



# Linking Risk Management to Business Strategy, Processes, Operations and Reporting

Financial Management Institute of Canada

February 17<sup>th</sup>, 2010

# Agenda

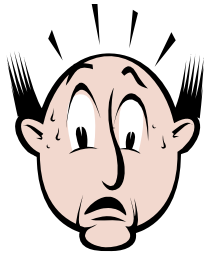
1. Leading Practice Risk Management Principles & Benefits
2. Enterprise Risk Management – Strategic Application
3. Linking Strategy, Risk Management & Performance – Examples
4. Enterprise Risk Management as a Strategic Tool - Prerequisites
5. Questions & Answers



Part 1

## Leading Practice Risk Management Principles & Benefits

# Risk as Threat but what about the Opportunities



Risk as HAZARD

*Prevent bad stuff*

- Statutory requirements
- Compliance
- Internal Controls
- Environment

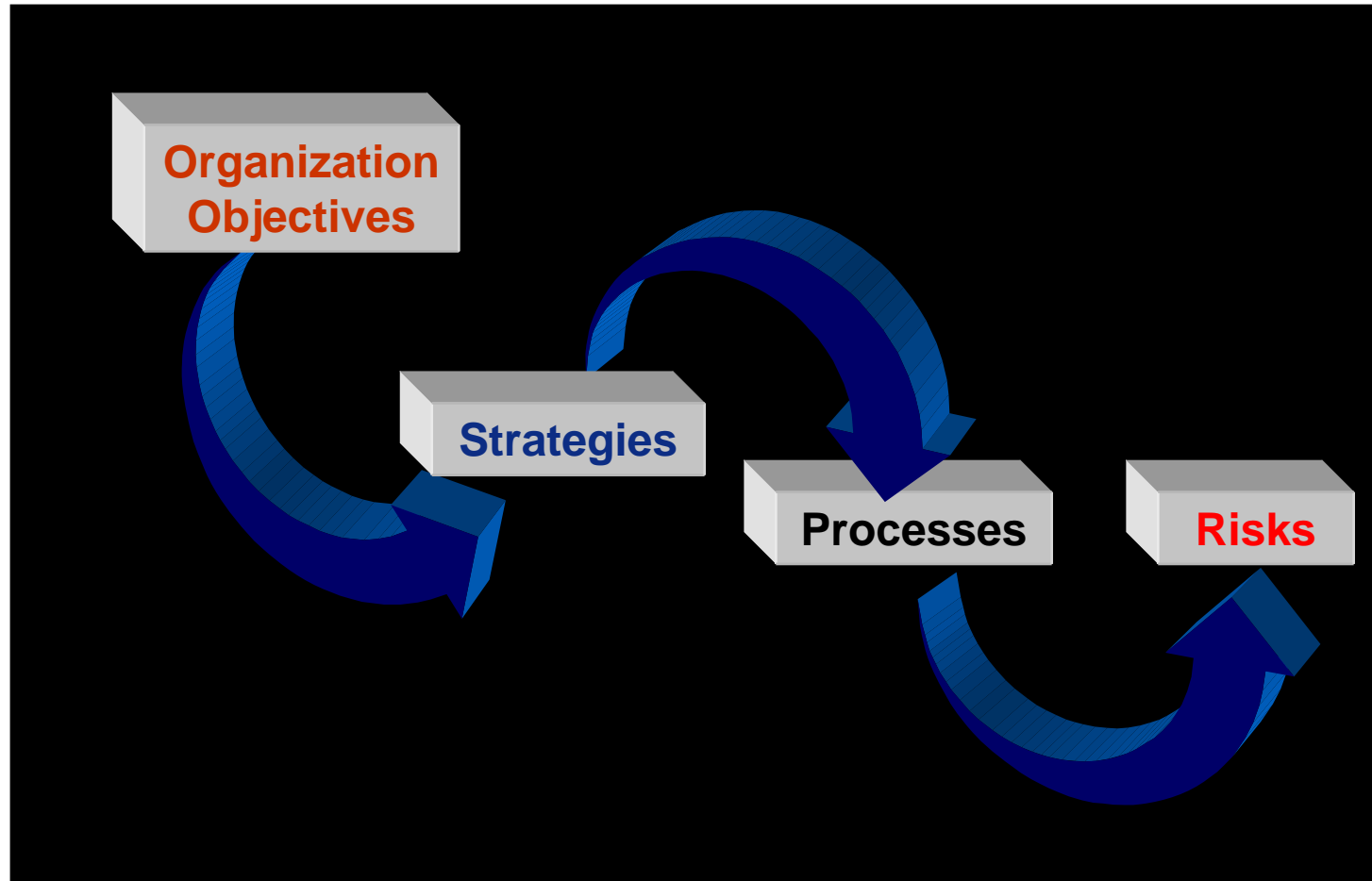


Risk as OPPORTUNITY

*Enable good stuff*

- Pursue opportunities
- New areas development
  - Invest in people
- Strategic alliances

# Know What Risks Threaten or Enhance Objectives



## Risk Management Principles – ISO 31000

### a. Risk management creates and protects value.

- Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

### b. Risk management is an integral part of all organizational processes.

- Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

### c. Risk management is part of decision making.

- Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

### d. Risk management explicitly addresses uncertainty.

- Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

Source: ISO 31000, 2009

## Risk Management Principles – ISO 31000

- e. Risk management is systematic, structured and timely.
  - A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
- f. Risk management is based on the best available information.
  - The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.
- g. Risk management is tailored.
  - Risk management is aligned with the organization's external and internal context and risk profile.
- h. Risk management takes human and cultural factors into account.
  - Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

Source: ISO 31000, 2009

## Risk Management Principles – ISO 31000

- i. Risk management is transparent and inclusive.
  - Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
- j. Risk management is dynamic, iterative and responsive to change.
  - Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.
- k. Risk management facilitates continual improvement of the organization.
  - Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization

Source: ISO 31000, 2009

# Enterprise Risk Management Benefits – A Strategic Perspective

- Enterprise Risk Management improves an organization's ability to:
  - Encourage proactive rather than reactive management
  - Establish a reliable basis for decision making and planning
  - Improve identification of opportunities and threats
  - Improve operational effectiveness and efficiency
  - Improve corporate governance
  - Improve stakeholder confidence and trust
  - Improve financial reporting
  - Improve organizational learning
  - Improve organizational resilience

