MERCER OLIVER WYMAN

May 20, 2005

Enterprise Risk Management (ERM): Getting Beyond Risk Identification to Sustainability

Michael Chagares - Washington, DC
Christopher McCarthy - Atlanta, GA

CORPORATE RISK CONSULTING

Confidentiality

Our clients' industries are extremely competitive. The confidentiality of companies' plans and data is obviously critical. Mercer Oliver Wyman will protect the confidentiality of all such client information.

Similarly, management consulting is a competitive business. We view our approaches and insights as proprietary and therefore look to our clients to protect Mercer Oliver Wyman interests in our presentations, methodologies and analytical techniques. Under no circumstances should this material be shared with any third party without the written consent of Mercer Oliver Wyman.

Contents

Section 1

Introduction – ERM drivers & trends

ERM key drivers – is there a really a need?

External

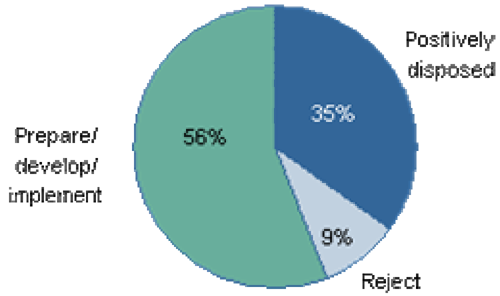
- Pressure from:
  - Key stakeholders (e.g., debt holders, rating agencies, investor community, exchanges)
  - Corporate governance requirements
  - Regulatory (e.g., SOX)
  - Legislature (e.g., SOX) – extension into broader RM)
  - Other:
    - COSO ERM framework adoption
    - International risk management standards
    - Federal government
- Shareholder advocacy
- Need for greater disclosure and transparency

Internal

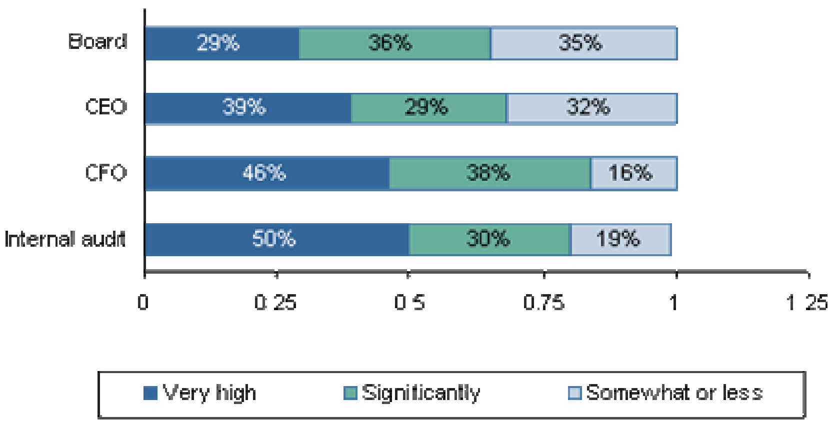
- Desire for increased understanding and quantification of strategic and operational risks
- Pressure from the Board and Audit Committee to understand the risk profile
- Desire for improved informed decision-making and communications
- Need to demonstrate a continuous sustainable ERM process and framework
- Limited tolerance for surprises
- Desire to align risk with strategy and key decision-making
- Desire to increase ability to identify, quantify, measure and monitor risks across the organization

Selected findings from the Conference Board's ERM survey

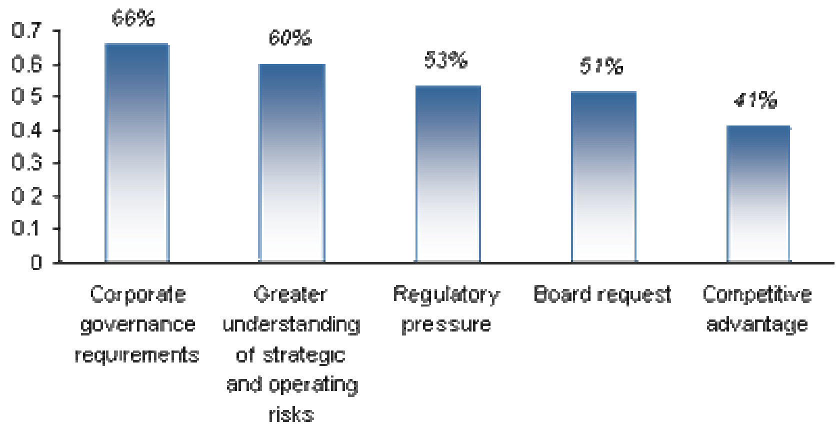
A majority of companies are choosing ERM



ERM is seen as an increasingly important responsibility by the ...



Primary drivers for implementing ERM



Highest priority ERM objectives

Ensure risk issues are explicitly considered in decision making	1
Avoid surprises and “predictable” failures	2
Align risk exposures and mitigation programs	3
Institute more rigorous risk measurement	4
Integrate ERM into other corporate practices like strategic planning	5

(Source - The Conference Board/Mercer Oliver Wyman ERM Survey Executive Action Report, January 2005).

Companies with advanced ERM experience greater benefits

Benefit	Advanced ERM companies Rank	Advanced ERM companies Percent	All other companies Rank	All other companies Percent
Better informed decisions **	1	86%	1	58%
Greater management consensus ***	2	83	5	36
Increased management accountability ***	3	79	7	34
Smoother governance practices ***	4	79	3	39
Ability to meet strategic goals ***	5	76	5	36
Better communication to board +	6	69	2	52
Reduce earnings volatility	7	62	4	37
Increased profitability **	8	59	8	33
Use risk as competitive tool **	9	46	9	22
Accurate risk-adjusted pricing **	10	41	10	2

*** 99.9% likelihood of significant difference between advanced ERM and all other companies

** 99% likelihood * 95% likelihood + 90% likelihood

(Source - The Conference Board/Mercer Oliver Wyman ERM Survey Executive Action Report, January 2005).

Implementation difficulties

	Very significant challenge	Significant	Moderate	Less than moderate
Competing priorities	25%	34%	24%	17%
Insufficient resources (people/tech/financial)	12	32	29	27
Lack of consensus in ERM's benefits	10	22	31	37
Getting organization to make changes	10	27	31	32
Lack of quantification of "soft risks"	7	31	30	32

(Source - The Conference Board/Mercer Oliver Wyman ERM Survey Executive Action Report, January 2005).

ERM: shift in focus

From		To
Fragmented	→	Integrated
Negative	→	Positive
Reactive	→	Proactive
Ad hoc	→	Continuous
Historical-looking	→	Forward-looking
Cost-based	→	Value-based
Narrowly-focused	→	Broadly-focused
Silos	→	Systematic
Functionally-driven	→	Process-driven

Assessing your organization

- Does management agree on the corporate risk profile for your organization?
- How is the corporate risk profile derived?
- Is the corporate risk profile continuously updated?
- Does management know the real level of impact and likelihood for these risks?
- Does management understand how effectively these critical risks are being managed?
- For risks that are undermanaged, does your organization have a plan in place to improve the management of these risks and how is this plan tracked/ monitored?
- For risks that are overmanaged, does your organization have a plan in place to improve the management of these risks?

Source: Making Enterprise Risk Management Pay Off, 2002.

Assessing your organization (continued)

- Does your organization take inconsistent levels of risks?
- What is your organization's risk appetite?
- How do your strategies align with your risk appetite?
- Is risk management an integral part of your organization? If not, why not?
- What governance structure is in place at the board and management level to ensure appropriate understanding and analysis of risk information?
- How is risk information communicated to external stakeholders, i.e., analysts, debt holders, shareholders, etc.?

Section 2

Overview of path to sustainability/ ERM Framework

Mercer Oliver Wyman ERM definition

Enterprise Risk: The uncertainties that a company must understand and effectively manage as it develops and executes its strategies and creates shareholder value.

