Enterprise Risk Management (ERM)

An understanding of key concepts for a sustainable implementation

April 2020
ENTERPRISE RISK MANAGEMENT (ERM)
WHAT IS ERM?

ERM

COSO 2017
ISO 31000: (ERM)
ISO 9000: (QM)
ISO 14000: (EM)
ISO 45000: (OH&S)

Is a process

Organization is geared towards achieving stated objectives

Provides reasonable assurance to Management, BOARD Stakeholders

Effectuated by the people at all Levels

Applied across the Enterprise

Designed to identify potential events

In strategy setting

And in managing risks within the risk appetite

EPR

WHAT IS ERM?
REGULATORY EMPHASIS ON ERM

1. **Companies Act 2013 and SEBI’s Clause 49**
   The Board and audit committees have been given specific responsibilities in assessing the robustness of risk management framework implemented in the company.

2. **Section 134**
   The Board’s Directors report should include a statement on development and implementation of risk management framework for the company, including identification of risk which, as per the Board’s opinion, could threaten the very existence of the company.

3. **Section 177**
   The audit committee shall act in accordance with the terms of reference specified in writing by the Board, inter alia evaluation of risk management system.

4. **Schedule IV**
   Independent directors are required to get assurance the systems of risk management are robust and defensible.
ERM BEYOND REGULATORY: FOCUS ON CULTURE, CAPABILITY & PROCESS BUILDING

Management, Board and the Stakeholders want more value from ERM

Today, Organization’s risk exposures are changing and evolving more rapidly than ever before.

Several factors are contributing to this trend, such as globalization, growing speed of transactions, growing information sharing and big data, greater instability and volatility of markets, higher expectations from investors and more complex regulations.

Many traditional ERM initiatives are no longer able to meet the strategic needs of the business as they are:

- Risk listing activities carried out for compliance/assurance purposes
- Standalone processes with no or limited integration with decision making
- Often qualitative exercises, with limited or no quantification
- Focused on day-to-day activities instead of strategic objectives
- With limited or no impact on key decision-making

Towards a Risk-Informed Perspective
ORGANIZATIONS FOCUS OF ERM CONVERSATION

- Focused on what really matters
- Provide information that can drive strategic decisions
- Executive led

- Strategic planning
- Budgeting and forecasting
- Evaluation of Strategic / Investment Options
- Strategy and Business execution

- Risks / Opportunities
- Qualitative / Quantitative
- Bottom-up / Top-driven

- Consider client’s business characteristics and its cultural and organizational attributes
- Respond to specific stakeholders’ expectations
- Align with market/industry requirements
ESSENTIAL BUILDING BLOCKS OF ERM

- Vision
- Communication and support
  - Sponsorship & Positioning
  - Risk Management Support
  - Expertise and Resources
- Loss Reporting
  - Strategic & Cultural Alignment
  - Accountability
  - Dashboard/KRI's
  - Risk Champions, Performance management link
  - Budgeting, Forecasting, Audit
- Training – awareness and embedding
  - Management Information
  - Confidence to Act
  - Risk Appetite and Tolerance defined and used to aide decision making
  - Common risk language
- Strategic planning
  - Embedding in Business Processes
  - Documentation (Policy, Registers, Guidelines)

© 2020 Protiviti India Member Private Limited
CONFIDENTIAL - This document is created for ICAI training purposes and should not be copied or distributed to any third party.
ERM FRAMEWORKS: COSO 2017

- Establishes the entity’s risk culture
- Sets the Enterprise Risk Objectives
- Identifies events that affect entity’s objectives
- Assesses risks based on likelihood and impact
- Evaluates possible responses to risks
- Establishes policies, procedures and controls
- Enables information exchange
- Evaluates effectiveness of the ERM Program
ERM FRAMEWORKS: COSO 2017

Risk management

- Creates and protects value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on the best information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement of the organisation
PROTIVITI ERM FRAMEWORK

