ENTERPRISE RISK MANAGEMENT (ERM)

The Conceptual Framework
ENTERPRISE RISK MANAGEMENT (ERM)

ERM Definition
The Conceptual Frameworks: CAS and COSO
Risk Categories
Implementing ERM
Why ERM?
ERM Maturity Model
Key Factors for ERM Success
ERM Definition
ERM Definition

ERM is the discipline by which an organization in any industry
● assesses;
● controls;
● exploits;
● finances; and
● monitors
risks from all sources for the purpose of increasing the organization short- and long-term value to its stakeholders.

(Casualty Actuarial Society, Overview of Risk Management P. 10)
ERM is a process, affected by an entity’s board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to **identify** potential events that may affect the entity, and **manage** risk to be within its **risk appetite**, to provide **reasonable assurance** regarding the achievement of entity goals.”

(COSO, ERM-Integrated Framework, P. 8)
The Conceptual Frameworks for ERM
Conceptual Frameworks

- Casualty Actuarial Society (CAS) Framework
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework
CAS Framework

Hazards  Financial Risk

Operational Risk  Strategic Risk

- Establish Context
- Identify Risks
- Analyze/Quantify Risks
- Integrate Risks
- Assess/Prioritize Risks
- Treat/Exploit Risks

Monitor & Review
COSO Framework

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring
Merging CAS and COSO Models

Information Risk

Hazards

Financial Risk

Operational Risk

Strategic Risk

Compliance Risk

1. Establish Context
2. Identify Risks
3. Analyze/Quantify Risks
4. Integrate Risks
5. Assess/Prioritize Risks
6. Treat/Exploit Risks

Monitor & Review
Risk Categories
Hazards

- Fire
- Tornadoes
- Storms
- Hurricanes
- Earthquakes
- Terrorism
- Injuries to Employees and Third Parties
Financial Risk

- Adverse movement in exchange rates
- Adverse movement in interest rates
- Adverse movement in price and costs
- Credit Risk
- Liquidity Risk
- Bankruptcy Risk
Operational Risk

- Employee fraud
- Labor relations
- Production breakdowns
- Supply chain problems
- Problems in distribution
- Product quality issues
- Physical safety and security
Strategic Risk

- Fluctuations in demand
- Competitors entry / rivalry
- Increase in intensity of competition
- Technological advances
- Social changes having an adverse impact on the business
- Economic cycles
- Adverse legislation
Information Risk

- Incorrect information leading to incorrect decision making
- Unavailability of required information
- Unauthorized access to confidential information by competitors
- Malicious attacks
- Cyber Crime
- Loss of Claims / lawsuits by the parties whom confidential information is disclosed
Compliance Risk

- Penalties and fines
- Reputation losses
- Claims by third parties
- Lawsuits
- Lack of understanding the law
- Inability to comply with a law or standard
- Losing patents / legal rights
Implementing ERM

Step 1: Establish Context
The Conceptual Framework

Information Risk

Hazards

Operational Risk

Financial Risk

Strategic Risk

Compliance Risk

19
Establish Context

- Define the relationship of organization with its external and internal environment
- Perform SWOT Analysis
- Identify stakeholders
- Understand organization’s objectives and strategies
- Identify Key Performance Indicators (KPIs)
- Identify relevant key risk categories
- Identify existing risk management practices
- Determine the “Risk Appetite” of management
## SWOT Analysis

<table>
<thead>
<tr>
<th></th>
<th>Positive Risk</th>
<th>Negative Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal</strong></td>
<td>Strengths</td>
<td>Weaknesses</td>
</tr>
<tr>
<td><strong>External</strong></td>
<td>Opportunities</td>
<td>Threats</td>
</tr>
</tbody>
</table>
## SWOT Analysis – An example

