COSO Enterprise Risk Management – Aligning risk and strategy

March 2019
About Risk Management
Evolution of Risk management

Traditional Risk Management - It is associated with the use of market insurance to protect individuals and companies from various losses associated with accidents.

1947: Establishment of International Organization for standardization (ISO)

1973: Non Life insurance directives is considered as a format point for solvency requirements

1974: Establishment of Basel Committee in response to the serious disturbances in International currency and banking market

1980: Companies begin Risk departments: It was during this time when companies began to consider financial management or risk portfolio & emergence of Basel I – The Basel Capital Accord


2017: ERM – Integrating with Strategy and Performance

2010: Introduction of Basel III norms

2013: COSO Internal control – Integrated framework

PwC has been the knowledge partner with Committee of Sponsored Organizations (“COSO”) in all its initiatives, including the latest ERM 2017 framework.
While many report on risk using metrics, fewer of these are linked to the strategic priorities of the business

PwC COSO ERM Survey 2018

Question: How well do you believe management performs the following activities:

- Provide effective summary-level metrics and reporting to the board
- Links risk to strategic objectives
- Leads effective ERM efforts

<table>
<thead>
<tr>
<th>Activity</th>
<th>Very</th>
<th>Somewhat</th>
<th>Not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide effective summary-level metrics and reporting to the board</td>
<td>67%</td>
<td>33%</td>
<td>0%</td>
</tr>
<tr>
<td>Links risk to strategic objectives</td>
<td>50%</td>
<td>0%</td>
<td>50%</td>
</tr>
<tr>
<td>Leads effective ERM efforts</td>
<td>69%</td>
<td>31%</td>
<td>0%</td>
</tr>
</tbody>
</table>
58% of Boards do not receive updates at every meeting on the amount of risk the company is taking

PwC COSO ERM Survey 2018

Question: How often does your board get updates and reports from management on:

- The company’s key risks
- The amount of risk the company is taking
- Changes to the company’s approach to enterprise risk management

- At every meeting
- Twice annually
- Annually
- Never
So what are risk and business professionals saying?

**PwC COSO Survey 2018**

- I want an ERM Framework that drives improvements to business functions beyond risk avoidance.
- As an innovative company, I want to use risk to create value and not only to protect value.
- I want to reduce performance variability and respond more quickly to opportunities.
- I need insights that help me understand risks and opportunities and evaluate strategic options.
- When I develop my strategy, I want to have a full picture of the potential risks and the capabilities I need to create advantage.
ORM v/s ERM

Enterprise Risk Management
- Scope of much wider and includes all types of risk like default risk, credit risk, marker risk, reputational risk, strategic risk, liquidity risk and also includes operational and legal risk.
- Generally measured in terms of appetite statement, tolerance and threshold limits.
- Flows as “tone at the top”.
- Tackle the loss/risks which affects the organization in drastic and adverse way.

Operational Risk Management
- Subset of Enterprise Risk. Includes operational and legal risk only.
- Generally measured in terms of operational loss, foregone income, control and self assessment.
- Embedded at the more micro level of individual processes.
- Tackle the loss/risks which generally has monetary impact.

One of the key challenges faced in an ERM implementation, is the tendency to confuse it with an Operational Risk Management (“ORM”) exercise. ORM is a subset of ERM and in some organizations may have a very large attribution, but the objective of an ERM exercise is to have a broader view of the risks in an organization. PwC given its association with COSO over 2 decades, understands the importance of the same.
ERM definitions

COSO Definition
The culture, capabilities and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving and realizing value:

• It focuses on managing risk through-
• Recognizing culture
• Developing capabilities
• Applying practices
• Integrating with strategy setting and performance
• Managing risk to strategy and business objectives
• Linking to value

Institute of Internal Auditors (IIA)
Enterprise-wide risk management (ERM): A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives

ISO-31000
Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

According to the Introduction to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk. This architecture includes risk management principles, a risk management framework, and a risk management process.
**Importance of ERM?**

- **Boards are expecting more** from their organization’s ERM practices and capabilities
- Stakeholders are seeking **greater transparency** and accountability
- Business **environments are increasingly complex**, technologically driven, and global
- There is a need to **incorporate lessons learned** from recent events and the bar is rising
- Risk professionals are looking for a **more up to date resource** describing ERM concepts
- The range of ERM **practices continues to evolve**
**ERM definitions**

**COSO Definition**
The culture, capabilities and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving and realizing value:
- It focuses on managing risk through-
- Recognizing culture
- Developing capabilities
- Applying practices
- Integrating with strategy setting and performance
- Managing risk to strategy and business objectives
- Linking to value