Enterprise Risk Management: A structured and disciplined approach that supports the alignment of strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties an organization faces as it creates value.

- Aligns with strategic intent and related objectives.
- Includes all business risks, not just financial ones.
- Integrates into the management process - becoming every manager’s responsibility.
- Addresses both the hard and soft sides of risk management.

COSO ERM definition

COSO Definition of Enterprise Risk Management: 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.

The definition reflects certain fundamental concepts. Enterprise risk management is:

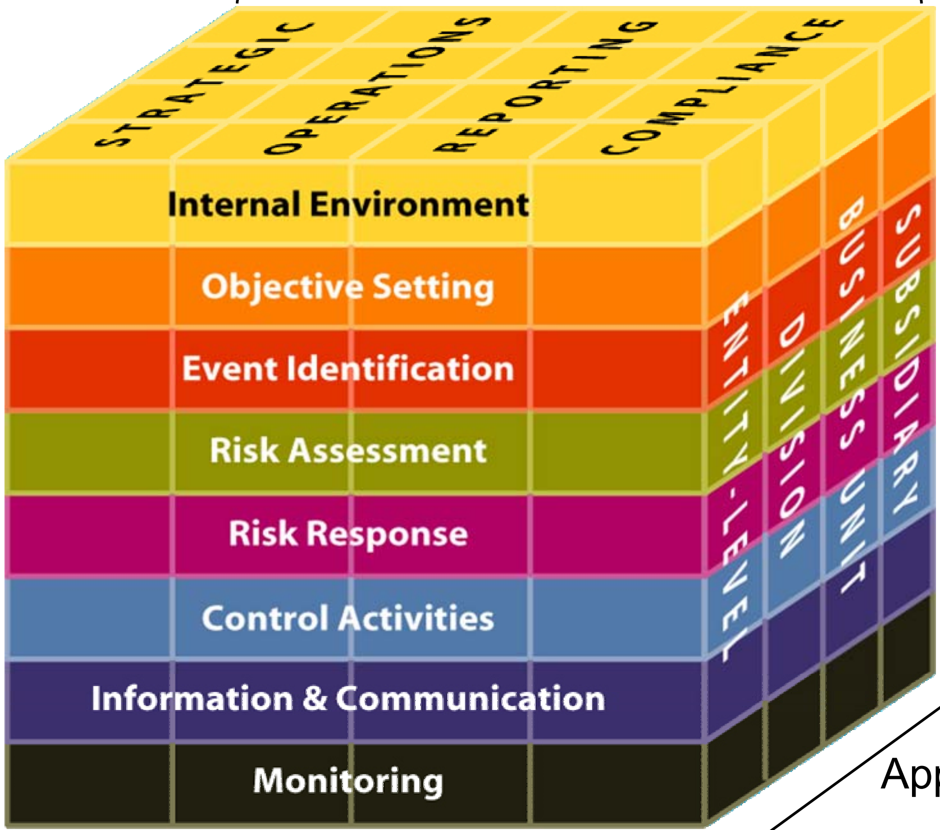
- A process, ***ongoing*** and flowing through an entity
- Effected by people at every level of an organization
- Applied in ***strategy*** setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level ***portfolio view of risk***
- Designed to ***identify potential events*** that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide ***reasonable assurance*** to an entity's management and Board of Directors
- Geared to ***achievement of objectives*** in one or more separate overlapping categories

Source: *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, 2004, (see www.coso.org).

The COSO ERM framework

ERM is a process to help achieve entity objectives across these categories

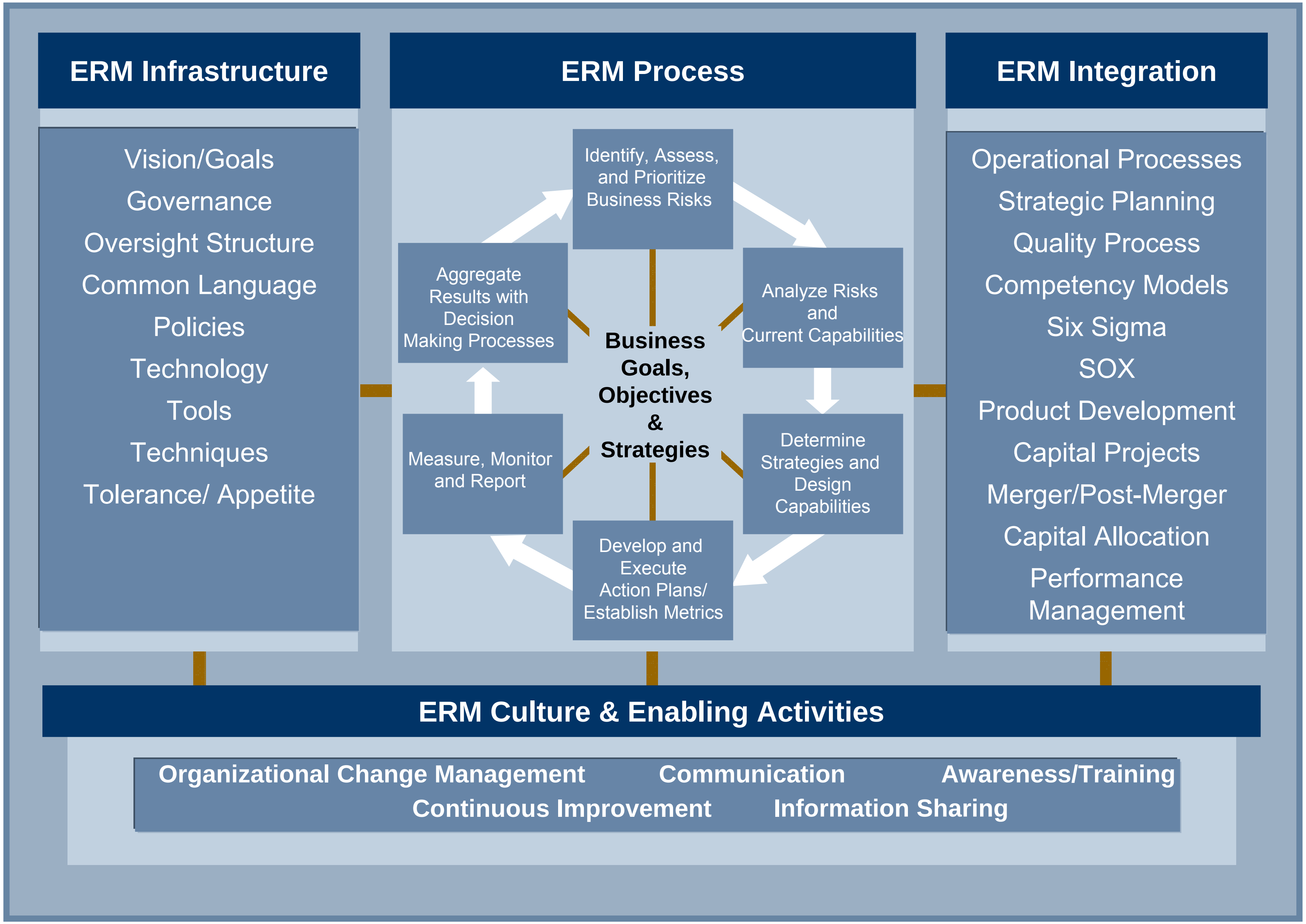
Eight interrelated components



Applies to activities at all levels of the organization

Source: *Enterprise Risk Management – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission, 2004, (see www.coso.org).

Framework for implementing ERM



ERM Infrastructure

Vision/Goals
Governance
Oversight Structure
Common Language
Policies
Technology
Tools
Techniques
Tolerance/ Appetite

Objective: Network of organizational and governance tools/ components to support the ERM Process and integration.

