

***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.

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

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**

2002: Sarbanes Oxley Act of 2002
2009: Introduction of ISO 31000-Risk Management

2010: Introduction of Basel III norms
2013: COSO Internal control – Integrated framework

1950 -1960

1973:

1974:

1980

1990 -2000-

2000 -2010:

2010 – Now

1947: Establishment of International Organization for standardization (ISO)

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

1992: COSO published internal control – Integrated framework

2004: Release of COSO ERM integrated framework & Basel II – The new capital framework

2017: ERM – Integrating with Strategy and Performance

PwC has been the knowledge partner with Committee of Sponsored Organizations (“COSO”) in all its initiatives, including the latest ERM 2017 framework.

Changing Expectation of the Board

While many report on risk using metrics, fewer of these are linked to the strategic priorities of the business

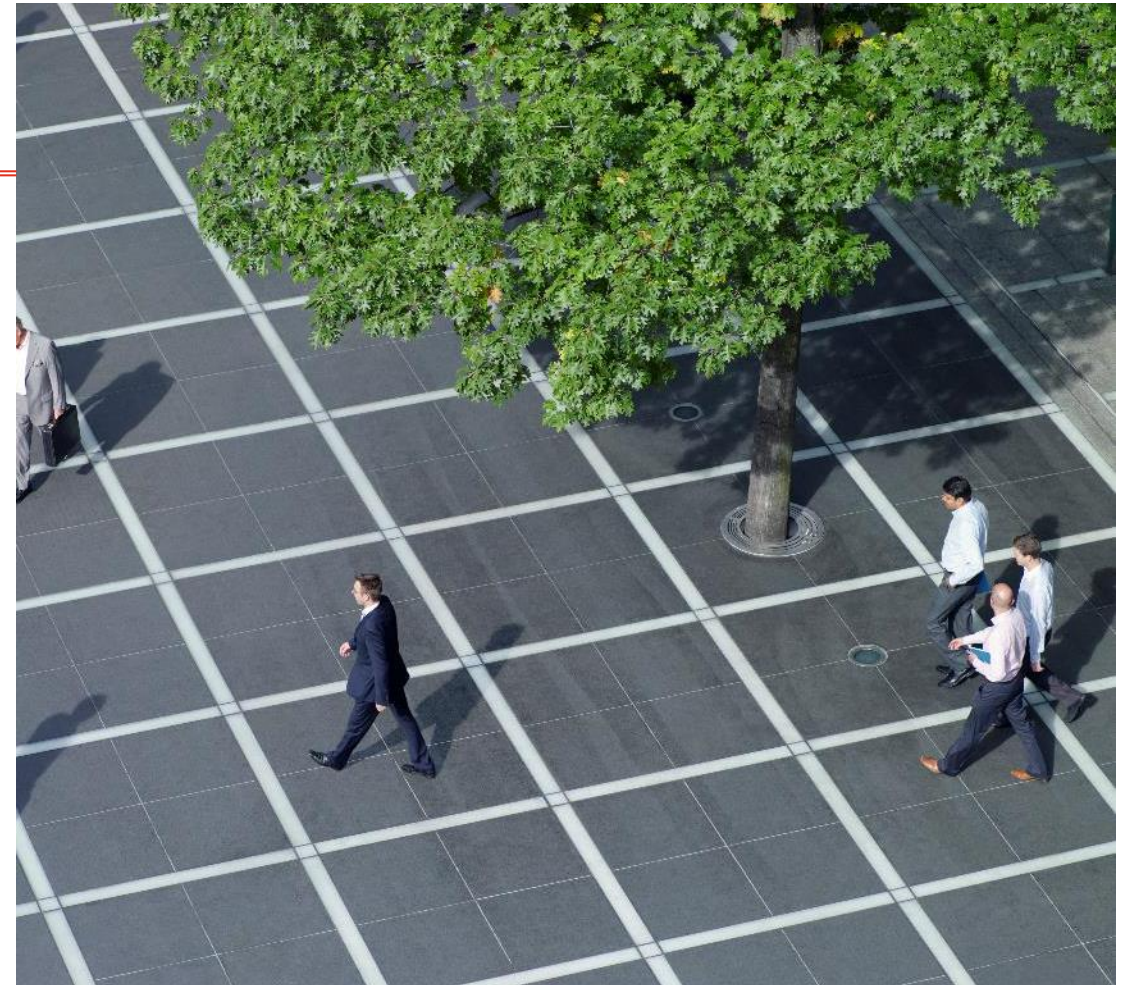
PwC COSO ERM Survey 2018



Board oversight and Management Information


58% of Boards do not receive updates at every meeting on the amount of risk the company is taking

