OLIVER WYMAN

AFERM
Best Practices: Guideposts, Risk Registers and a Maturity Model

G.Edward DeSeve, Senior Advisor

September, 2014

MARSH & McLENNAN COMPANIES

Introduction

- Guide Posts- As governments design ERM programs, they must look to existing guidance as a “necessary but not sufficient “ starting point
- Risk Registers- These capture, classify and monitor risks
- Maturity Model- Gives agencies a self- evaluation against accepted standards.

Guide Posts

- **Guidance for Federal Agencies**
- National Preparedness Goal- Presidential Decision Directive Eight (PDD 8)
- National Planning Frameworks:
  - National Prevention Framework
  - National Protection Framework
  - National Mitigation Framework
  - National Response Framework
  - National Disaster Recovery Framework

Guide Posts cont'd

- National Infrastructure Protection Plan- PDD 21
- Continuity of Operations- National Security Presidential Directive 51
- Internal Controls- OMB Circular A-123
- ERM Strategy- OMB Circular A-11
- Private Sector Guidance
- Committee of Supporting Organizations (COSO)
- International Organization for Standardization (ISO) 31000

Risk Registers: Questions to be addressed

- Drivers- What are the key factors that give rise to the risk?
- Consequences- What are the potential effects of the risk on agency performance?
- Impacts- If the event contemplated occurs, how significant is it?
- Related risks- Are there other risks that would be triggered if this risk transpired?
- Indicators- What will indicate the presence and severity of the risk?
- Thresholds- When does the risk become significant?
- Mitigation- What can be done to prevent or contain the risk?
- Ownership- Who is responsible for identifying, monitoring and dealing with the risk?
- Future Actions- If the risk occurs and spreads, who will deal with it?

Risk capture

Risks should be captured by the sectors and functions on a common template with a shared understanding of terms

Risk Category	Risk	Key drivers	Consequences	Financial impacts	Related risks
• *Standard high-level risk category*	• *Category of events that could increase the volatility of planned outcomes* • *Standard risk name from revised categorisation document – for consistency across the Group*	• *Key factors / events that give rise to the risk* • *May vary according to region / market circumstances* • *Helps to focus mitigation actions*	• *Effect of risk on strategic goals / financial performance / operational effectiveness* • *Helps in the identification of severity*	• *Quantification of the consequences of the risk* • *Input from assessment of severity and likelihood (gross and net)*	• *Other risks the risk is influenced by* • *Risks this risk influences* • *Contributes to aggregation and scenario analysis*
Fixed across years[1]		Broadly stable		Varies across/within years	

1. Subject to review

Risk monitoring

Key risks should be monitored against key indicators, giving rise to increased mitigation efforts as required

Risk	Key drivers	Risk indicators and threshold	Risk status	Adjustment to financial impacts	Current mitigation actions	Owner	Additional decision
• *Standard risk name for consistency across the Group*	• *Key factors / events that give rise to the risk* • *May vary according to market circumstances* • *Helps to focus mitigation actions*	• *Ideally leading, but lagging where necessary* • *External (e.g. economic, market, etc)* • *Internal performance (e.g. operational, financial)* • *Tolerance thresholds for indicators*	• *Indicator results at last time period* • *Indicator results at current time period* • *Traffic light status against tolerance thresholds*	• *Qualitative change in severity of impact* • *Qualitative change in likelihood of impact*	• *Focused set of actions designed to address the key risk drivers*	• *Individuals / bodies responsible for mitigation actions* • *Support of additional key individuals / bodies noted as required*	• *Proposed further actions to be undertaken to bring amber and red results back to green*
Fixed across years[1]	Fixed within the year		Varies by reporting period		Fixed within the year		

Traffic light reporting

Within acceptable bounds	No additional action required
Cause for concern	Additional action to be considered
Significant concern	Additional action required immediately