Source: ISO 31000, 2009



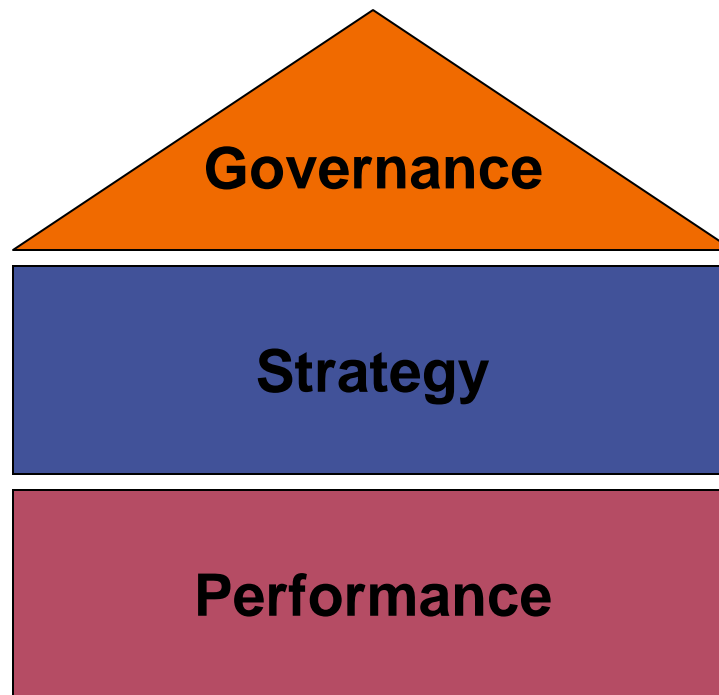
Part 2

## Enterprise Risk Management – Strategic Application

# What Should Be The Role of Enterprise Risk Management



## ERM Drivers



# Using ERM to Link Strategy, Performance and Governance



## Governance

Monitoring and reporting of key risks and actions to manage risk for Management and the Board

## Strategy

Realignment of business strategies by maneuvering through choices via analysis of key risks and potential financial, operational, compliance, etc. impacts

## Performance

Utilization of key risk indicators and insights provided by risk intelligence drives decision making and improves business performance

# Risk Management Maturity Model



**The Risk Maturity Model is based on a continuum of risk management attributes:**

**Basic – Risk Management is Compliance Focused**

The organization meets basic internal and external stakeholder risk management expectations from primarily compliance or internal control perspectives.

**Mature – Risk Management is a Management Process**

Activities and techniques are employed for enhanced stakeholder confidence that risk is being managed proactively. Integration of risk management activities is progressing.

**Advanced – Risk Management is a Strategic Tool**

Risk management is seen as a strategic tool to enhance performance and is a core value of the organization.

# Setting the Tone - Attributes of Enhanced Risk Management (Cont'd)



Enhanced Risk Management Attribute	Basic Remain in Compliance	Mature A Management Process	Advanced A Strategic Tool
<b>Governance &amp; Accountability</b>	Comprehensive, fully defined and fully accepted accountability for risks, risk controls and risk treatment tasks. The organization's governance and accountability structure and process are based on the management of risk.		
<b>Decision Making</b>	All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.		
<b>Risk Management and Optimization</b>	Risk management is viewed as central to the organization's management processes so that risks are considered in terms of effect of uncertainty on objectives. Risk are assessed and managed from both threats and opportunities perspectives. Risk management resources are aligned to the areas of highest risk or significant opportunity.		
<b>Communications and Reporting</b>	Continual communications with internal and external stakeholders including comprehensive and frequent reporting of risk management performance is part of good governance.		
<b>Performance Assessment &amp; Continuous Improvement</b>	An emphasis on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.		

