Capacity Building Seminar On Enterprise Risk Management
Hotel Sea Princess, Juhu
10 August 2018

Enterprise Risk Management

Amol Padhye

Head Market Risk, HDFC Bank

Institute of Actuaries of India

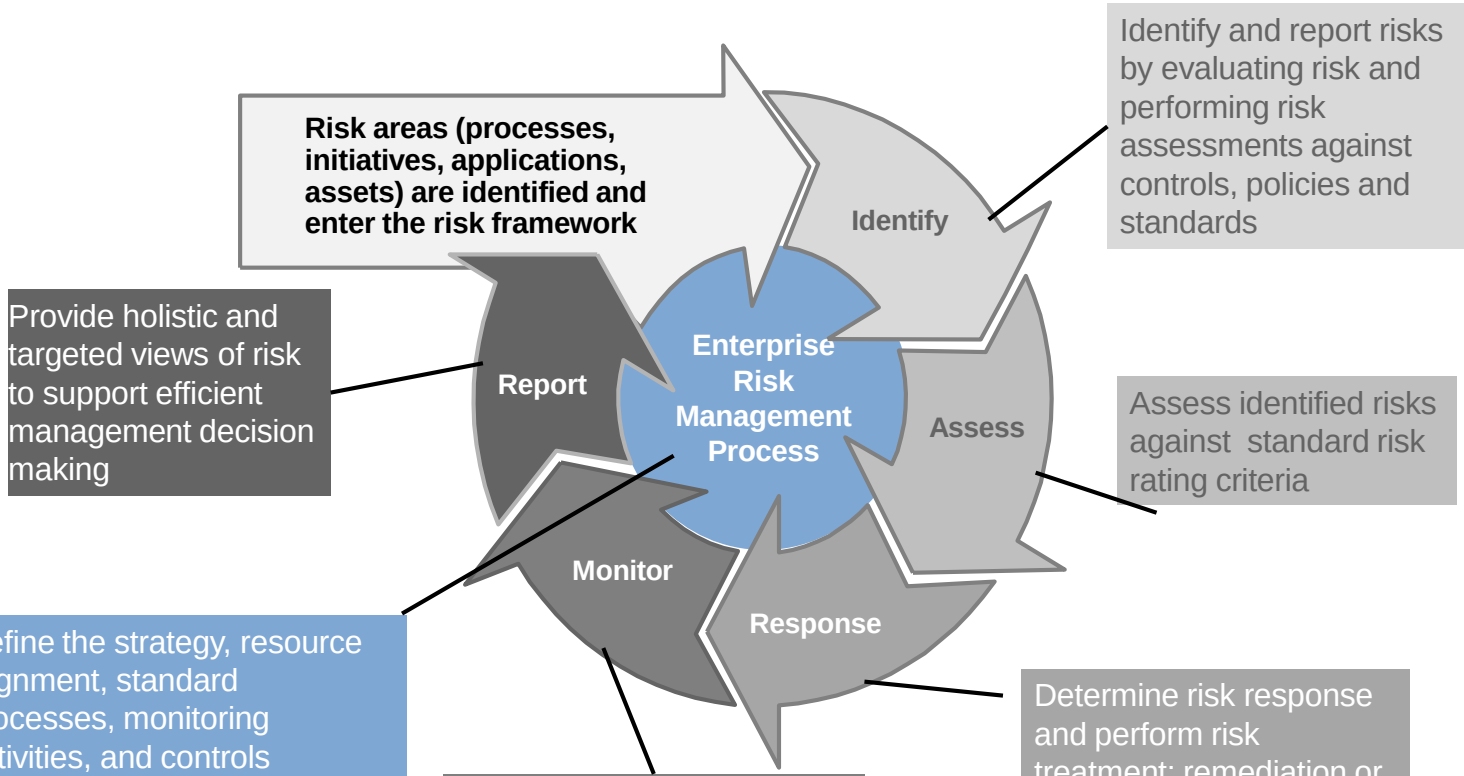
What is ERM

ERM is a framework of systematic management practices to assess and monitor risk

"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

1. Minimizing Threats
2. Maximizing opportunities

ERM Process


Risk areas (processes, initiatives, applications, assets) are identified and enter the risk framework
Identify
Identify and report risks by evaluating risk and performing risk assessments against controls, policies and standards
Assess
Assess identified risks against standard risk rating criteria
Response
Determine risk response and perform risk treatment; remediation or acceptance
Monitor
Analyze risk trends and monitor status of risk mitigation plans
Report
Provide holistic and targeted views of risk to support efficient management decision making