EXTERNAL FACTORS

ERM ENABLERS

ERM PROCESS STEPS
INTEGRATED INTO PERFORMANCE MANAGEMENT

ERM PILLARS

INTERNAL FACTORS

INDUSTRY / BUSINESS CONTEXT

METHODOLOGIES, DATA & TOOLS

IDENTIFY
QUANTIFY
DECIDE
MONITOR

IDENTIFY RISKS AND OPPORTUNITIES
ASSESS & QUANTIFY IMPACTS
MAKE RISK-INFORMED DECISIONS
MONITOR AND REPORT

EXPECTATIONS, NEEDS AND CONSTRAINTS

STRATEGY AND BUSINESS EXECUTION
BUSINESS PLANNING & FORECASTING
EVALUATION OF STRATEGIC OPTIONS
RISK GOVERNANCE
RISK APPETITE
RISK CULTURE
Protiviti’s methodology is a judicious blend of recommended standards and field tested practical activities, aimed at building an effective proactive framework encompassing a universe of applicable business risks.
CAPABILITY MATURITY ASSESSMENT: STARTING POINT FOR ERM

Areas of Focus

- Strategy and Business Execution
- Evaluation of Strategic Options
- Business Planning and Forecasting
- Risk Culture and Behaviors

Establish and evolve the overall ERM governance

- Disseminate a risk-based mindset across the organization
- Implement a robust Risk Appetite Framework

Value Added to “Risk-Informed” Decision-Making

- Identify and prioritize enterprise risks
- Quantify, proactively manage and monitor top risks
- Do we know our risks? Do we manage and monitor what really matters?
- Integrate risk and opportunity analysis into strategy setting and planning
- Do we make risk-informed decisions?
- Do we make decisions in line with our risk appetite?
- Do we act as desired at all levels?
ERM FRAMEWORK CONSTITUENTS

1. **Risk appetite and tolerance (RACM)**
   Define risk appetite/tolerance at an Enterprise and SBU level for guidance, evaluation and acceptance or risks

2. **Risk Governance structure**
   Define key constituents of the governance structure (sponsors; decision makers; custodians and enablers)

3. **Risk Identification**
   - Risk identification techniques
   - Risk capture into risk register

4. **Risk analysis method**
   - Qualitative analysis - Impact/Likelihood matrix
   - Quantitative analysis – Monte Carlo simulation

5. **Risk Treatment**
   - Risk treatment strategy and process of risk mitigation

6. **Risk monitoring and reporting**
   - Risk monitoring mechanism
   - Risk reporting mechanism
RISK APPETITE AND TOLERANCE

Risk Assessment Criteria Matrix (RACM) is a reflection of Company’s risk appetite and tolerance, in the current context of business and economic environment.

1. Entity level RACM

Entity level risk assessment criteria matrix may be based on key parameters like:
- Strategic
- Operational
- Financial
- Legal, contractual, Compliance,
- Reputational.

![Risk Assessment Criteria Matrix (RACM) Image]
<table>
<thead>
<tr>
<th></th>
<th>RISK IDENTIFICATION TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Questionnaires and risk surveys</td>
</tr>
<tr>
<td>2</td>
<td>Interviews and discussions</td>
</tr>
<tr>
<td>3</td>
<td>Financial statement analysis</td>
</tr>
<tr>
<td>4</td>
<td>Process flowcharts analysis</td>
</tr>
<tr>
<td>5</td>
<td>Analysis of business process drivers</td>
</tr>
<tr>
<td>6</td>
<td>Periodic MIS reports for the division (corporate, regions and projects) and review meetings</td>
</tr>
<tr>
<td>7</td>
<td>On a review of Internal and external audit reports</td>
</tr>
<tr>
<td>8</td>
<td>Update on several on-going matters and personal inspection</td>
</tr>
<tr>
<td>9</td>
<td>Loss histories / hazardous events</td>
</tr>
</tbody>
</table>
FORMATION OF RISK STATEMENT

Risk statement provides three-part structured “Risk Statement” : “As a result of <definite cause>, <uncertain event> may occur, which would lead to <effect on objective(s)>.”