Vision/Goals
- Mission statement
- Value Proposition and Benefits statement

Governance/Oversight
- Organizational accountabilities and responsibilities
- Oversight structure/span of control
- Roles and responsibilities
- Monitoring

Common Language
- Company-wide understanding of risk terminology
- Business Risk Inventory

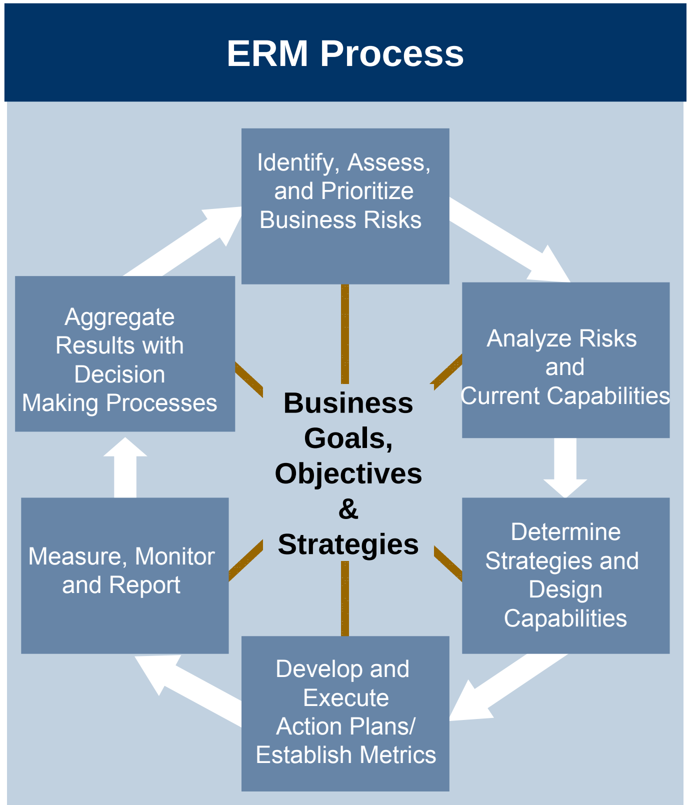
Policies & Procedures
- Risk policy manuals
- Standard operating procedures

Technology & Tools
- Risk management databases
- Analytical applications

Tools/ Techniques
- Risk diagnostic tools
- Measurement
- Modeling
- Casual Analysis

Tolerances/Limits
- Matrix of tolerances and limits
- Process for defining tolerance/ appetite

Objective: Methodology to identify, assess, prioritize, manage, and aggregate risk exposures and opportunities across the enterprise.



- Formal & continuous
- Align risks with goals and objectives
- Identify, assess, and prioritize risks
- Analyze risks (root cause, impact, interrelationships, and capabilities)
- Identify gaps in management of risks
- Develop and determine risk strategies
- Execute risk mitigation plans
- Create risk metrics
- Monitor and report on current status

Objective: Method to integrate risk management approach into both core and project related management processes and decision-making.

Business Planning
- Budgeting and planning forecasts
- Resource constraints (e.g., human, technological, and financial)
- Cost/ benefit analysis
- Cash flow analysis

Product Development
- New product development
- Business portfolio balancing
- Detailed selection criteria and decision-making process

Performance Management
- Competency models
- Reward/incentive programs
- Scorecards

Operational Processes
- Changes managed with an eye towards risk
- Workflow diagrams
- Action plan development
- Apply ERM principles

Quality/ Compliance
- Focused projects
- Metrics and reporting

ERM Integration

Operational Processes
Strategic Planning
Quality Process
Competency Models
Six Sigma
SOX
Product Development
Capital Projects
Merger/Post-Merger
Capital Allocation
Performance Management

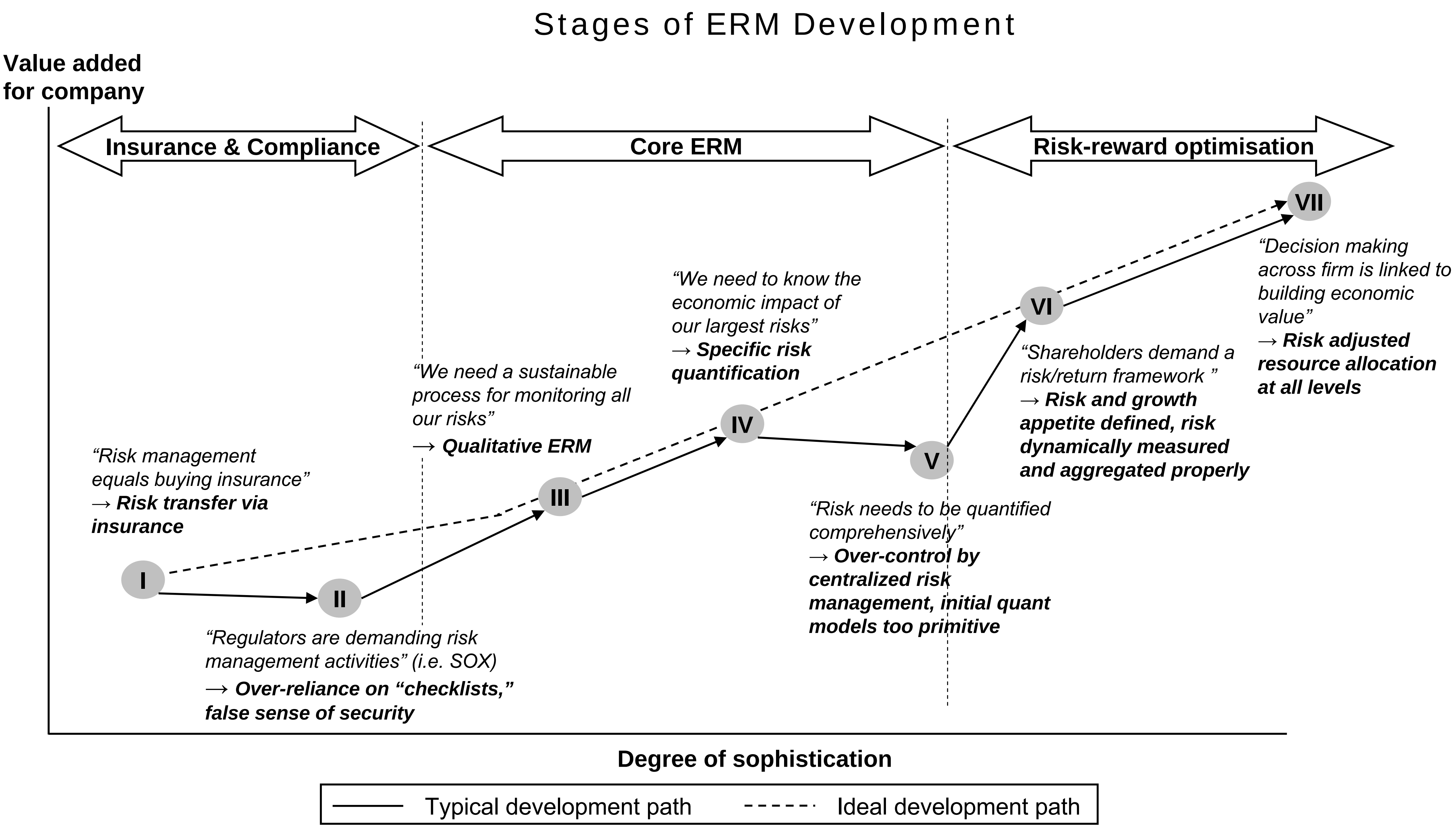
Objective: Organizational behavior reinforcing the ERM structure.