Enterprise Risk Management Process
Define the strategy, resource alignment, standard processes, monitoring activities, and controls necessary to consistently and effectively manage enterprise risks to an acceptable level

COSO Framework

Institute of Actuaries of India

Internal Environment
Sets the basis for how risk is viewed and addressed by the Bank's top management.

Objective Setting
Senior Management sets the business strategy and ensures these are consistent with risk appetite

Event Identification
Internal and external events that could affect achievement of Bank's objectives are identified and assessed to distinguish between risks and opportunities

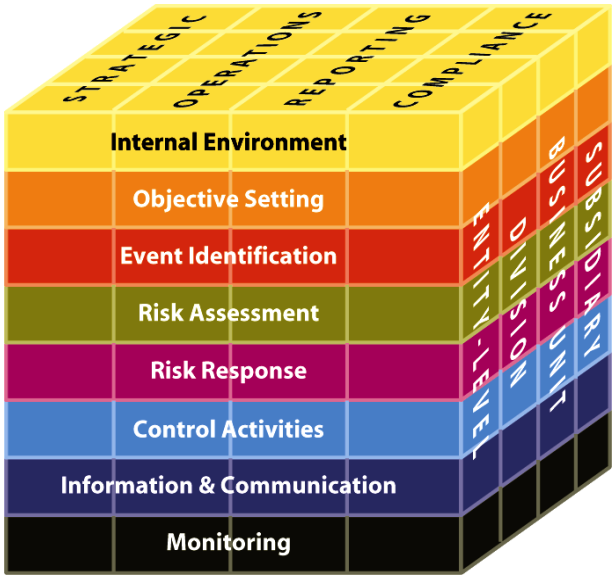
Risk Assessment
Cost versus benefit of activity takes account of the possible risk impacts of the internal model and the value in protecting against these exposures

Risk Monitoring
Identify and evaluate possible risk responses given by business units