PwC COSO ERM Survey 2018



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

I want to reduce performance variability and respond more quickly to opportunities

When I develop my strategy, I want to have a full picture of the potential risks and the capabilities I need to create advantage

As an innovative company, I want to use risk to create value and not only to protect value

I need insights that help me understand risks and opportunities and evaluate strategic options

ORM v/s ERM

- 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.

Enterprise Risk Management

- Scope of much wider and includes all types of risk like default risk, credit risk, market 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.





COSO ERM 2017 - Snapshot

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.



COSO 2017 ERM Framework- A Progressive Approach



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



Adopt a principles-driven view of ERM –applying principles that align to the business lifecycle, making risk conversations more intuitive for your organization



Explore the different benefits of ERM–consider the spectrum from loss mitigation through to strategic advisor and how they inform the practices within the organization



Link risk management into strategy– link risk with strategy setting, using ERM principles to support the creation, realization, and preservation of value



Explore governance oversight and management of risk at all altitudes–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



Communicate from the perspective of the business– discuss risk management concepts in terms of helping your organization create value, enabling you to realize benefits from ERM



Emphasize on culture– reflect on the changing demands and expectations of today's markets, helping your organization make responsible risk decisions



Have deeper discussions on risk appetite–have meaningful conversations on risk appetite and how



Address the evolving role of technology in managing risk– explore the evolving role of technology's influence on managing risk



Shift assessments from risk centric to performance oriented–explore ways to evolve beyond lists and heat maps to provide insights into risk's impact on performance



Consider your reporting–explore how current risk reporting is providing insight to the users