# Risk Management Maturity Assessment Criteria

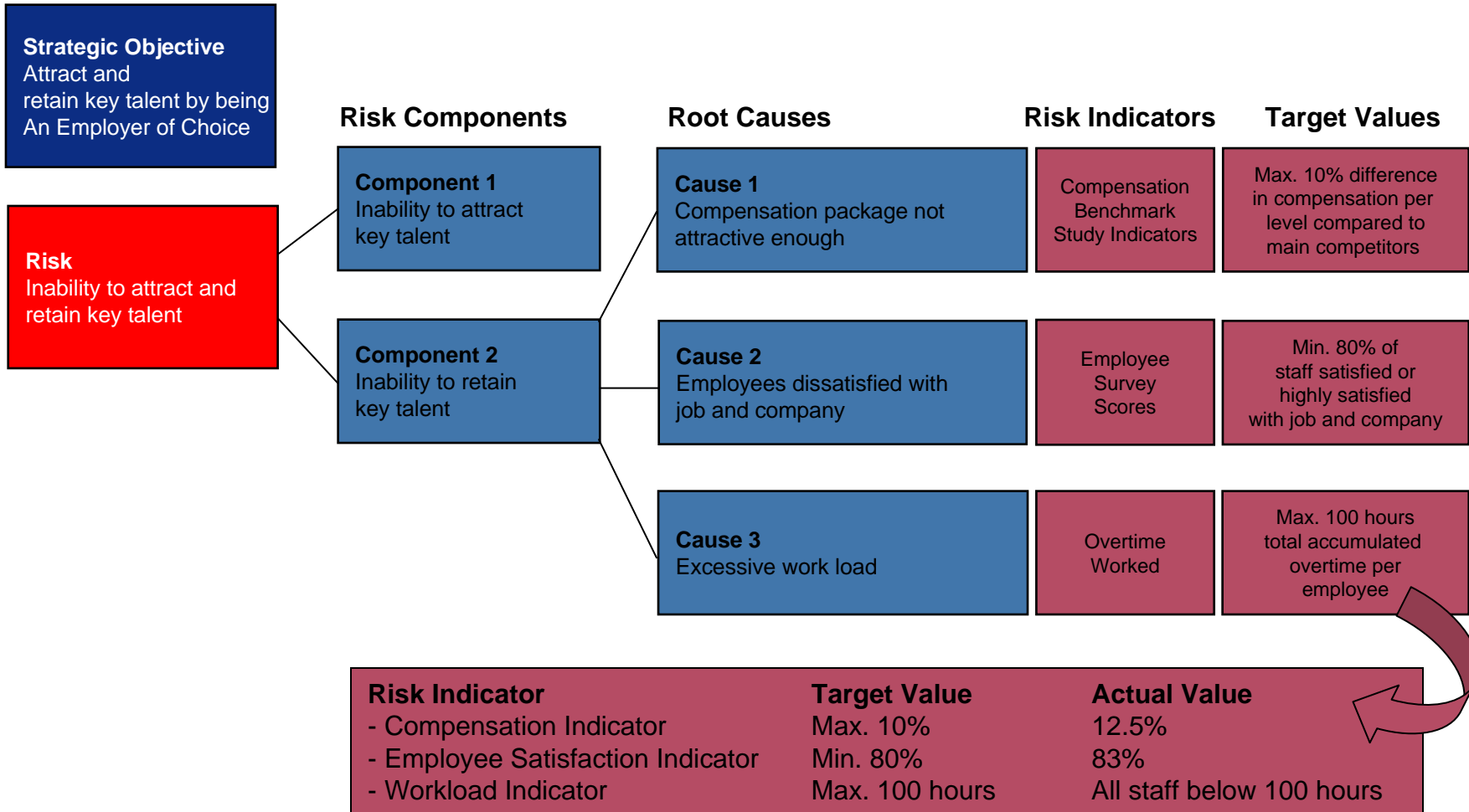
Enhanced Risk Management Attribute	Basic	Mature	Advanced
<b>Maturity Description</b>	The organization meets basic internal and external stakeholder risk management expectations from a compliance perspective	Activities and techniques are employed for enhanced stakeholder confidence that risk is being managed proactively. Integration of risk management activities	Risk management is seen as a strategic tool to enhance performance and is a core value of the organization
<b>Governance &amp; Accountability</b>	Risk management policies and procedures exist to meet compliance and internal control requirements.	An enterprise risk management framework and governance structure exists with clear accountabilities to support risk management objectives.	Risk management accountability integrated with performance management
<b>Decision Making</b>	Decision making is supported by limited or highly specialized risk analysis at the functional level	Major capital, operational, technology and change management decisions are supported by risk assessments. Risk and control activities embedded in business processes	The strategic planning process is fully supported and aligned with the risk management process. Strong evidence that both formal and informal decision making are enhanced by risk management.
<b>Risk Management and Optimization</b>	Functional risk assessments with limited analysis and interpretation from an organizational-wide perspective.	Frequent risk assessments in line with normal management analysis and reporting. Risks are assessed and managed in an integrated fashion across the organization.	The organization conducts strategic risk assessments, business unit or operational risk assessments and major investment or project risk assessments. The risk assessment cycle is aligned with the multi-year strategic planning and annual business planning cycles.
<b>Communications and Reporting</b>	Business risk reporting designed to support primarily external reporting or compliance requirements.	Extensive reporting to the board or governing body, the audit committee and key stakeholders on current risk levels and future risk issues.	Entity-wide analysis, aggregation and reporting across all risk areas. Supported by specialized risk management information systems. Alignment of all risk reporting to provide a comprehensive top-down and bottom-up view of risk.
<b>Performance Assessment &amp; Continuous Improvement</b>	Performance assessment is tied to functional or highly specialized risk management responsibilities.	Explicit requirement for risk management performance assessment aligned with the governance and accountability structure. Periodic and independent evaluation of the risk management framework, policies, procedures and personnel. A multi-year continuous improvement program is in place.	Risk-adjusted strategy performance evaluation and resource allocation