**Institute of Internal Auditors (IIA)**
Enterprise-wide risk management (ERM):
A structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on

responses to and reporting on opportunities and threats that affect the achievement of its objectives

**ISO-31000**
Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

According to the Introduction to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk. This architecture includes risk management principles, a risk management framework, and a risk management process.
The graphic symbolizes the dynamic, integrated nature of ERM that begins with the mission, vision and core values of the organization through to the creation of enhanced value.
### 10 Considerations in Getting Started

<table>
<thead>
<tr>
<th>Adopt a Principles-Driven View of ERM</th>
<th>Explore Governance Oversight and Management of Risk at All Altitudes</th>
<th>Have Deeper Discussions on Risk Appetite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link risk management into strategy</td>
<td>Communicate from the Perspective of the Business</td>
<td>Explore the Evolving Role of Technology in Managing Risk</td>
</tr>
<tr>
<td>Explore the Different Benefits of ERM</td>
<td>Emphasize on Culture</td>
<td>Shift Assessments from Risk Centric to Performance Oriented</td>
</tr>
<tr>
<td>Link risk with strategy setting, using ERM principles to support the creation, realization, and preservation of value</td>
<td>Reflect on the changing demands and expectations of today’s markets, helping your organization make responsible risk decisions</td>
<td>Explore ways to evolve beyond lists and heat maps to provide insights into risk’s impact on performance</td>
</tr>
<tr>
<td>Link risk with strategy setting, using ERM principles to support the creation, realization, and preservation of value</td>
<td>Discuss risk management concepts in terms of helping your organization create value, enabling you to realize benefits from ERM</td>
<td>Have meaningful conversations on risk appetite and how</td>
</tr>
<tr>
<td>Explore the spectrum from loss mitigation through to strategic advisor and how they inform the practices within the organization</td>
<td>From entity level through to procedural level risks, make ERM more than just an isolated view of risk in the business and something that resonates with the board</td>
<td>Explore the evolving role of technology’s influence on managing risk</td>
</tr>
</tbody>
</table>

---

COSO Enterprise Risk Management

PwC

March 2019
Adopt a principles-driven view of ERM

Considerations in getting started

• Delve into the 20 COSO principles and what they say – not what you think they might say
• Consider how these principles are applied today, and how they might shape the future evolution of your practices and capabilities
• Assess the maturity of your current practices and the value that these practices provide across the organization
Explore the different benefits of ERM

ERM is not a “one-size-fits-all” program – activities must be tailored to align with the benefits

- Reducing negative outcomes
- Enhancing enterprise resilience
- Improving resource deployment
- Reducing performance variability
- Identify and manage risks entity-wide
- Increasing the range of opportunities

Considerations in getting started

- Explore with the board and management which of these benefits should have higher focus
- Evaluate current practices in place to determine the actual benefits you should expect of your ERM efforts

COSO Enterprise Risk Management

PwC

March 2019
Building Effective Risk Culture

- Board oversight of risk culture expectations
- Risk culture gap assessment
- Consider a Board & C-Suite Driven/Objective-Centric approach to ERM and Internal Audit
- Hold the CEO accountable for building and maintaining effective risk appetite frameworks and providing the board with periodic consolidated reports on the company’s residual risk status
- A sound risk culture promotes an environment of open communication and challenge in which decision-making processes encourage a range of views

Risk framework-Taking the Right Risk

- Effective and Timely Feedback Mechanism
- Transparent Governance Mechanism
- Reward and Incentives, risk based remunerations
- Trainings, Common Understandings and Knowledge
- Sound and Effective Board/Leadership
- Competitive and transparent fee structure

- An experienced, multi-disciplinary team
- Clear Organisation Structure, Roles and Responsibilities
- Technology–based solutions
- Comfort to Talk and Challenge Others

Organisation

COSO Enterprise Risk Management

PwC

March 2019
Scope and Approach
ERM Implementation
Governance Around Risk Management and Board’s Role

Globally Three LOD mechanism is an accepted structure for effective risk management. Given the context we can assist AEON in reviewing the effectiveness around Three LOD mechanism implemented within the organisation.

A risk management ecosystem led from the front line, that fosters collaboration and shared accountability across all three lines of defence, positions a company to effectively meet the challenges of today’s risk landscape. To get there, a company should:

- Setting a strong organisational tone focused on risk culture that starts with the board and CEO and permeates the entire organisation.
- Align risk management with strategy at the point of decision making so the first line anticipates business risks when setting tactical priorities.
- Recalibrate the risk management programme across the three lines of defence.
- Implement a clearly defined risk appetite framework across the organisation.
- Develop risk reporting that enables executive management and the board to effectively execute their risk oversight responsibilities.