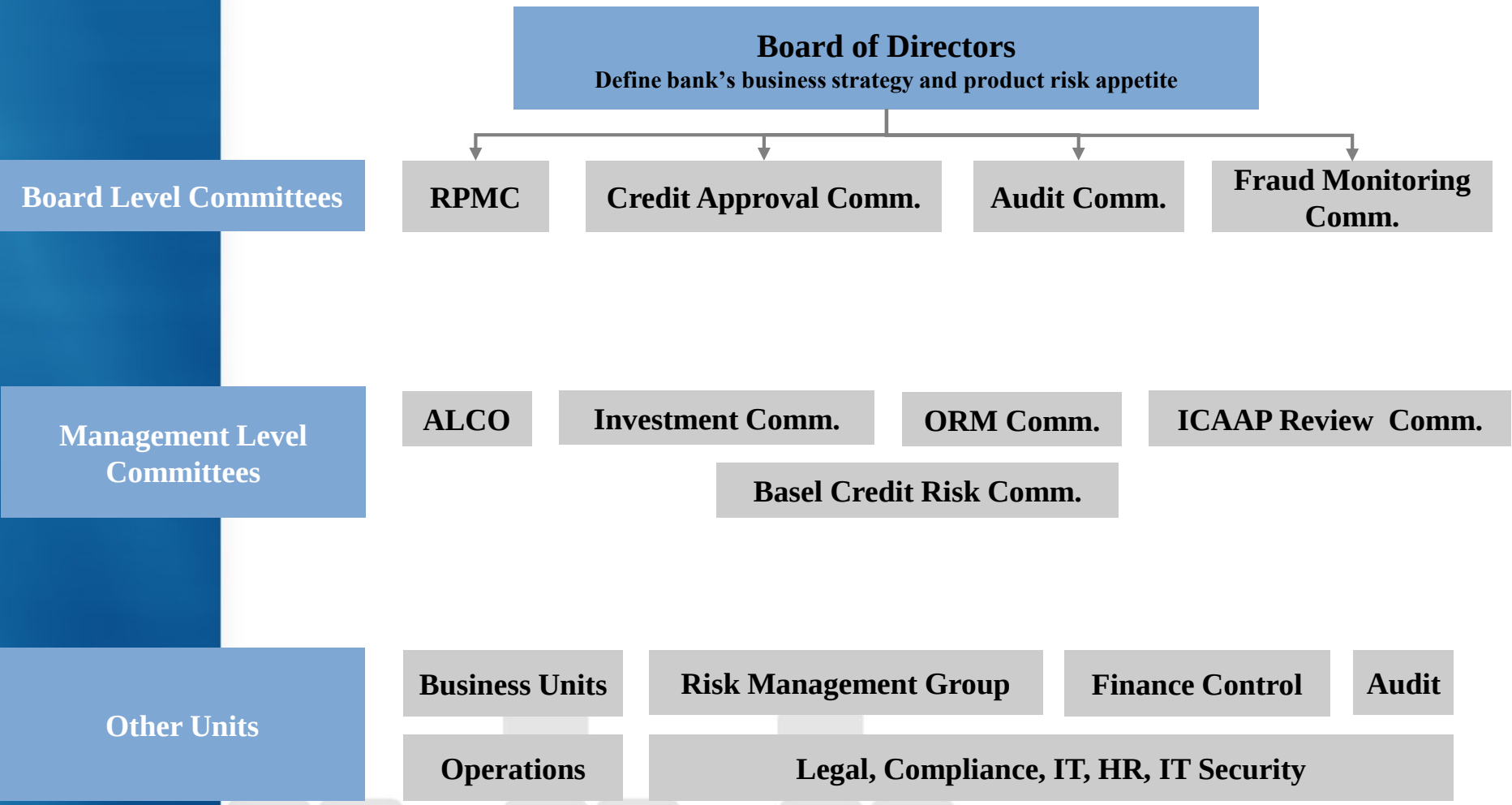
Control Activities
Encompass all the possible responses to risk, whether viewed as opportunities, uncertainties or hazards.

Information & Communication
Ensure relevant information is identified, captured, and communicated throughout the organization

Monitoring
A good mix of indicators and other internal and external data is identified to monitor and manage risks



Control Environment



Risk Assessment

Institute of Actuaries of India

Credit Risk

- Possibility of losses that stem from outright default due to inability or unwillingness of a customer or counterparty to meet commitments in relation to lending, trading, settlement and other financial transactions
- Bank identifies existing and potential credit risks inherent in any product, exposure or activity, involving a comprehensive review of existing and potential credit risk characteristics.

Market Risk

- Market risk refers to price risk which is the risk of the asset value declining, over a reporting period, due to changes in risk factors.
- The major risk factors include interest rates, foreign exchange rates, equity/commodity prices, basis/spread curves and volatility curves for various assets or currency pairs.
- It also arises due to demand & supply gap i.e. liquidity tightness resulting into impact cost of the asset/liability.

Risk Assessment

Liquidity Risk

- Liquidity risk is the risk that the bank may not be able to fund increases in assets or meet obligations as they fall due without incurring unacceptable losses.
- Interest rate risk is the risk where changes in market interest rates might adversely affect a bank's financial condition.
- The immediate impact of changes in interest rates is on Net Interest Income (NII) and long term impact of changing interest rates is on bank's net worth.