Example:

- Incorrect item rate analysis (Fact=cause) at the tendering stage due to unrealistic assumptions (Uncertainty=risk) may lead to incorrect cost (Contingent possibility=effect) estimations for the project

- Overwhelming project compulsions (i.e. completion of project in stipulated time, cost and margins etc.) and pressures from the project manager (Fact=cause) may curb the assertiveness and independence of the quality manager at site (Uncertainty=risk) leading to compromise in quality enforcement (Contingent possibility=effect).
RISK ANALYSIS

Risk Analysis involves clearly understanding of the risk sources, the potential impact/consequences and any treatments/controls that are currently in-place.

Qualitative risk analysis – Impact / Likelihood rating matrix

Impact matrix
Impact matrix lists the standard definition of impact matrix based on various parameters like delay, shortfall of revenue etc. The rating of the impact is a scale from “1 to 5”

- Negligible
- Minor
- Moderate
- Significant
- Severe

Likelihood matrix
Likelihood matrix represent the probability of the impact to occur on the business activities in case the risk occurred. The rating of the probability is a scale from “1 to 5”:

- Very unlikely
- Unlikely
- Possible
- Likely
- Very Likely

ENTERING THE RISKS INTO RISK REGISTER
A culture of open dialogue and empowerment, at all levels, greatly benefits the risk management process. Organization wins.

Risk Champion identifies and assesses a risk

Referrers the Risk for a Discussion with Risk Owner

Mediation or risk assessment with concerned Leadership

Risk Mitigation Action

Risk Mitigation Action taken

Risk validation with Source

Back to Winning days
RISK TREATMENTS

Risk treatment involves selecting one or more options for modifying risks, and implementing those options.

- **Risk Strategies**
  - Retain
  - Reduce
  - Transfer
  - Avoid

- **Risk Treatment Process**
  - Root cause analysis
  - Development of treatment plans

- **Effectiveness Tracking**
  - Review of treatment by (Risk Officers)
  - Effectiveness tracking by pre define template

*Suggested treatment plans implementation tracker*
RISK TREATMENTS: PREREQUISITES

1. Every root cause should at least have one treatment plan.

2. Treatment plans need to be modular in nature with clear-cut action steps.

3. Treatment plans can be described at a concept level for lower risk ratings. However, with higher rating, they need to be articulated with detailed action plans, sub-tasks with dates for implementation.

4. Pre-articulated treatment plans must be validated to withstand the ‘test of time and current set of challenges’ and either be fine-tuned or revamped to achieve the desired mitigation.

5. Every treatment plan should have a clear ownership and single-point accountability.
RISK MONITORING & REPORTING

Risk reporting involves key stakeholders to timely report the updated risk registers and related information based on the frequency defined for different levels.

- **Sponsors** (Quarterly)
  - BOARD
  - C – Suite Leadership
  - Risk Committees formed at various levels

- **Decision makers** (Frequency: 1st week of each month / quarter)
  - Management at various levels
  - Risk Champion (RC)

- **Custodians** (Frequency: Escalation – 27th of each month
  - Final submission – 29th of each month)

- **Enablers** (Frequency: 25th of each month)
KEY CHALLENGES IN ERM IMPLEMENTATION

- Failure to obtain “buy-in” and support from Executive Management / Allowing ERM to become a compliance program.

- Development of a centre of excellence for managing risk, drawing on the expertise of highly skilled individual risk managers.

- Risk management not embed in day to day operations. Roles & responsibilities of participants not clearly defined.

- Insufficient emphasis on defining information and reporting needs / Failure to integrate ERM into key management processes and performance management (i.e., metrics, scorecards, dashboards).

- Lack of planning and foresight in roll out a training, communication and sustenance programme for ERM.

- Incentivizing ERM program for its success and sustenance.