- Supports other aspects of ERM Framework through enabling activities:
  - Awareness/ Training
  - Communication
  - Continuous improvement
  - Information Sharing
  - Performance Management and Rewords
  - Organizational Change Management
  - Voice of the Employee

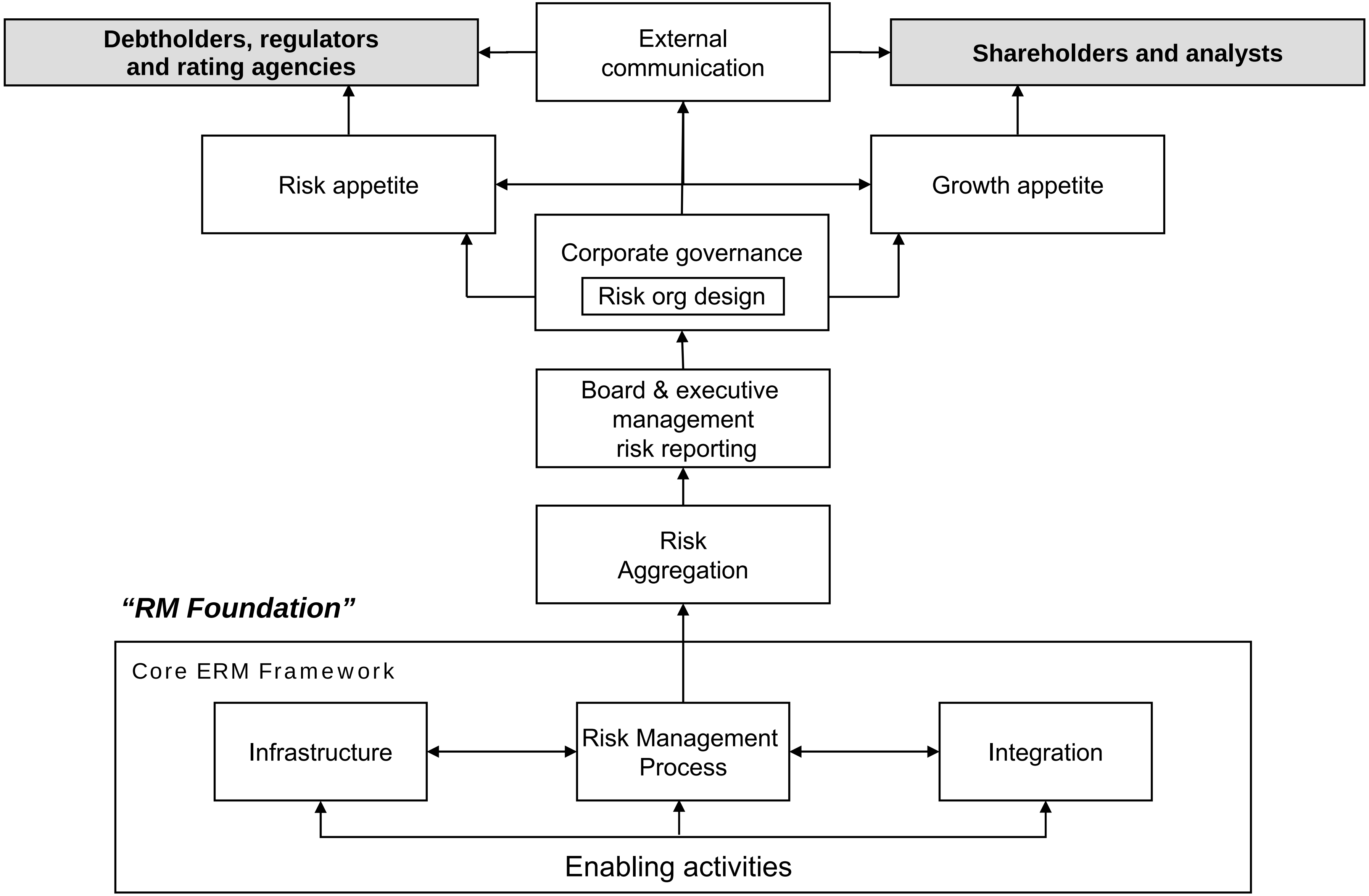
Section 3

Getting started – potential approaches & options

Seven stages of ERM . . .



ERM programs should be designed with all stakeholders in mind



Developing ERM – an evolution not revolution

PHASE I

Assessing the current state

- Risk identification
- Risk prioritization
- Risk analysis
- Risk organization
- Risk management capabilities

PHASE II

Developing the ERM framework

- Infrastructure
- Risk quantification
- Risk policies and procedures
- Technology
- Communicate initiative to organization

PHASE III

Implementing ERM

- Integrate ERM into existing risk management processes
- Integrate ERM into strategic planning / budgeting, BCP, SOX, etc…
- Integrate ERM into company culture
- ERM software integration

Getting started – implementing ERM

Assessment (A)

- Analysis of current risk exposures and management practices

Tools and techniques
- Survey
- Risk prioritization
- Business Risk Assessment

Risk Diagnostic (D)

- Expert-led analysis and assessment of specific risks.

Tools and techniques
- Risk modeling and quantification
- Monte Carlo simulation
- Facilitated workshop

Governance (G)

- Establish organizational and governance aspects of ERM

Tools and techniques
- Define role of: Board, CRO, ERM dept., risk councils
- Integrate with existing processes
- Industry best-practices/benchmarking

Strategic planning and risk appetite (S)

- Assess risk implications of strategic initiatives and verify strategic objectives they are within appetite of organization.

Tools and techniques
- Scenario analysis
- Business Risk Assessment
- Derivation of risk appetite and tolerances

Assessing the current state

A

– Illustration –

Phase I - Current State Assessment
(4-6 months)

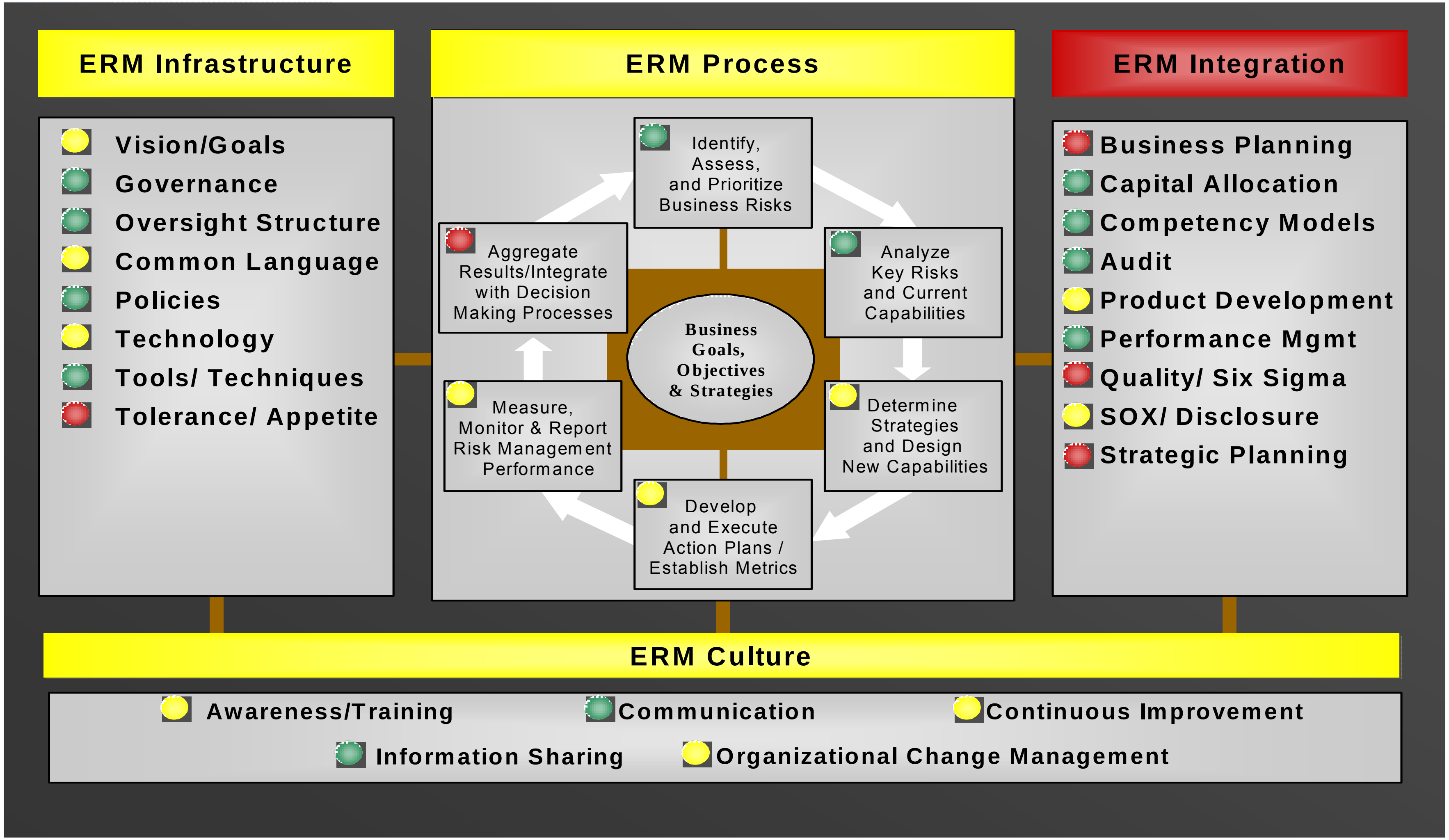
Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Finalize project workplan	**Evaluate current risk management practices**	**Define ERM future state vision**	**Conduct risk assessment to identify the most critical risks**	**Develop recommendations for: specific risk strategies**	**Develop a detailed Phase II workplan**