Operational Risk

- Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
- Primary tools for risk assessment used are:
  1. Risks and Controls Self – Assessment (RCSA)
  2. Scenario Analysis (severe infrequent but plausible events)
  3. Internal Loss events database

Control Activities

Institute of Actuaries of India

Preventive Controls

- **Credit Risk**: based on an adequately comprehensive risk assessment, credit exposure limits are set on individual counterparties, pursuant to dimensioning the overall credit appetite on the counterparty
- **Market Risk**: specifies the risk appetite of the Bank in the form of limits and triggers for positions. For IRRBB, the impact on NII and MVE are tracked against limits linked to the budgeted NII and capital for the year respectively.
- **Liquidity Risk**: Banks set tolerance limits on cash-flow gaps, stock ratios, Basel III ratios, limits on borrowing and lending sources etc.
- **Operational Risk**: identification of KRIs and develop scorecard to keep track of risk of loss resulting from inadequate or failed internal processes, people and systems or from external events

Detective Controls

- **Stress Testing**: Stress testing is commonly described as the evaluation of a bank's financial position under a severe but plausible historical or hypothetical scenario to assist in decision making within the bank. The stress framework is applied to credit risk, market risk, liquidity risk, operational risk, securitization risk, retail credit.
- **Reverse Stress Testing**: It starts from an outcome of business failure and identifies circumstances where this might occur. Reverse stress testing is primarily designed as a risk management tool in identifying scenarios and underlying dynamism of risk drivers in those scenarios that could cause an institution's business model to fail.

ICAAP provides comprehensive guidance to develop a framework which shall include the capital adequacy assessment and projections of capital requirements along with the plans for maintaining capital levels, framework for risk assessments, stress testing etc.

Challenges

Institute of Actuaries of India

Challenge	Business consequence	Impact
Oversight & Governance ▪ Different governance structures. Oversight conducted by different management committees	▪ No enterprise-wide risk and control oversight ▪ No clear basis for enterprise-wide decision making ▪ Confusing lines of authority and responsibility	▪ Duplication and overlap results in inefficient use of risk resources ▪ Business units feel an excessive burden, resulting in fatigue and increased costs ▪ Inconsistent reporting to senior management, limiting its effectiveness and hindering analysis ▪ Excessive risk governance and remediation costs ▪ Too much focus and attention paid to low priority issues ▪ Lack of comprehensive, transparent and consistent risk information for decision making
Organizational View ▪ Differing organizational views: legal entity, process, function, business hierarchy, financial statement, or rule-based perspectives	▪ Misalignment of roles and responsibilities ▪ Inconsistent view of organization, reducing transparency and capacity for effective enterprise-wide governance and reporting (and , ultimately, resource allocation)	
Risk & Control Definitions ▪ Business risks and controls are described, assessed and reported differently under each process	▪ Overlapping assessments performed on same processes. Difficult to roll-up risks/results	
Risk & Control Criteria ▪ Measurement and assessment criteria for the same risks and controls may differ	▪ Ambiguity among risk owners of how to assess the risk ▪ Inconsistent ranking of similar risks and controls ▪ Varying risk tolerance thresholds	
Reporting & Technology ▪ Siloed reporting for each process with inconsistency in approach and information ▪ Multiple IT platforms	▪ Multiple reporting covering similar activities ▪ Restricted view of overall risk profile at business and enterprise level ▪ Siloed technology impedes management's ability to gain a consolidated view of key exposures	
Quality Assurance & Validation ▪ Multiple QA initiatives to validate effectiveness ▪ Varied approaches to monitoring and testing	▪ Multiple testing groups ▪ Confusion over roles and responsibilities	

Institute of Actuaries of India

Thank You