Rather than representing a threat to the risk management, compliance, and audit functions, the shift of certain risk management activities to the first line represents an opportunity. By aligning all lines of defence within a collaborative, strategic framework, business-led risk management enables the second and third lines to become true partners in creating value for the enterprise.

Increasing Board’s Role

- Bringing Risk Expertise through risk committee or risk experts in the organisation.
- Oversight on Roles and Responsibilities and risk appetite framework.
- Conversation between, risk committee, audit committee and senior management.
- Effective Risk Culture - Strategies are linked to objectives. Promoting culture of common risk language.
- Challenging and Questioning. Supporting with adequate budgets for Risk Management Activities.
- Top Down Approach on Stress Testing.
- Improved risk information, reporting, data and analysis. Focus on cyber and emerging risk management.
- Effectiveness around compliance and internal control mechanism.
Implementing ERM with New COSO ERM 2017 Framework

The PwC’s GAP analysis on the existing enterprise risk management would be the starting point for assessing completeness and maturity of what the Organisation has previously built as a risk management. A strong framework for managing enterprise wide risk needs to cover all aspects of organisation. PwC Uses COSO 2017 ERM as an effective model to understand the existing enterprise risk management structure and its effectiveness. Revised COSO framework includes 5 components and 20 principles.

The graphic symbolizes the dynamic, integrated nature of ERM that begins with the mission, vision and core values of the organization through to the creation of enhanced value.

COSO Enterprise Risk Management
PwC
There is clear recognition of the need for risk functions to evolve with the changing risk and business environment. There is increased focus around 1) allocation of adequate resources to new and emerging risks 2) Leveraging the effective technology 3) Availability of risk analysis and information to support key business decision making 4) Linking strategies with objectives 5) Changing risk conversation and building effective risk culture. These all requires significant change in operating model of risk management and to positively handle future scenarios. We can assist our clients in reviewing the existing ERM framework and implementation of COSO 2017 with below phase wise approach

**PwC’s Phase wise approach**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. GAP Assessment</td>
<td>Conducting review of Existing ERM/Risk Management framework which includes existing ERM policy, governance framework and related. Mapping it against COSO 2017 ERM framework and conduct a Gap assessment and provide recommendations based on expectations to Management for decision making.</td>
</tr>
<tr>
<td>B. Revised Governance Framework</td>
<td>Assistance in redevelopment of governance framework which includes re designing board and committees charter, roles and responsibilities, implementation model for risk ERM, enhancement of policy and procedures, re-designing of org. structure, development of KPI’s. Assessment of delegation of authorities and recommendation to Management basis industry practice. Development approach around risk identification.</td>
</tr>
<tr>
<td>C. KRI, Appetite and Risk Register</td>
<td>Redvelopment of function wise risk register. Development /redevelopment of KRI’s. Suggest update regarding the risk appetite framework. i.e. Assist in defining risk appetite statements and defining risk tolerance limits for risk appetite statements. The risk appetite statements will be developed at the company level as well as individual department and or risk level. The appetite statements will be developed considering the AEON's business model, size and scale of operations.</td>
</tr>
<tr>
<td>D. Risk Assessment and Monitoring</td>
<td>Review of Risk assessment and prioritization framework to assess the impact and likelihood of the identified risks. Assistance in developing risk mitigation plans for the risks that are above tolerance level. Review the MI dashboards governing the trends of risks, prepared for monthly/quarterly management presentation and suggest enhancements as appropriate. Assistance in development of various risk strategies i.e. termination, transfer, treatment etc.</td>
</tr>
</tbody>
</table>
Detailed Approach (1/4)

**Phase A: Gap Assessment**

<table>
<thead>
<tr>
<th>Day-1 to 5</th>
<th>Day-9</th>
<th>Day-13 to 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct discussions with the management to understand the existing risk management framework. Conduct initial walkthrough with the key stakeholders to get a high level understanding. Obtain the existing policies and procedures.</td>
<td>Understand the regulatory environment and framework applicable to the company and existing compliance framework. Review the delegation of authority and segregation of duties among different departments and personnel.</td>
<td>Review the existing tools, risk registers, techniques and system used for risk measurement and control. Review the Internal Control System and mechanism regarding Reporting (MIS). Also review the reporting to external stakeholders.</td>
</tr>
</tbody>
</table>

**Key Activities**

<table>
<thead>
<tr>
<th>Day -6 to 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct meetings and process walkthroughs with all the relevant process owners to understand the as-is situation. Understand the organization structure. Obtain an in depth understanding of the 'as is' framework.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Day- 10 to 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform document review of existing policies and understand key controls in place. Understand the existing process around risk identification, measurement and control. Understand the flow of information between Risk Team and Other departments and functions and related entities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Day-16 to 18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carry out review and assessment of existing process documents through discussions with stakeholders. Carry out a current state assessment of the documents against the CPSO ERM 2017. Discussion of draft report with process owners and finalization of GAP assessment report.</td>
</tr>
</tbody>
</table>

**Value addition**

End to end assessment of existing risk management framework within the organisation. A key take away for senior management/chief risk officers, which assists them in decisions making for changes or amendments in the existing risk management framework along with the accountability for implementation.