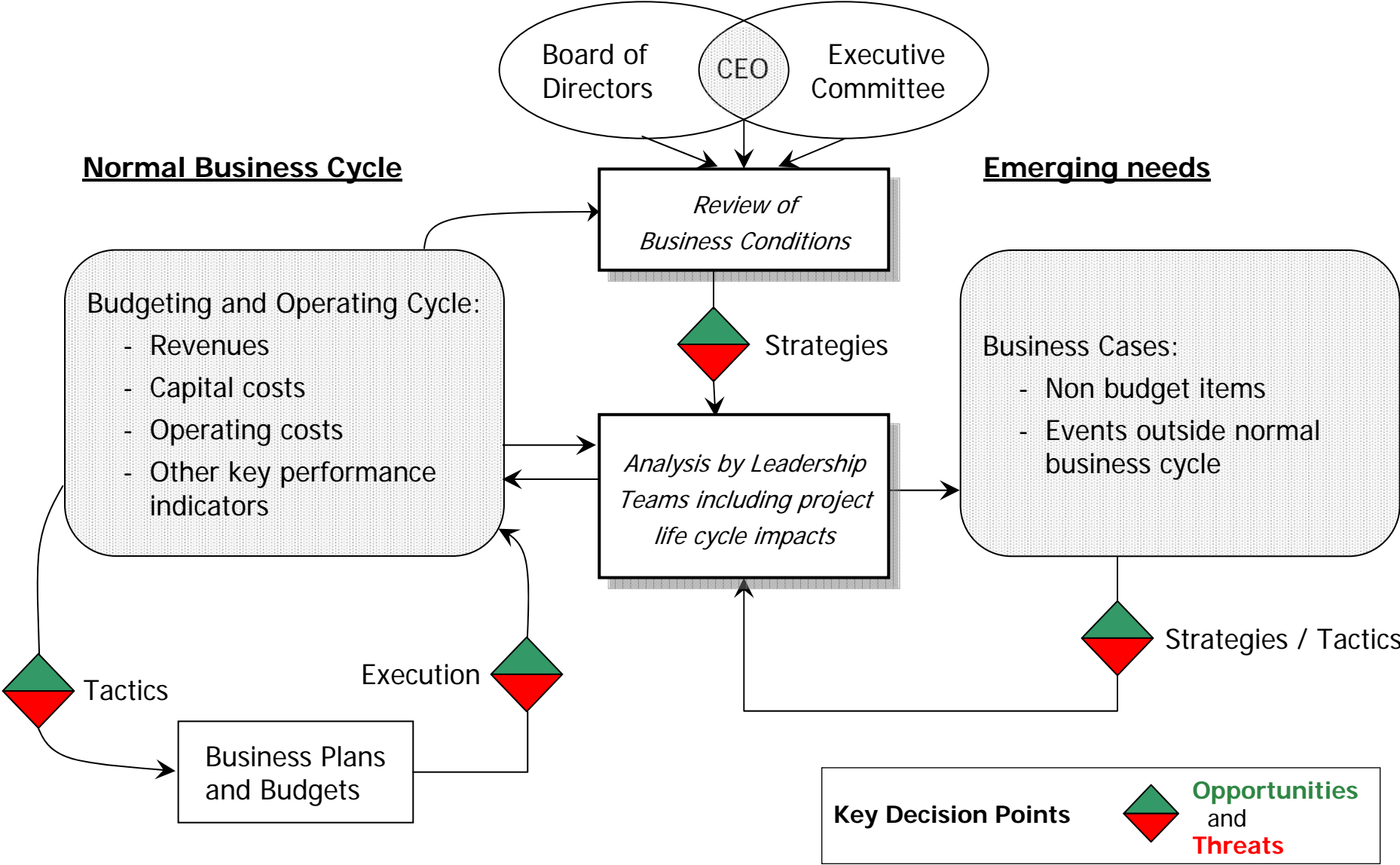
**Part 3**

**Linking Strategy, Risk Management & Performance -  
Examples**

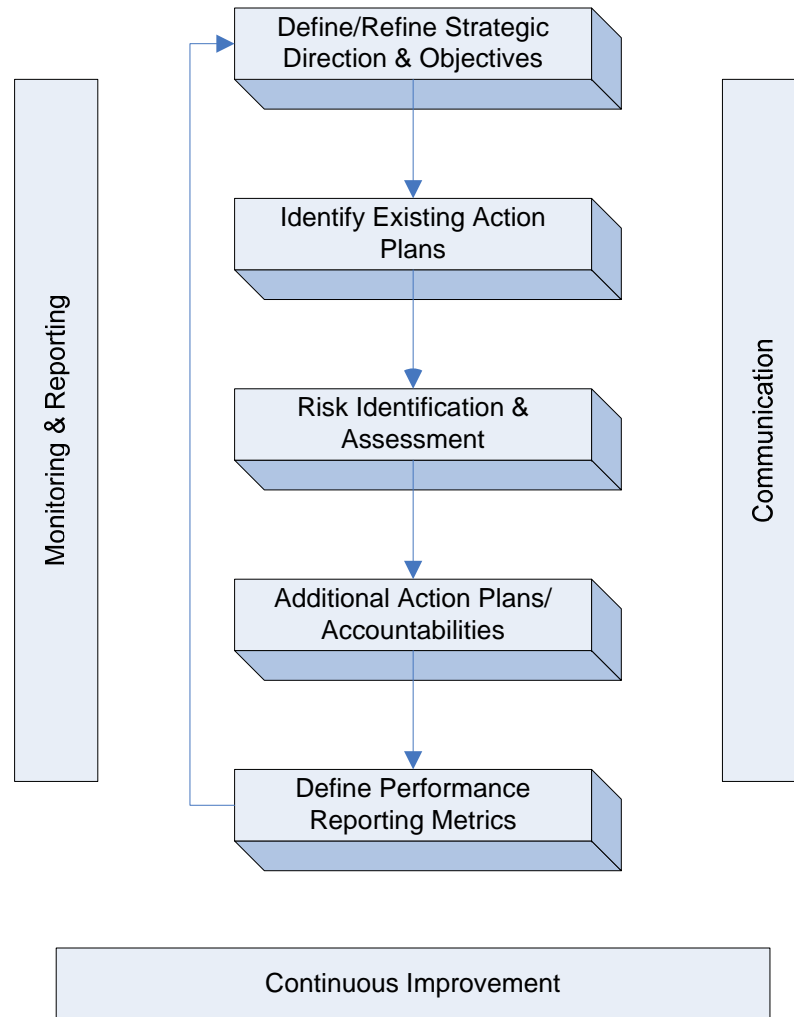
# Example 1 – HR Strategy, Risk & Performance



# Example 2 – Risk-Based Decision Making Process



# Example 3 - Integrated Planning, Risk & Performance



## Example 3 - Integrated Planning, Risk & Performance (Cont'd)



### 1. Defining Supporting Objectives for the Strategic Direction of the Organization

- Working with Senior Management in the initial identification of supporting objectives for the Strategic Plan
- Schedule and Conduct Senior Management Validation Workshops
- Board of Directors Validation Sessions