<table>
<thead>
<tr>
<th>Positive risk</th>
<th>Negative risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td>• Our tradespeople are exceptionally skilled</td>
<td>• Our tools of trade are second hand and may be unreliable</td>
</tr>
<tr>
<td>• We have excellent relationships with our existing customers</td>
<td>• Ageing workforce</td>
</tr>
<tr>
<td>• Our work is considered high quality and our service reliable.</td>
<td>• Limited familiarity with new technology.</td>
</tr>
<tr>
<td><strong>Opportunities</strong></td>
<td><strong>Threats</strong></td>
</tr>
<tr>
<td>• The only other plumber in town wants to retire</td>
<td>• Somebody from out of town might buy retiring plumber's business</td>
</tr>
<tr>
<td>• A new industry development is currently tendering to outsource trade services.</td>
<td>• Another business may start up in town</td>
</tr>
<tr>
<td></td>
<td>• Difficulties in recruiting new staff due to skill shortages</td>
</tr>
<tr>
<td></td>
<td>• Loss of an existing employee leaving the business unable to cope with workload.</td>
</tr>
</tbody>
</table>
Stakeholders Analysis

- Shareholders
- Potential Investors
- Management
- Employees
- Creditors / Bankers
- Government
- General Public

Requirements of all stakeholder groups with respect to risk management
Key Performance Indicators

- Return on Capital Employed
- Net Profit of each division
- Customer Satisfaction Index
- % of Sales Returns
- Current Ratio
- Financial and Operating Leverage
- HR Training Hours
Implementing ERM

Step 2: Identify Risk
The Conceptual Framework

Hazards

Information Risk

Operational Risk

Financial Risk

Compliance Risk

Strategic Risk

Establish Context → Identify Risks → Analyze/Quantify Risks → Integrate Risks → Assess/Prioritize Risks → Treat/Exploit Risks

Monitor & Review
How to identify risks?

- Perform brainstorming sessions
- Perform risk surveys
- Conduct risk workshops
- Review and discuss internal audit reports
- Review and discuss reports of other assurance groups e.g. health & safety, quality assurance, security management etc.
Developing the Risk Universe
Developing the Risk Universe

Risk category: Safety

- Staff injury
  - Breach of compliance with OH&S regulations
  - Poor understanding of regulations
  - Lack of training

- Customer injury
  - Inability to respond to an emergency
  - Insufficient resources

- Inappropriate signage
- No hazard identification tools
- No feedback mechanisms

Risk category: Casual factor
## Developing the Risk Register

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cybercrime, including virus damage, identity theft, spyware, general fraud</td>
<td>2</td>
<td>Costs associated with online transactions outweigh benefits associated with initiative</td>
<td>Breach of regulations within e-business legislation</td>
</tr>
</tbody>
</table>

**Impact**

**Consequence**

**Likelihood**

**Level of risk**

**Risk priority**

**Treatment options**
Implementing ERM

Step 3: Analyze / Quantify Risks
The Conceptual Framework

Hazards

Information Risk

Operational Risk

Compliance Risk

Financial Risk

Strategic Risk

Establish Context → Identify Risks → Analyze/Quantify Risks → Integrate Risks → Assess/Prioritize Risks → Treat/Exploit Risks → Monitor & Review
Risk Measurement

Overall Risk = Likelihood \times Magnitude

\[ \text{Likelihood} \times \text{Magnitude} \]

- High Likelihood, High Magnitude: Extreme
- High Likelihood, Low Magnitude: Moderate
- Low Likelihood, High Magnitude: High
- Low Likelihood, Low Magnitude: Low
Risk Analysis Tools

- Qualitative Risk Analysis
- Fault Tree Analysis
- Probability Distribution (for Likelihood)
- Maximum Loss Estimation (for Magnitude)
- Risk and Control Matrix
## Qualitative Risk Analysis