Adopt a principles-driven view of ERM



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance



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



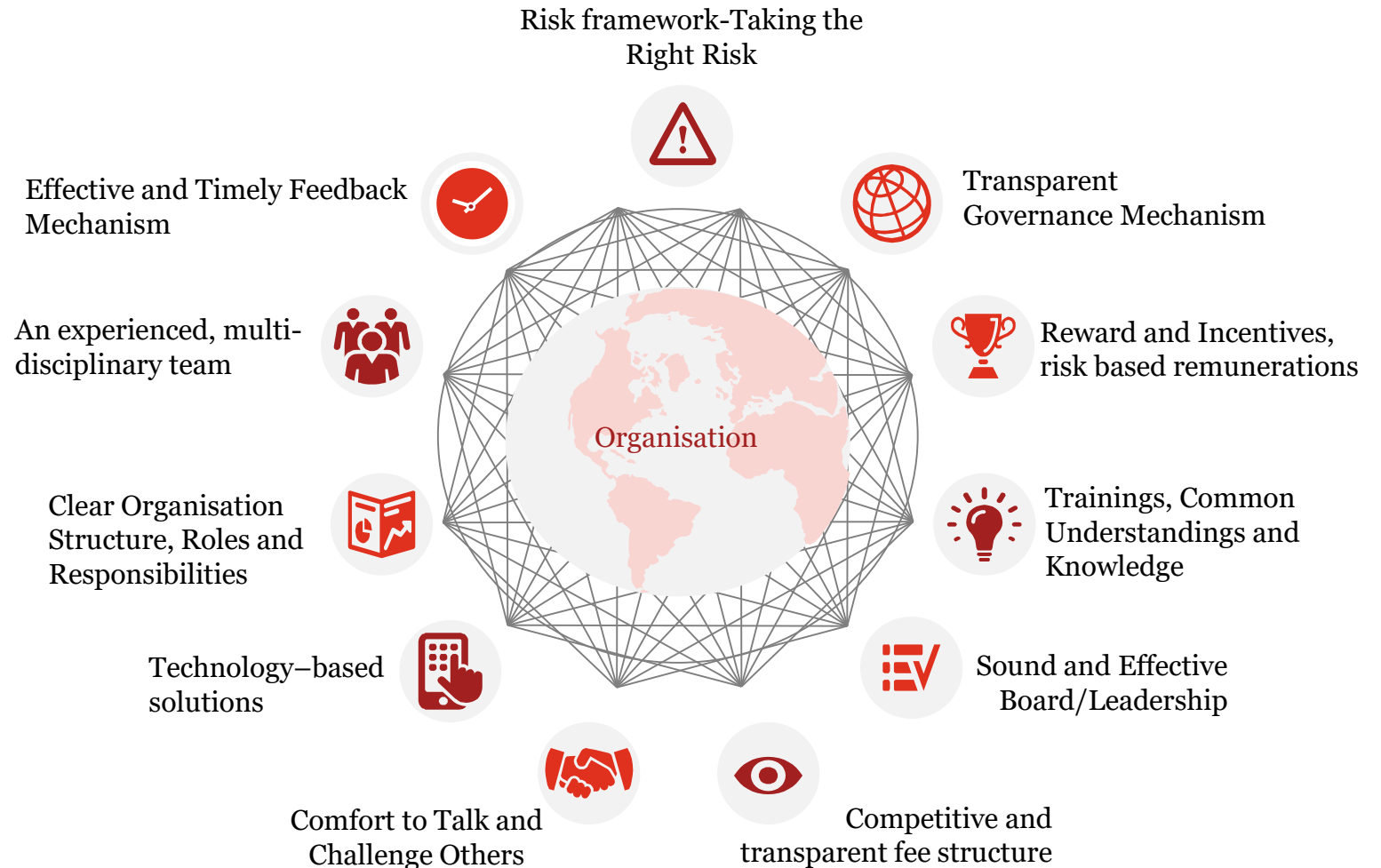
Considerations in getting started

- 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

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





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:

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.

Set 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 with the first line owning business risk decision making, the second line monitoring the first, and the third line providing objective oversight

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



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 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 component 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.



PwC's Phase wise approach

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

A. GAP Assessment	B. Revised Governance Framework	C. KRI, Appetite and Risk Register	D. Risk Assessment and Monitoring
<p><i>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</i></p>	<p><i>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</i></p>	<p><i>Redevelopment 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</i></p>	<p><i>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.</i></p>



Detailed Approach (1/4)

A.



Phase A: Gap Assessment

Key Activities

Day-1 to 5	Day-9	Day-13 to 15
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	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	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
Day -6 to 8	Day- 10 to 12	Day-16 to 18
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	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	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

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			Action: Timely
<p>4. Exercise board's risk oversight</p> <p>The board of directors have the primary responsibility for risk oversight in the entity, which includes conducting the review of enterprise risk management, leaving the day-day responsibility of managing the risk to management. While board may retain the ownership they can delegate the responsibilities to the committee for ensuring effective enterprise risk management. The board should also consist a member who has skill, experience, business knowledge and efficiency to carry the risk management function. The risk oversight is possible only when the board understands the entity strategy and industry, stays informed on relevant issues.</p>			
#	Existing practice / GAP	Recommendation	Rating
4.4	<p>On analysis of the existing policies, documents defining the roles & responsibilities, department structures, organisation structure and basis interview with key stakeholders, we noted that:</p> <ul style="list-style-type: none"> While the current governance mechanism is monitored through the AXA Group Standards Handbook (GSH), the company does not have a documented governance pyramid / governance framework suitable to domestic operations of the company which can establish the linkage of strategy and business objectives with the vision and mission, further mechanism for regular monitoring and assessing the achievement of strategic goals are not put in place in governance framework. GSH defines the legal, management and functional structure which at present is considered as working governance framework of the company. Elements like assessing the fitness, proprietary / performance of the board, policy and procedural framework of the organisation, assessing the effect of group structure, crisis management and business continuity, implementation model for corporate governance etc., are not considered in this framework. In present composition of the Board, we noticed that though independent directors possess the required skill and expertise in their respective areas, an independent director(s) as an expert from the Insurance field is not included. 	<ul style="list-style-type: none"> Develop a governance pyramid to suit the domestic operations of the company. The governance structure should establish a link between the strategy, business objectives and the vision and mission of the company. The governance framework of the company to be enhanced by considering the elements like fitness, proprietary / performance of the board, policy and procedural framework of the organisation, assessing the effect of group structure, crisis management and business continuity, implementation model for corporate governance etc., Necessary steps to be taken to impart the necessary skills to the existing independent directors or to induce a new independent director with the required expertise into the board. 	Needs Improvement

Week 1 to Week 4



Detailed Approach (2/4)

B.