**Deliverables**

Executive Summary and Gap Reports

**Detailed observations**

[Table content]

**Week 1 to Week 4**
**Detailed Approach (2/4)**

### Key Activities

<table>
<thead>
<tr>
<th>Day-1</th>
<th>Day 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review of existing governance framework and understanding the group level policy, procedures and guidelines. Review of objective and vision statement of the Organisation.</td>
<td>Assistance in re-designing the framework, organisation structure and Re-document the TOR, charter, roles and responsibilities basis the gap identified.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Day 2 to 3</th>
<th>Day 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct meetings/discussion to understand various committees, board structure and organisation structure. Review of delegation of authority and segregation of duties, review of KPI and KRI statements. Review of annual performance system. Review of operating structure and</td>
<td>Assistance in redefining of the revised governance framework</td>
</tr>
</tbody>
</table>

### Phase B: Revised Governance Framework

**Value addition**

Consistent definition of the ERM program, expectations, KPIs, roles and responsibilities. Reinforces accountability for integrating risk management into decision-making.

**Deliverables**

**Revised Framework**

**Week 5**
Phase C: KRI, Appetite and Risk Register

Day 1 to 14

There will be 2 sets of document i.e. department/function wise risk register and risk register for at entity level. This also includes the development of the appetite statement at department/function level and at organisation level. Based on the gap identified in phase A and number of departments involved below activities will be performed.

- Understand the department structure, roles and responsibilities
- Conduct meetings with CRO/Risk-coordinator to understand the goals of the organization and board approved organization objectives
- Understand whether organization objectives are aligned to the goals of the organisation
- Conduct discussion for understanding the activities/process/strategies implemented or planned to be implemented for achieving the objectives

Key Activities

Central Level

- Obtain existing policies, SOP and Manuals and perform document review
- Conduct discussion with the department officials to understand the brief about the activities conducted by the department
- Discuss on the critical activities undertaken by the officials, risks and implications involved in the activities and potential effect on the organization
- Understand the regulatory risk and various category of risk arising from the various process/activities undertaken by the department
- Documentation of risk description and mapping the controls against each risk description basis the discussion held and documents review. Defining key risk indicators; mapping the risk category against risk description in risk register
- Conduct meetings with the HODs and risk coordinator for defining threshold limits/appetite limits, risk champions, documenting mitigation plans if any and finalizing other elements of risk register
- Prepare and document the risk appetite statement for each stated objectives

Week 6 to Week 7

Revised Risk Registers

Deliverables

Revised risk registers at department level and at entity level along with value/amount based threshold. Consistent formats of risk registers and facilitating fresh view of broader risk inventory. Defining of roles and responsibilities at department level and for risk team. Creates deeper insights into individual risk exposures and related management capabilities.
Given the context, we can assist organisations in identifying the gap in existing risk assessment frameworks, methodology to use, risk identification process, and monitoring process which helps organisations in making decisions and achieving strategy and business objectives.

Conduct discussion with the ERM team, department officials, Risk champions if any, for understanding the current process of risk assessment, monitoring, and reporting to the ERM team.

Understand the various risk strategies utilized by the organisation. Understand the frequency of risk assessment and monitoring.

Review of methods and approach for emerging risk and cyber risk. Review of process for assessing the severity of the risk.

Review of process for prioritizing risk and assessing severity of risk. Analyze the process of monitoring the implementation of mitigation plan.

Review of process adopted for developing portfolio view of risk.

Analyze the process of monitoring the implementation of mitigation plan. Suggestion of enhanced MIS and dashboards.

Linking Risk Assessment Processes, Inputs, Approaches and Outputs
Our View - Risk Management Framework

Risk Strategy

Core capabilities of Risk Management
- Understanding emerging risk
- Risk agility (events, crises and 2nd order impact)
- Connecting the dots
- Risk as a Business Partner
- Efficient risk management

A vision for risk management

Governance and policy framework

Front office
- Enterprise-wide risk insight and control

Enablers
- Efficient risk processes
- Risk technology
- Organisational design and alignment
- Regulation as an opportunity
- Risk analytics
- The risk professional of the future
- Risk culture and behaviours

Risk origination
Risk management

COSO Enterprise Risk Management
PwC

March 2019
Thank you