<table>
<thead>
<tr>
<th>LEGEND</th>
<th>Extreme</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Almost certain</td>
</tr>
<tr>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Almost certain to occur at some time.</td>
</tr>
<tr>
<td>Commercial</td>
<td>Finance</td>
<td>Security</td>
<td>Safety</td>
<td>Legal and regulatory compliance</td>
<td></td>
</tr>
<tr>
<td>Significant</td>
<td>Loss &gt; 30% of total income or budget.</td>
<td>Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Significant reputation damage.</td>
<td>Death of multiple injuries requiring hospitalisation.</td>
<td>Investigation by authority and significant penalty awarded. Very serious litigation, including class actions. Closure of business.</td>
<td>Extreme</td>
</tr>
<tr>
<td>Major</td>
<td>Loss of 20–30% of total income or budget.</td>
<td>Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Some reputation damage.</td>
<td>Major injury requiring hospitalisation.</td>
<td>Major breach with potential major penalty and/or investigation and prosecution by authority. Major litigation. Future of the business threatened.</td>
<td>Extreme</td>
</tr>
<tr>
<td>Moderate</td>
<td>Loss of market share. Current clients are retained but no new clients for 1–3 months.</td>
<td>Staff threat resulting in some injury but no hospitalisation required. Minor reputation damage.</td>
<td>Minor injury – first aid required.</td>
<td>Serious breach with investigation by or report to authority. Moderate penalty possible.</td>
<td>High</td>
</tr>
<tr>
<td>Minor</td>
<td>Loss &lt; 10% of income or total budget.</td>
<td>Staff threatened, but no injury. No reputation damage.</td>
<td>No injury.</td>
<td>Low-level legal issue. Penalty or prosecution unlikely.</td>
<td>High</td>
</tr>
</tbody>
</table>
Fault Tree Analysis

- Fire breaks out
  - Leakage of flammable fluid
  - Ignition source is near fluid
    - Spark exists
    - Someone smokes
Probability Distribution

![Probability Distribution Graph]

- Loss
- Probability

## Maximum Loss Estimation

<table>
<thead>
<tr>
<th>Risk</th>
<th>Maximum Possible Impact</th>
<th>Estimated Loss in $ million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earthquake</td>
<td>Entire factory will be destroyed</td>
<td>45,000</td>
</tr>
<tr>
<td>Sensitive information hacked</td>
<td>Lawsuits, advantage gained by competitors</td>
<td>15,300</td>
</tr>
<tr>
<td>Terrorist attack</td>
<td>Some facilities will be damaged</td>
<td>5,000</td>
</tr>
<tr>
<td>Competitor launched new product</td>
<td>Market share will be lost by 30%</td>
<td>3,000</td>
</tr>
</tbody>
</table>
Risk & Control Matrix

Example "What Can Go Wrong" Questions

What ensures that coding of purchases is correct?

- Accounts payable subledger is reconciled to the general ledger.
- Accounts payable subledger/aging is reviewed.
- Accrual for goods received not invoiced is reviewed.
- Advanced bookings are reviewed and approved by executive management.
- Classification of PP&E versus expense is reviewed and approved by appropriate personnel.
- Costs by department/division/etc. are compared to budget.
- Debit memos are matched with vendor’s credit memos.
- Debit memos require approval.
- Exceptions to 3-way match (purchase order, receiving report and invoice) are investigated daily.
- Inventory count crews are supervised.
- Movement of inventories during physical counts is controlled.
- Out-of-balance reports are reviewed.
- Overrides of validation edits are reported, reviewed and authorized.
- Significant debit balances in individual vendor accounts are investigated.

What ensures that proper cut-off information is generated and used for purchases?