Deliverables

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Phase I workplan	Current State Assessment	ERM Future State Vision	Risk Profile	Recommendations	Phase II workplan
		Initial Governance/ Oversight	Gap Analysis		

Current state assessment

– Illustration –



Risk assessment

Document review

Determine preliminary risks.

Identify existing ERM components.

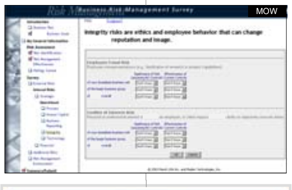
Create initial Business Risk Inventory.

Key Documents

- Annual Report
- Financial Statements
- Analyst Reports
- Strategic Plan
- Board Reports

Survey

ERM survey for bottom up risk assessment and to understand risk management practices.



Interviews

Interview executives and managers to gain understanding of risks.

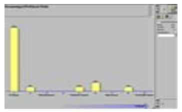
Workshop

Conduct facilitated workshop with key stakeholders, managers and executives.

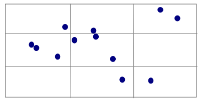
Use sophisticated voting software to facilitate session.

Analysis of workshop results.

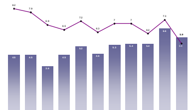
Voting



Risk profile



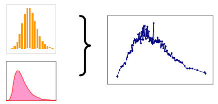
Gap analysis



Risk analysis

Conduct additional quantitative and qualitative analysis for key risks identified.