Phase B: Revised Governance Framework

Key Activities

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

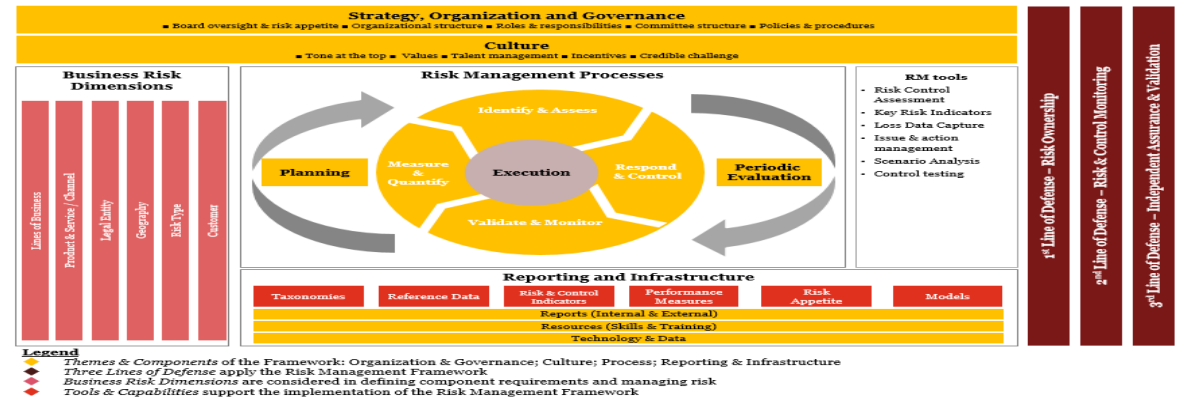
Day 2 to 3	Day 5
Conduct meetings/discussion to understand various committees, board structure and organisation structure. Review of delegation of authority and segregation of duties, review of KPI and KRI statements. Review of annual performance system. Review of operating structure and	Assistance in redefining of the 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

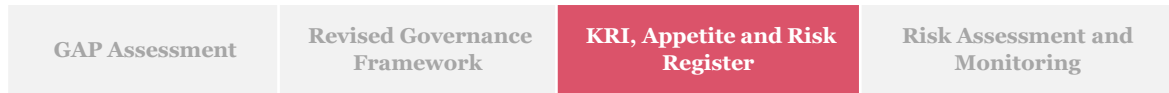


Week 5



Detailed Approach (3/4)

C.



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.

Key Activities

Central Level

- 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

Department 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

Value addition

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

Deliverables

Revised Risk Registers

No.	Key Risk Item	Risk Type	Current Risk Rating	Residual Risk Rating	Progress	Risk Owner	Remarks
			Current at 30th September 2017	Projected at 31st March 2018			
1	Expense over run risk - Risk that the actual expenses being higher than the assumed expense leading to pricing leading to lower profitability resulting in deferment of breakeven point	Life Insurance	Serious / Frequent	Serious / Frequent		Finance/Actuarial	Expense overrun continues to be risk as there was an outage of 15% in FY 2016-17. The under performance of channels compared to plan has led to outage in overruns. Measures are taken to mitigate risk with continuous efforts to improve Revenue KPIs of Proprietary Channel, acquire strategic partners and synergies with B&G which would help to optimize cost
2	Mortality risk - Risk of higher incidence of deaths against expected, due to anti selection, fraud, natural calamities, etc. resulting in adverse impact on profit	Life Insurance	Minor / Frequent	Minor / Frequent		Actuarial/Claims/Sales	Quarterly monitoring of actual to expected claims is performed and underwriting practices are aligned based on this monitoring.
3	Lapse risk- Inability to achieve planned / priced persistency Risk that non achievement of persistency assumed in pricing and business plans leading to underachievement of plans resulting in impact on Company's profitability	Life Insurance	Minor / Frequent	Minor / Frequent		Actuarial/Persistency Sales	i) Risk has been maintained at the same level as at an entity level and we expect no significant increase / decrease in risks ii) CAB will continue to be a challenge with the share of good persistency partner share decreasing but will be compensated with an improvement in prop channel performance as a lot of steps have been taken to ensure the renewal improve.
4	Solvency risk- Risk that the company is not able to maintain the Solvency Margin as mandated by the Regulator.	Life Insurance	Serious / Remote	Serious / Remote		Finance/Actuarial	Three months solvency projection is performed. This helps to initiate capital call in advance.