<table>
<thead>
<tr>
<th>IT</th>
<th>IT</th>
<th>IT</th>
<th>PP</th>
<th>PP</th>
<th>IT</th>
</tr>
</thead>
</table>

39
The Conceptual Framework

Hazards

Information Risk

Establish Context
Identify Risks
Analyze/Quantify Risks
Integrate Risks
Assess/Prioritize Risks
Treat/Exploit Risks

Monitor & Review

Operational Risk

Compliance Risk

Financial Risk

Strategic Risk
Integrate Risks

- Consolidate all identified risks
- Consolidate the likelihood and overall impact of each risk on Key Performance Indicators (KPIs)
- Align risks with business objectives
Implementing ERM

Step 5: Assess / Prioritize Risks
The Conceptual Framework

Hazards

Information Risk

Operational Risk

Compliance Risk

Financial Risk

Strategic Risk

- Establish Context
- Identify Risks
- Analyze/Quantify Risks
- Integrate Risks
- Assess/Prioritize Risks
- Treat/Exploit Risks

Monitor & Review
## Risk Prioritization

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Commercial</th>
<th>Finance</th>
<th>Security</th>
<th>Safety</th>
<th>Legal and regulatory compliance</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major</td>
<td>Significant loss of market share resulting in 10–30% loss of current clients and no increase in new clients over a three-month period. Loss of 20–30% of total income or budget.</td>
<td>Loss &gt; 30% of total income or budget.</td>
<td>Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Significant reputation damage.</td>
<td>Death of multiple injuries requiring hospitalisation.</td>
<td>Investigation by authority and significant penalty awarded. Very serious litigation, including class actions. Closure of business.</td>
<td>Extreme</td>
</tr>
<tr>
<td>Moderate</td>
<td>Loss of market share. Current clients are retained but no new clients for 1–3 months. Loss of 10–20% of total income or budget.</td>
<td>Loss of 10–20% of total income or budget.</td>
<td>Staff threat resulting in some injury but no hospitalisation required. Minor reputation damage.</td>
<td>Minor injury – first aid required.</td>
<td>Serious breach with investigation by or report to authority. Moderate penalty possible.</td>
<td>High</td>
</tr>
<tr>
<td>Minor</td>
<td>Minor loss of market share. Current clients are retained but new clients have visibly decreased (50% of normal uptake). Loss &lt; 10% of income or total budget.</td>
<td>Staff threatened, but no injury. No reputation damage.</td>
<td>No injury.</td>
<td>Low-level legal issue. Penalty or prosecution unlikely.</td>
<td></td>
<td>High</td>
</tr>
</tbody>
</table>
Risk Prioritization

**Overall Report Risk Rating**

- **High**
  - Focus on strategic risk management tools
- **Low**
  - Contingency Planning
- **MODERATE**
  - Build internal controls
- **LOW**
  - Monitor/Systematic Controls
  
**Magnitude**

- **EXTREME**
  - Containment Strategies
- **HIGH**
- **MODERATE**
- **LOW**
- **Low**

**Likelihood**

- **High**
Implementing ERM

Step 6: Treat / Exploit Risks
The Conceptual Framework

- Hazards
  - Information Risk
    - Establish Context
    - Identify Risks
    - Analyze/Quantify Risks
    - Integrate Risks
    - Assess/Prioritize Risks
  - Financial Risk
    - Treat/Exploit Risks

- Operational Risk
- Strategic Risk
- Compliance Risk
Risk Treatment Strategies

- **Risk Avoidance**
  - **Overall Risk or Inherent Risk**
  - **Reduced Risk**
  - **Further Reduced Risk**
  - **Residual or Accepted Risk**
Risk Treatment Tools

- **Risk Avoidance:** Quit the activity which results in exposure to risks e.g. avoid dealing in cash or foreign currency
- **Risk Transfer:** Insurance, Factoring
- **Risk Mitigation:** Internal control, Hedging, Credit Management, Business Continuity Planning etc.
- **Risk Acceptance:** Exploit the risk to get benefit
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cybercrime, including virus damage, identity theft, spyware, general fraud</td>
<td>Costs associated with online transactions outweigh benefits associated with initiative</td>
<td>Breach of regulations within e-business legislation</td>
</tr>
<tr>
<td>Impact</td>
<td>Direct financial loss, reputation damage, equipment damage, system unavailability</td>
<td>Direct financial loss due to increased fees Customer loss due to increased costs</td>
<td>Possible fine and/or legal prosecution</td>
</tr>
<tr>
<td>Consequence</td>
<td>Significant</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Likely</td>
<td>Likely</td>
<td>Possible</td>
</tr>
<tr>
<td>Level of risk</td>
<td>Extreme</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Risk priority</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Treatment options</td>
<td>1. Update anti-virus software and check firewall viability 2. Review requirements to ensure secure online banking 3. Develop and test security policies 4. Develop disaster recovery plan</td>
<td>Develop business case to identify impact of increased fees</td>
<td>1. Review all legislation 2. Consult solicitor to seek advice 3. Develop and test compliance policies and procedures</td>
</tr>
</tbody>
</table>
Implementing ERM