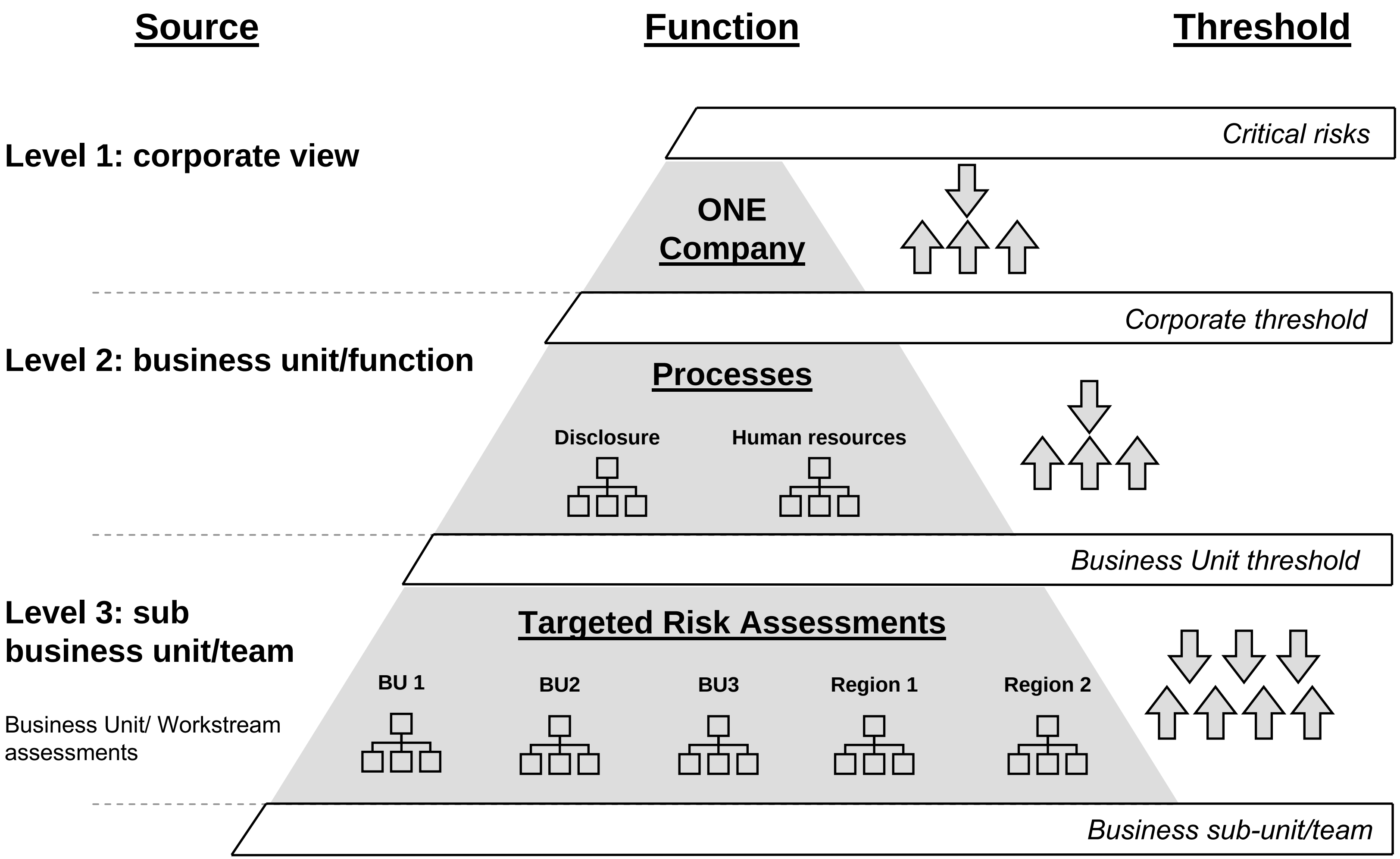
Quantification



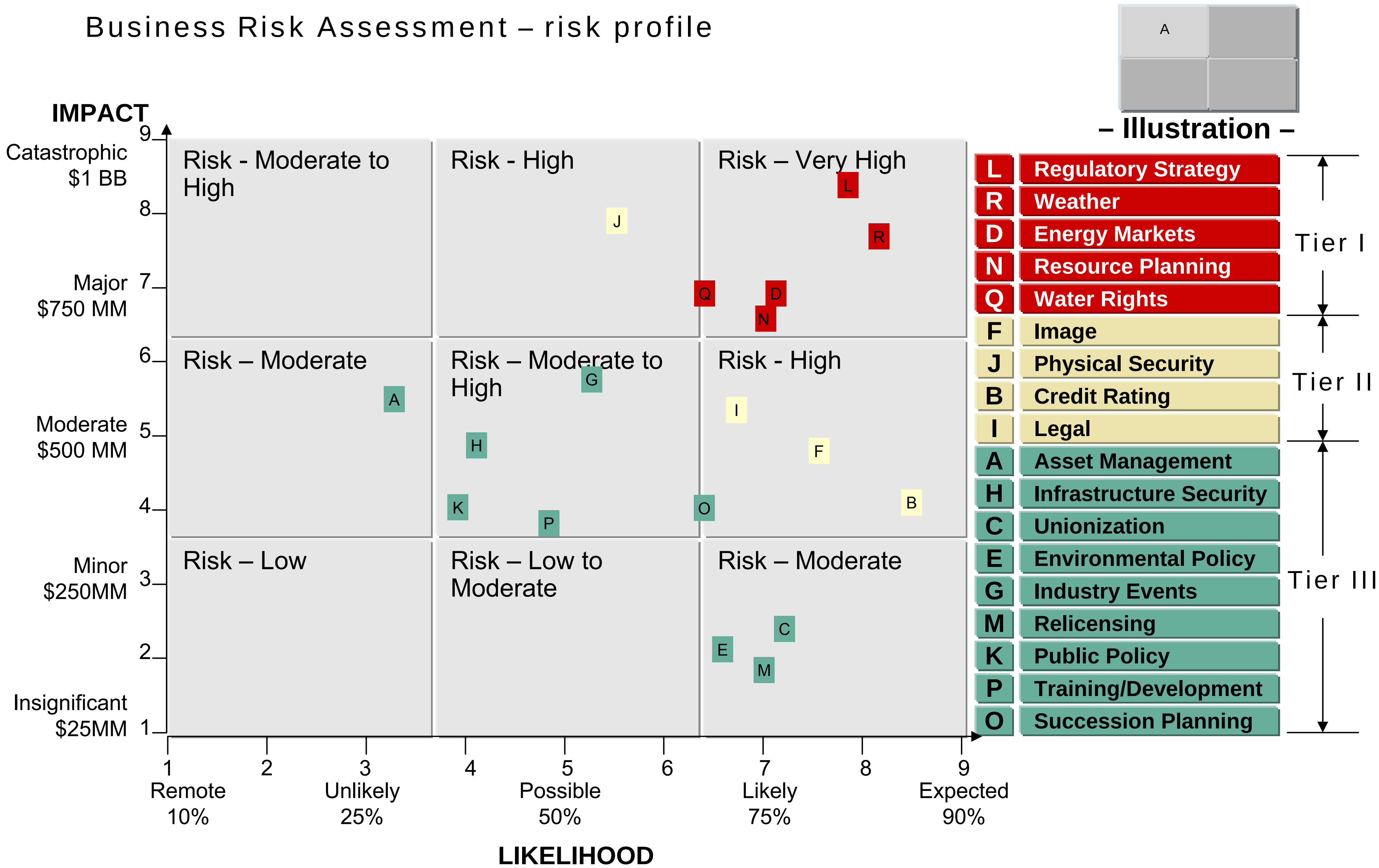
Risk hierarchy

Build a risk hierarchy to ensure that most urgent risks across the enterprise are managed at the appropriate level.

Business Risk Assessment approach

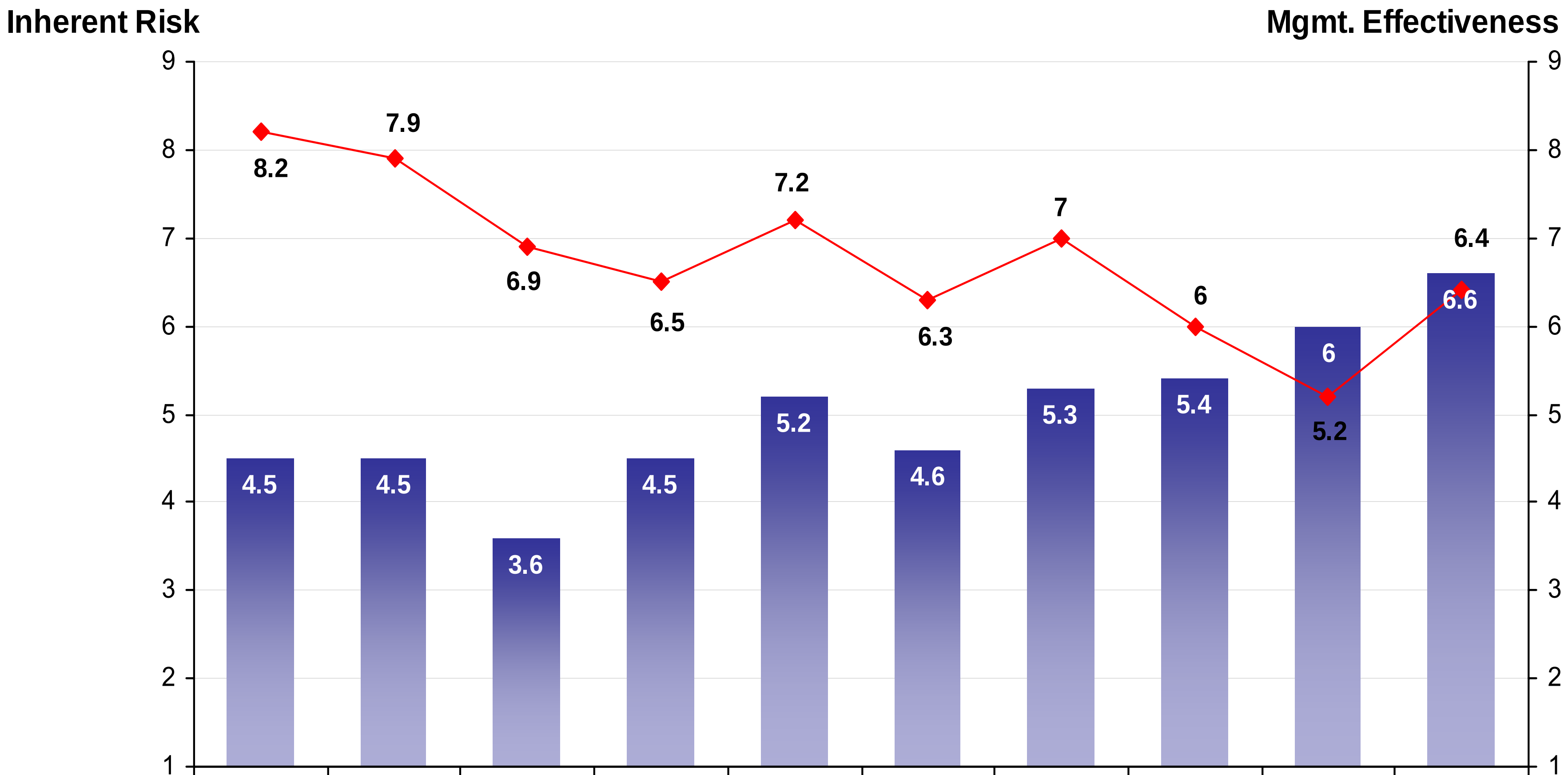


Business Risk Assessment – risk profile



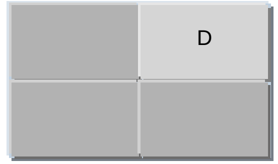
Business Risk Assessment - Gap Analysis chart

– Illustration –



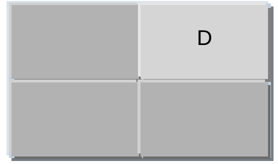
	Risk A	Risk B	Risk C	Risk D	Risk E	Risk F	Risk G	Risk H	Risk I	Risk J
Mngt. Effect.	4.5	4.5	3.6	4.5	5.2	4.6	5.3	5.4	6	6.6
Inherent Risk	8.2	7.9	6.9	6.5	7.2	6.3	7	6	5.2	6.4