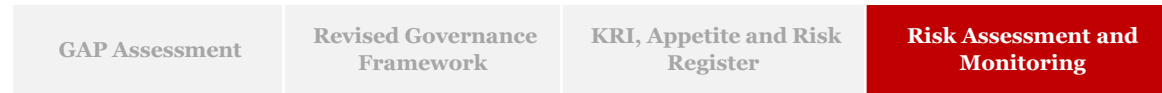
Week 6 to Week 7



March 2019
23

Detailed Approach (4/4)

D.



Phase D: Risk Assessment and Monitoring

Given the context we can assist organisation in identifying the gap in existing risk assessment framework, methodology to use, risk identification process and monitoring process which helps organisation in making decisions and achieving strategy and business Objectives.



1 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

2 Detailed discussion for understanding the data points utilized for risk assessment procedures and assessing the achievement of risk threshold limit

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

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

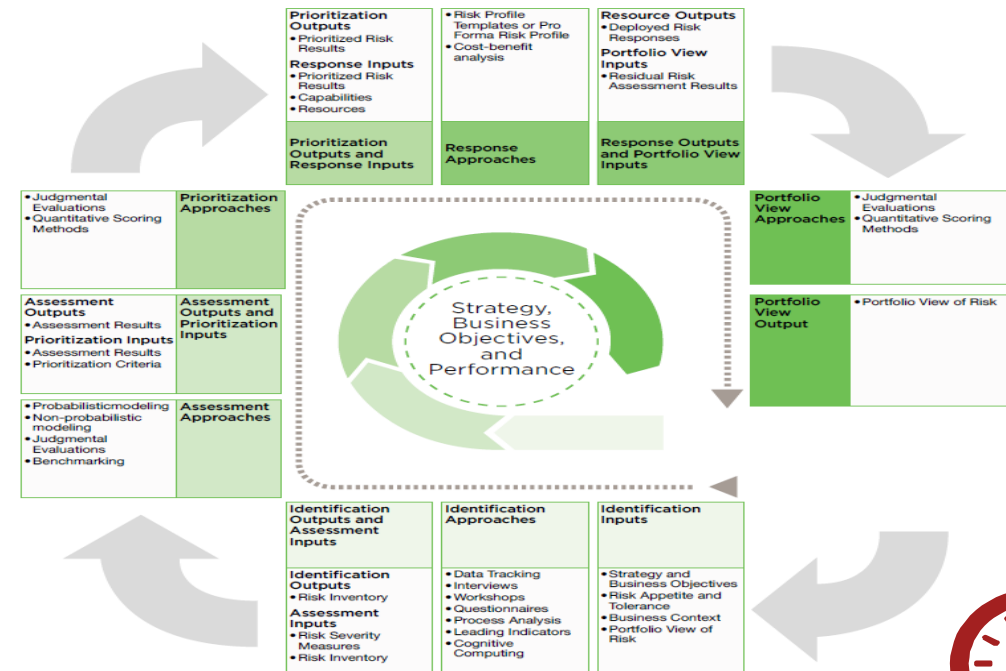
5 Review of methods and approach for emerging risk and cyber risk. Review of process for assessing the severity of the risk

6 Review of process adopted for developing portfolio view of risk

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

8 Analyze the process of monitoring the implementation of mitigation plan. Review of Reporting to Board and Management Suggestion of enhanced MIS and dashboards

Linking Risk Assessment Processes, Inputs, Approaches and Outputs



Week 8

Our View- Risk Management Framework



■ Risk origination ■ Risk management



Thank you

All images in this presentation are protected by copyright, trademark, patent, trade secret and other intellectual property laws and treaties. Any unauthorised use of these images may violate such laws and shall be punishable under appropriate laws. Our sharing of this presentation along with such protected images with you does not authorise you to copy, republish, frame, link to, download, transmit, modify, adapt, create derivative works based on, rent, lease, loan, sell, assign, distribute, display, perform, license, sub-license or reverse engineer the images. In addition, you should desist from employing any data mining, robots or similar data and/or image gathering and extraction methods in connection with the presentation.

© 2019 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Private Limited (a limited liability company in India), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity

MB/December 2019-12801