Step 7: Monitor & Review Risks
The Conceptual Framework

Information Risk

Hazards

Establish Context
Identify Risks
Analyze/Quantify Risks
Integrate Risks
Assess/Prioritize Risks
Treat/Exploit Risks

Financial Risk

Monitor & Review

Operational Risk

Strategic Risk

Compliance Risk
Risk Monitoring Tools

- Key Risk Indicators (KRIss)
- Risk Governance, Policies & Procedures
- Establishing the Risk Management Department
- Risk Register
- Risk Reporting
- Internal Audit
Develop Key Risk Indicators (KRIIs)

- Market share
- Number of direct competitors
- Loss caused by frauds during the period
- Total exposure to foreign exchange risk
- Number of significant internal control weaknesses reported
- % of price fluctuation
- Bad debts written off
- Avoidable losses during the period
ERM: Other Issues

- Why ERM?
- ERM Maturity Model
- Key Factors for Success of ERM
Why ERM????

- Reduced losses
- Enhanced business processes
- Improved reputation
- Enhanced control over the business
- Reduced penalties
- Secured information
- Effective use of technology
- Fewer surprises
- Effective decision making
- Improved corporate governance
ERM Maturity Model

Increased awareness of executive responsibility to shareholders

- A more comprehensive and rigorous understanding of the impact of risk
- More active management of risk

Source: Enterprise Risk Management: Trends and Emerging Practices, by Jerry A. Miccoli, Kevin Hively, and Brian W. Merkley
Copyright 2001 by the IIA Research Foundation. All Rights Reserved.
The Risk Intelligent Enterprise Maturity Model

How capable is your company today? How capable does it need to be? Every industry, company and division is probably at a different stage of development. Where should they be and how do they get there?

1: Tribal & Heroic
- Ad-hoc/chaotic; depends primarily on individual heroics, capabilities and verbal wisdom
- Reaction to adverse events by specialists
- Discrete roles established for small set of risks
- Typically finance, insurance, compliance

2: Specialist Silos
- Tone set at the top
- Policies, procedures, risk authorities defined and communicated
- Business function
- Primarily qualitative
- Reactive

3: Top-Down
- Integrated response to adverse events
- Performance linked metrics
- Rapid escalation
- Cultural transformation underway
- Bottom-up
- Proactive

4: Systematic
- Built into decision-making
- Conformance with enterprise risk management processes is incentivized
- Intelligent risk taking
- Sustainable
- "Risk management is everyone's job"

5: Risk Intelligent

Un-Rewarded Risk

Rewarded Risk
Key Factors for ERM Success

- **Agreed risk strategy:** The audit committee and management must provide guidance on the appropriate strategy and approach to risk management aligned to the organisational structure.

- **Clear governance framework:** The audit committee will usually delegate day-to-day governance through an oversight structure that includes a Chief Risk Officer.

- **Efficient risk management processes:** The organisation needs firm procedures for assessing and continuously monitoring risks on an enterprise wide basis.

- **Appropriate technology:** Effective systems providing access to information about risk identification, assessment and solutions to support the risk management process.

- **Co-ordination of risk management functions:** Integrated risk functions embedded within the business to leverage expertise across the entire organisation.

- **The right culture and capability:** Everyone in organization must be attuned to the risk culture and performance measurements must be risk based.
Thank you