Specific risk diagnostic

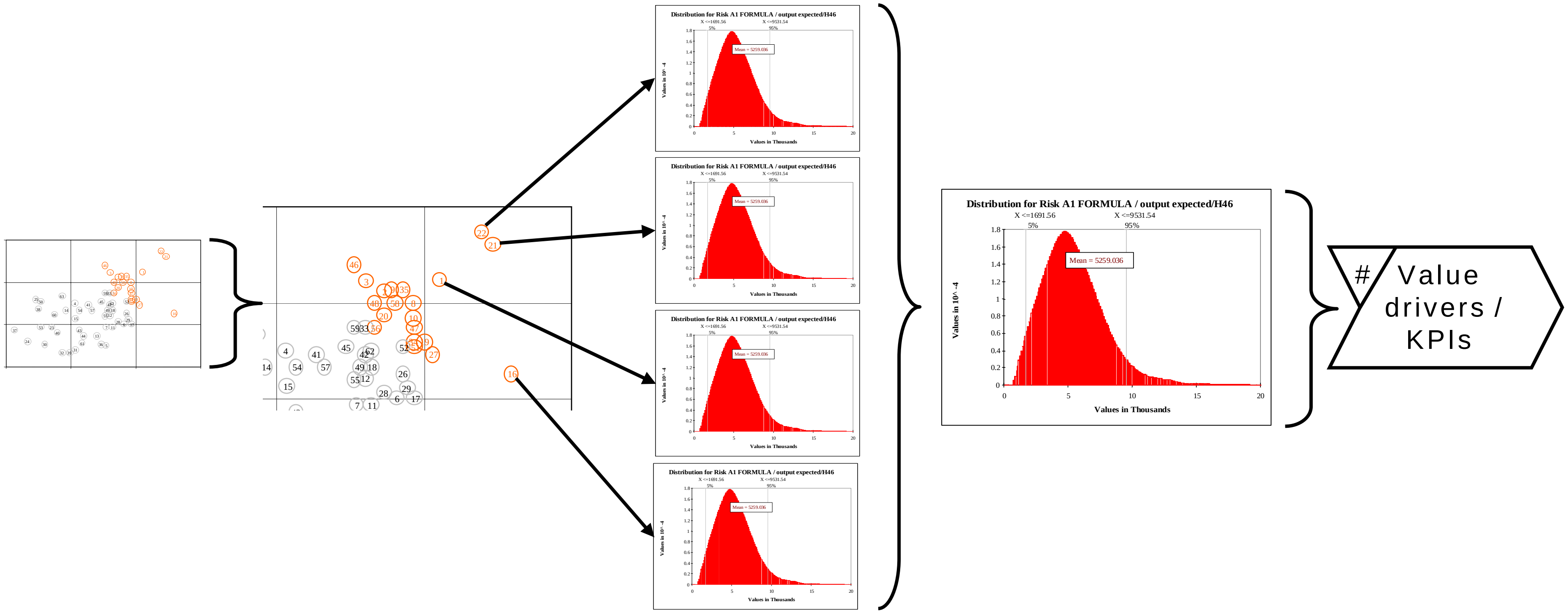


- Risk
- Risk definition
- Risk overview/scope
- Risk ownership & responsibility
- Contributing factors/root causes
- Current risk management activities & capabilities
- Risk quantification
- Risk strategy
- Strategy cost analysis/evaluation
- Risk management plans
- Metrics

Risk quantification



Risk prioritization | Critical risk selection | Individual risk modelling | Integrated risk modelling | Shareholder value link



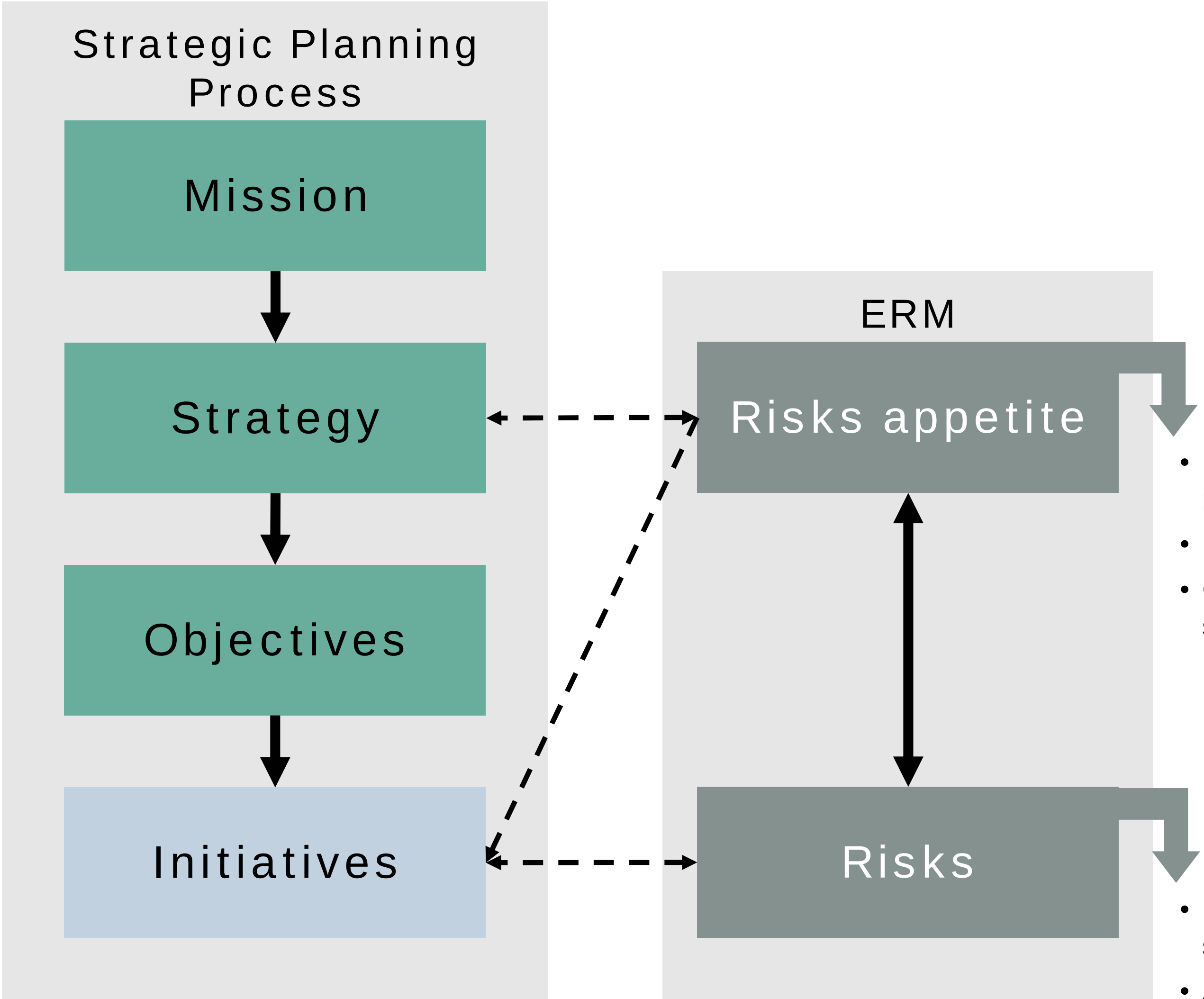
Risk appetite & strategy

	S

Risk appetite is a statement of the risks that the organization is willing to accept. It is closely linked to risk management philosophy and the organization's strategic choices:

- Management forms a risk appetite at the entity level
- The broad-based amount of risk an entity is willing to accept in pursuit of its mission (or vision)
- Risk appetite is encompassed in policy, guidelines and procedures
- Sets the boundaries for risk tolerances (the acceptable level of variation around objectives)

Strategic planning process integration



- Ensure strategies are aligned with risk appetite.
- Ensure that risks fall within appetite.
- Guide setting of risk tolerances for specific objectives and initiatives.

