customer base (complaints)</td>
<td>Impacts &gt; 0.5% of customer base (complaints)</td>
</tr>
<tr>
<td>Systems &amp; Tools</td>
<td>Loss or exposure of confidential master or transaction data, System Availability impacting business performance</td>
<td>Lack of adequate system validations/ access control (incl password management)/ controls which might lead to fraud</td>
<td>System bugs or functionality gaps impacting efficiency, speed of execution</td>
</tr>
</tbody>
</table>
# Report Rating Criteria

<table>
<thead>
<tr>
<th>Report Rating</th>
<th>Critical</th>
<th>Major</th>
<th>Moderate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable</td>
<td></td>
<td></td>
<td>Less than 4</td>
</tr>
<tr>
<td>Needs Improvement</td>
<td>1</td>
<td>1 to 2</td>
<td>More than or = 4</td>
</tr>
<tr>
<td>Unsatisfactory</td>
<td>2 to 3</td>
<td>3 to 5</td>
<td></td>
</tr>
<tr>
<td>Poor</td>
<td>More than 3</td>
<td>More than 5</td>
<td></td>
</tr>
</tbody>
</table>

**Conversion factor:**

1 Critical observation = 2 Major Observations = 4 Moderate Observations
Auditor’s Dilemma

Cost

Dilemma

- Use of Resources
- Use of resources
- Significance-Depth of audit
- Relevance-What to audit
- Coverage-How much to audit

Giving a level of confidence that IA has captured and assessed ‘all’ material risk that threaten the company
# Risk Based Audit

<table>
<thead>
<tr>
<th>Type</th>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
<th>Stage 5</th>
<th>Stage 6</th>
<th>Stage 7</th>
<th>Stage 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBIA</td>
<td>Framework</td>
<td>Defining Scope</td>
<td>Mapping</td>
<td>Risk Registration/Identification</td>
<td>Control Identification</td>
<td>Control Investigation</td>
<td>Audit Test</td>
<td>Audit Report</td>
</tr>
<tr>
<td>Risk profiling</td>
<td>Risk taxonomies</td>
<td>Business unit mapping</td>
<td>Risk register Risk evaluation</td>
<td>Control owner</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume</td>
<td>Risk definition</td>
<td>Processes Systems</td>
<td>All risks Risk type</td>
<td>Material and potential loss from control weakness</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
<td>KPIs Function boundaries</td>
<td>Risk levels Risk Sizes</td>
<td>Criteria to assess whether the control has been operated effectively or compromised by staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity</td>
<td>Includes</td>
<td>Transactions</td>
<td>Statistical tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>Excludes Driver</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOP</td>
<td>Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Past losses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Criteria to Assess**: Whether the control has been operated effectively or compromised by staff.
# My Risk Based Audit

<table>
<thead>
<tr>
<th>Type</th>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
<th>Stage 5</th>
<th>Stage 6</th>
<th>Stage 7</th>
<th>Stage 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBIA</td>
<td>Framework</td>
<td>Defining Scope</td>
<td>Mapping</td>
<td>Risk Registration/ Identification</td>
<td>Control Identification</td>
<td>Control Investigation</td>
<td>Audit Test</td>
<td>Audit Report</td>
</tr>
<tr>
<td>My IA</td>
<td>Financial</td>
<td>Scoping</td>
<td>Mapping</td>
<td>Top 3 Risks</td>
<td>Control Identification</td>
<td>Checkpoints</td>
<td>Testing</td>
<td>Audit report</td>
</tr>
<tr>
<td></td>
<td>Trial balance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Common size</td>
<td>Identification</td>
<td>Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>statement</td>
<td>of major items</td>
<td>of Major Items</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>groups</td>
<td>with in group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FA, Bank</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td>Pareto Rule</td>
<td>Audit Tracker,</td>
<td>Excel (Pivot, Sort, Index, vlookup),</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Audit Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Benford Law, Pareto Rule (80:20)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Tools

<table>
<thead>
<tr>
<th>Audit Tracker</th>
<th>1. Contacts (of auditee/ audit team)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Status Tracker (Scope, Start Date, Completion date, Reason for Pending, responsibility, Population, Sample, Sample methodology, remarks)</td>
</tr>
<tr>
<td></td>
<td>3. Review Notes</td>
</tr>
<tr>
<td></td>
<td>4. Requirement Tracker (Requirement, Area, Responsibility, Request Date, Received date, Time Lag in receipt of data, days lapsed)</td>
</tr>
<tr>
<td></td>
<td>5. Checklist (Scope, Sub scope, Risk, Control, Checkpoints, Population, Sample, Exceptions, Observations, Backup paper)</td>
</tr>
<tr>
<td></td>
<td>7. Audit Completion Checklist</td>
</tr>
</tbody>
</table>

Control Failure Vs. impact of business control failure
Traffic Light vs. specific financial amounts
# Tools

<table>
<thead>
<tr>
<th>Audit Report</th>
<th>1. Cover letter,</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Background and Objective of audit</td>
</tr>
<tr>
<td></td>
<td>3. Scope and approach</td>
</tr>
<tr>
<td></td>
<td>4. Detailed Observation (High, Medium, Low)</td>
</tr>
<tr>
<td></td>
<td>5. Other Points for Management Attention</td>
</tr>
<tr>
<td></td>
<td>6. Positive assurance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit Presentation</th>
<th>1. Audit Summary (Area, Location, Audit Period, Audit Team, Function Head, Scope, Field audit dates/ period)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Scope, Sampling and Limitation to scope</td>
</tr>
<tr>
<td></td>
<td>3. Positive Assurance</td>
</tr>
<tr>
<td></td>
<td>4. Key Observations</td>
</tr>
<tr>
<td></td>
<td>5. Other observations</td>
</tr>
</tbody>
</table>
Resources

• Risk Based Audit: https://drive.google.com/file/d/0B9LJxar8oKPmQ0JxaEpJRmxMaVU/edit?usp=sharing
• Risk Template: https://app.box.com/s/p7tns5kbrliny06mnouu
• www.auditnet.org for audit programs
• www.knowledgeleader.com for audit program
• www.cebglobal.com for audit trends
• www.globaliia.org
• www.coso.org
My Blogs and Post

1. Audit Client Categories
2. Role of Internal Audit
3. Value addition by internal audit
4. Revenue Assurance
5. Companies Act 2013 and Control Catalogues
6. Internal Controls in eCommerce Companies
7. How to create Internal Control Framework for your company
8. Creating An Internal Audit Plan
9. Governance for Approval Matrix
10. Right to Audit
11. Have you included vendor audit as part of your audit plan?

Manoj Agarwal
manojbagarwal@gmail.com
9820392252
Linkedin: https://in.linkedin.com/in/manojbagarwal