### 2. Identification of Existing Action Plans required to meet Supporting Objectives

- Work with Senior Management to identify existing action plans
- Senior Management assessment of related resource capabilities
- External/internal review of Management Plans & Assessments

### 3. Risk Identification & Assessment

- Schedule and Conduct Risk Assessment Workshops with Senior Management
- External/internal facilitators work with Senior Management to assess current action plans & identify gaps
- Identify threats and opportunities related to the supporting objectives
- Finalize risk assessment results & gap analysis

## Example 3 - Integrated Planning, Risk & Performance (Cont'd)

### 4. Develop Additional Action Plans and Accountabilities

- Senior Management develops additional actions plans to achieve objectives and manage identified risks
- Senior Management assessment of related resource capabilities and accountabilities
- Establish accountabilities and performance management requirements
- External/internal facilitators review of management plans & assessments
- Facilitated Senior Management & Board validation

### 5. Define Performance Reporting Metrics

- Metrics should link/incorporate strategic and operational objectives and related risks and should feed back into strategic planning and risk assessment processes
- Senior Management develops performance reporting metrics and related reporting processes
- Senior Management assessment of effectiveness of reporting metrics



**Part 4**

**Risk Management as a Strategic Tool – Pre-requisites**

## Risk Management as a Strategic Tool – Pre-requisites

- Risk management must be given greater authority and positioned an integral part of business planning and performance
- Senior executives must lead risk management from the top and actively participate in planning and risk analysis
- Organizations need to review the level of risk expertise in their organization, particularly at the highest levels
- Organizations should pay more attention to the data that populate risk models, and must combine this output with human judgment
- Stress testing and scenario planning can arm executives with an appropriate response to events
- Incentive systems must be constructed so that they reward long-term stability, not short-term profit
- Risk factors should be consolidated across all the organization's operations
- Organization's should ensure that they do not rely too heavily on data from external providers
- A careful balance must be struck between the centralization and decentralization of risk
- Risk management systems should be adaptive rather than static
- Embrace ISO 31000



**Part 5**  
**Questions & Answers**

## Contact Us

- *Peter Heimler*  
*Senior Principal*  
*Advisory Services*  
*KPMG LLP*  
*416-777-3509*  
[\*pheimler@kpmg.ca\*](mailto:pheimler@kpmg.ca)





**Appendix**  
**Risk Management Oversight Process**

## Risk Management Oversight Process – An Example

- Risk management performance is monitored on an ongoing basis.
- Risk related performance targets/measures are developed as part of strategic and operational planning processes and risk management response selection and implementation.
- Both inherent and residual risk exposures are monitored as is the effectiveness of risk management responses.
- Monitoring activities occur at several levels, including:
  - Unit Heads and risk process owners monitor risk exposures within operational processes on an ongoing basis;
  - The Chief Risk Officer (or equivalent) monitors the organizational risk profile and exposures on a periodic (monthly) basis and reports the status to the CEO and CFO;
  - The Audit Committee (or equivalent) monitors the organizational risk profile and exposures on a quarterly basis; and
  - The Board monitors risk profile and selected key high exposure risks on a quarterly/annual basis.

## Risk Management Oversight Process – An Example (Cont'd)

- The Audit Committee (or equivalent) is responsible for establishing policies and guidelines with respect to risk related reporting, including documentation and reporting standards and reporting frequency, subject to the following requirements:
  - Risk Process Owners must provide unit level risk reporting to the Chief Risk Officer (or equivalent) and Unit Head on at least a monthly or quarterly basis;
  - Chief Risk Officer must provide quarterly reporting to the Audit Committee (or equivalent) and the Board; and
  - The Audit Committee (or equivalent) must provide annual reporting to the Board including any related assurances requested by the Board.