- Identify and prioritize risks to strategic initiatives.
- Analyze risks.
- Assign ownership of risks.
- Risk management action planning guided by risk tolerances and appetite.

Governance – organization structure

There is no ‘correct’ organization structure. The structure should be:

- Aligned with the strategies, objectives, culture and personnel
- Consistent and meet regulatory expectations

Head of ERM should be no more than two levels below the CEO:

- Position should be held by a senior executive
- Need for strong organizational respect and knowledge

Appropriate and clear reporting lines for and between:

- Board
- Executive management
- Business owners
- Risk committees / risk managers
- Audit and compliance

Governance – roles & responsibilities

G

Distinct roles and responsibilities are necessary to ensure effective ERM:

The Board of Directors

- Oversee management's design and operation of ERM and whether management has established effective ERM
- Aware of and concurring with the entity's risk appetite
- Apprised of the most significant risks and whether management is taking appropriate responses

Management

- Responsible for the design of an entity's enterprise risk management framework
- Promote the desired risk culture and frames risks in the context of strategy and activities
- Establish risk appetite, provide portfolio view of risk and enforces compliance individually and in the aggregate

CRO/risk officers

- Work with managers in establishing and maintaining effective risk management in their areas of responsibility
- Has resources to help effect ERM

Internal auditors

- Assist both management and the audit committee by examining, evaluating, reporting and recommending improvements on the adequacy and effectiveness of management's risk management processes

Governance – organizational structure

– Illustration –

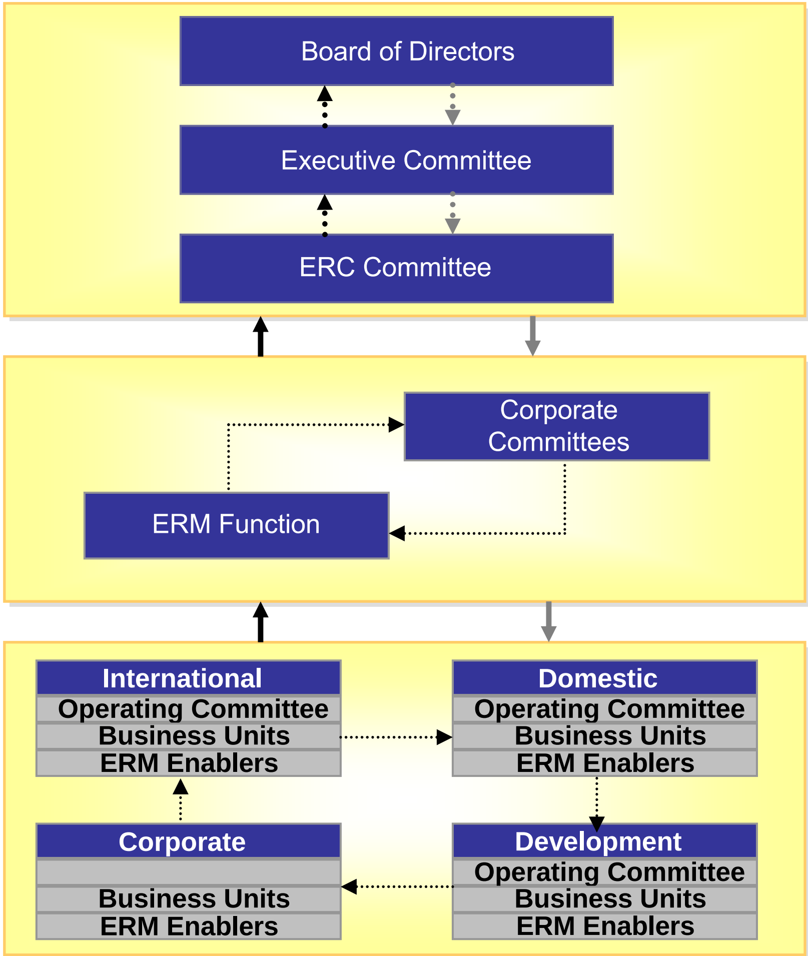
Risk Information

- Corporate Risk Data
- Corporate Issues
- Risk Tolerance Levels
- Risk Policies/Procedures
- Corporate Risk Strategies

- Consolidated Risk Data
- Integrated Reports (planning, disclosure)
- ERM Initiative Metrics

- Signal Detection
- Risks Exceeding Tolerances
- Risk Metrics
- Strategic Planning Data

Monitoring & Information Flow



Responsibilities

ERM Decisions

- Develop Risk Objectives
- Establish Risk Tolerances
- Define Risk Policies
- Approve Corporate Risk Strategies

ERM Review and Support

- Review Functional Risks
- Recommend Risk Strategies

- Monitor ERM Practices
- Review Risk Strategies
- Track and Analyze Risks
- Aggregate Risk Data

ERM Identification, Assessment and Management

- Identify critical risks
- Assess risks
- Develop risk strategies
- Monitor/manage risks

Section 4

Success drivers, pitfalls and benefits

Keys to successful ERM implementation

- Consensus vision for “future state”
- Well defined and communicated plan
- Realistic goals and timeframes
- Quick early “wins” to build organizational credibility and support
- Balancing qualitative and quantitative demands
- Allowing process to provide answers, not seeking all answers and value creation before process
- Integration with key decisioning process (i.e., Strategic Planning, M&A, Investments)

Common pitfalls

- Implementing ERM without a framework and strategic plan
- Lack of visible, active support from the CEO
- Overselling ERM value for initial risk assessment
- Risk identification confused with ERM
- Implementing ERM as a part-time job
- Treating ERM as project versus a long-term journey
- Becoming overwhelmed with initial risk assessment results
- Lack of true integration with strategic planning, budgeting/forecasting, etc.
- Failure to take risk management through full process
- Failing to realize the need for change management
- Lack of leadership and passion

ERM benefits

Shareholders/ Board

- Understand the organisation's risk appetite, acceptable earnings/cash-flow volatility, and measures required to maintain appropriate risk profile
- Ensure stronger corporate governance and full compliance based on increased transparency and disclosure
- Ensure sustainable process/framework is in place with appropriate culture
- Provide shareholders and the market with confidence that the risk profile is known and under control
- Ensure a continuous flow of risk-based information across the organization and to all key stakeholders
- Obtain a clear overview of the group's risk position at any time
- Ensure RM is a critical component of performance management

▶ Improved risk-reward ratios & reduced earnings volatility

Executive Management

- Support all strategic planning, CAPEX allocation, and new investment decisions with risk adjusted performance metrics
- Identify value eroding projects and activities where the risk-return ratio is sub-optimal
- Overview of risk portfolio across the company
- Improve risk mitigation strategies based on actual risk exposure
- Enhance communications/reporting and risk controlling, with a "risk dashboard" that determines risk exposures across business units and monitors KRIs
- Risk management /performance is incorporated in the executive competencies
- Develop a corporate "risk culture" which leads to risk-reward analysis being conducted by organisational decision-makers

▶ Enhanced decision making & improved earnings potential

Business Unit/ Functional Management

- Continuous identification, assessment, and monitoring
- Proactively define mitigation strategies for a range of potential scenarios
- Define contingency plans in case of extreme risk exposure
- Engrain an early warning system based on KRIs throughout the company
- Risk focussed goal setting with MBOs that include risk-reward targets
- Identify potential operational improvements

▶ Risk identification, assessment, and reporting

Critical success factors

- Leadership and sponsorship
- Cultural and behavioral change
- Ownership and commitment
- Disciplined, proven and flexible approach
- Time and resource dedication
- Continuous process improvement and feedback

"Organizations make money by taking risk and lose money by not effectively managing risk"