1. Subject to review

Toward a Maturity Model

- Framework
- Criteria
- Scorecard

Evaluation framework

Internal sources

Oliver Wyman intellectual capital

- Proprietary ERM framework
- Industry, FTSE 100 and Fortune 500 ERM experience

External sources

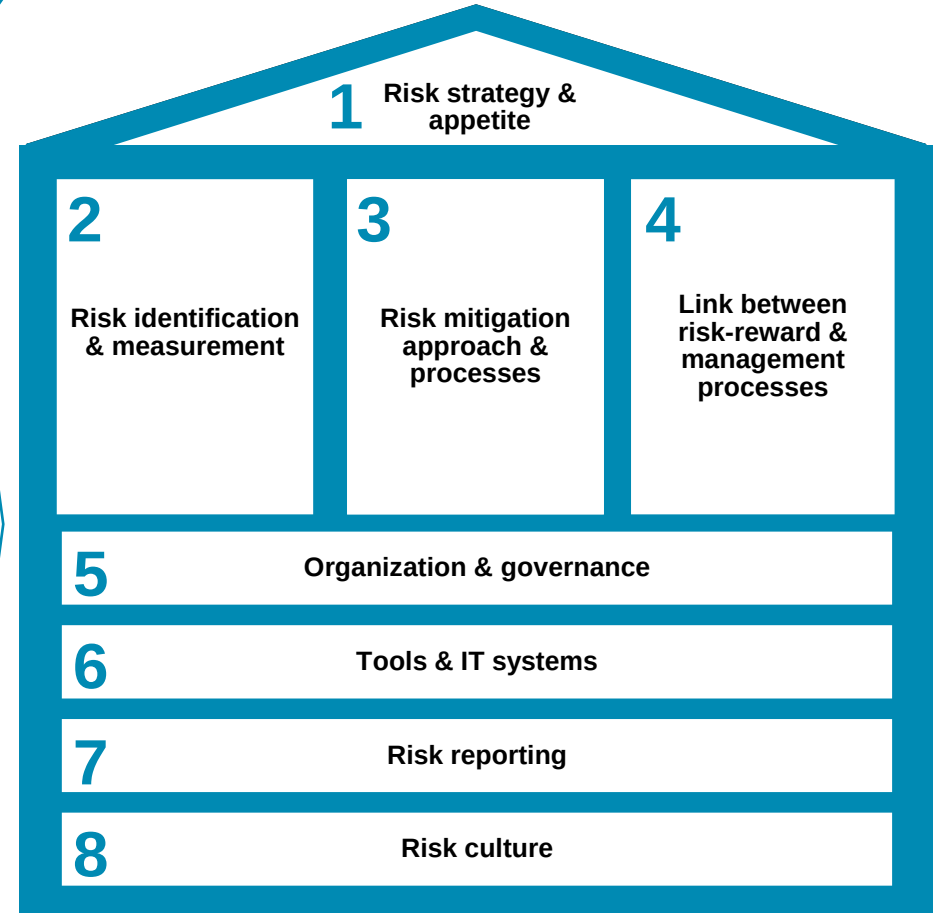
Laws, regulations and statements of financial practice

- AS/NZS 4360:2004 – Risk management standard
- Committee of sponsoring organizations (“COSO”) Enterprise Risk Management – Integrated Framework
- NYSE/SEC corporate governance rules
- Sarbanes Oxley Act
- Turnbull report – Internal control: Guidance for directors on the combined code
- Cadbury report – The financial aspects of corporate governance
- Principle 11 and Accompanying Singapore Code of Corporate Governance
- Rating agency (S&P, Moody’s, Fitch) ERM rating criteria
- ISO 31000 – Risk management principles and guidelines

Market-based research

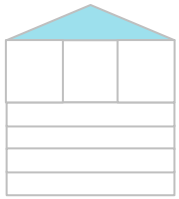
- Conference Board ERM survey – From risk management to risk strategy: Research report and guidelines
- Conference Board risk management publications – getting your arms around ERM; The future of ERM; ERM systems: Beyond the balanced scorecard
- Risk and Insurance Management Society (“RIMS”): Risk Maturity Model (“RMM”) for Enterprise Risk Management
- Publicly available market/industry ERM publications
- WEF Global Risks Report

Oliver Wyman’s ERM evaluation framework



Assessment criteria

Initial	• Capabilities related to the component are absent or completed on an ad-hoc basis only • Capabilities are characteristic of certain individuals, not of the organization
Basic	• Capabilities related to the component have some organizational framework, but practice is largely intuitively reinforced rather than embedded • Regulatory requirements related to the sub-component appear to be met where relevant
Established	• Key capabilities related to the component are present across the company • Policies, processes, and techniques, even if unsophisticated, are well-defined and applied with appropriate support
Advanced	• Sophisticated capabilities related to the component are tailored to the organization and proactively used to address its risk management needs • Policies, processes and techniques are well aligned and applied in a standardized way
Leading edge	• Sophisticated capabilities that are continually improved are embedded in decision-making processes across the company • The organization is focused on using its capability as a source of strategic advantage and increased operational effectiveness



Risk strategy & appetite
Oliver Wyman's ERM evaluation scorecard (1/8)

Draft

Design criteria	Basic	Established	Leading edge
Metrics/features used	• Defined along a very limited (1-3) set of metrics in expected case • No quantitative analysis conducted for parameterization • Not used for further limitation	• Delineation of strategic vs. non-strategic risk (risk accepted, risks to avoid) • Small set of (2-5) metrics (e.g. net debt factor, earnings volatility) under a simplified stress scenario (e.g. 1:10) • Top-down guidance on risk limits	• Definition of tolerance for multiple (~5-7) key trackable metrics under various scenarios (e.g. 1:10, specific crisis scenarios…) • Frequent tracking and monitoring of risk appetite levels (automated process) • Regular tracking of Risk Bearing Capacity vs. Risk Capital used • "Translation" into operational limits and bottom-up/top-down risk limit reconciliation
Purpose and relevance	• Mainly for informational purpose as an additional item for consideration	• Creates an explicit link between the business strategy and the risk taking activities undertaken	• Serves as the guideline for risk-taking and the basis for the overall risk limit system
Level of formalization	• Vaguely formalized • Typically not approved by the whole board (often only full endorsement by CFO/CRO) • Typically not part of senior stakeholder conversation and decision-making	• Formalized, aligned and comprehensive risk appetite which serves as the basis to control and limit any risk taking activity undertaken by the company • Formal risk appetite statement approved by the Managing Board considering input from key stakeholders	• Extended set of stakeholders involved during definition • Risk Capital introduced as common currency for risk
Implementation rigour	• Risk appetite non-prescriptive high-level guideline	• Risk appetite additional secondary target and constrain	• Risk appetite statement key element of steering
Frequency	• Tracked half-yearly • Reviewed 1x every 2 years	• Tracked quarterly • Reviewed 1x year	• Tracked monthly • Reviewed 1x year