Applying COSO's

Enterprise Risk Management — Integrated Framework

September 29, 2004

The Institute of Internal Auditors

Today’s organizations are concerned about:

- Risk Management
- Governance
- Control
- Assurance (and Consulting)

ERM Defined:

"… 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."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

Why ERM Is Important

Underlying principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

Why ERM Is Important

ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

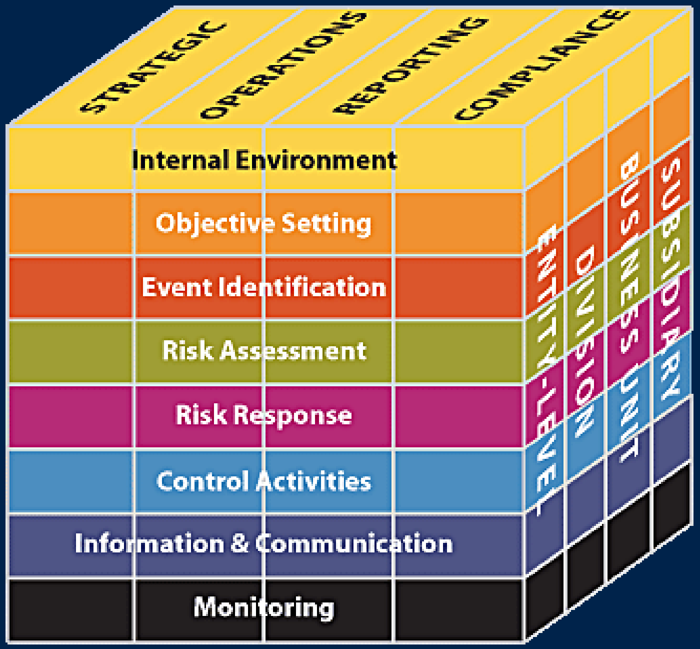
Enterprise Risk Management — Integrated Framework

This COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

The ERM Framework

Entity objectives can be viewed in the context of four categories:

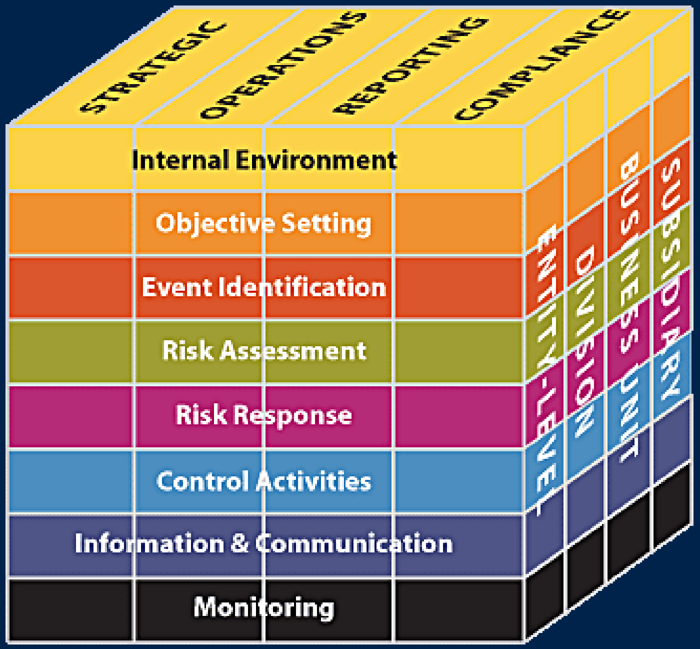
- Strategic
- Operations
- Reporting
- Compliance



The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes



The ERM Framework

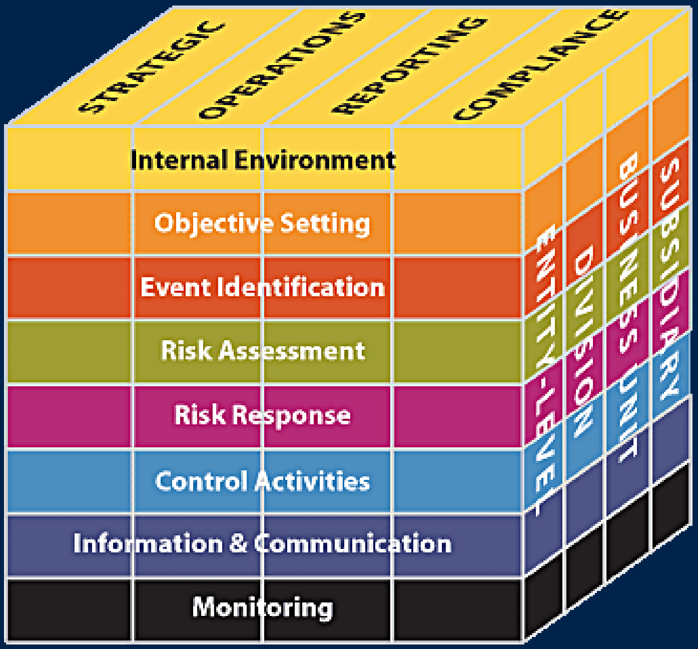
Enterprise risk management requires an entity to take a *portfolio view* of risk.

The ERM Framework

- Management considers how individual risks interrelate.
- Management develops a portfolio view from two perspectives:
  - Business unit level
  - Entity level

The ERM Framework

The eight components of the framework are interrelated …



Internal Environment

- Establishes a philosophy regarding risk management. It recognizes that unexpected as well as expected events may occur.
- Establishes the entity’s risk culture.
- Considers all other aspects of how the organization’s actions may affect its risk culture.

Objective Setting

- Is applied when management considers risks strategy in the setting of objectives.

- Forms the risk appetite of the entity — a high-level view of how much risk management and the board are willing to accept.

- Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.

Event Identification

- Differentiates risks and opportunities.
- Events that may have a negative impact represent risks.
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting.

Event Identification

- Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.

- Addresses how internal and external factors combine and interact to influence the risk profile.

Risk Assessment

- Allows an entity to understand the extent to which potential events might impact objectives.
- Assesses risks from two perspectives:
  - Likelihood
  - Impact
- Is used to assess risks and is normally also used to measure the related objectives.

Risk Assessment

- Employs a combination of both qualitative and quantitative risk assessment methodologies.
- Relates time horizons to objective horizons.
- Assesses risk on both an inherent and a residual basis.

Risk Response

- Identifies and evaluates possible responses to risk.

- Evaluates options in relation to entity’s risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.

- Selects and executes response based on evaluation of the portfolio of risks and responses.

Control Activities

- Policies and procedures that help ensure that the risk responses, as well as other entity directives, are carried out.
- Occur throughout the organization, at all levels and in all functions.
- Include application and general information technology controls.

Information & Communication

- Management identifies, captures, and communicates pertinent information in a form and timeframe that enables people to carry out their responsibilities.
- Communication occurs in a broader sense, flowing down, across, and up the organization.

Monitoring

Effectiveness of the other ERM components is monitored through:

- Ongoing monitoring activities.
- Separate evaluations.
- A combination of the two.

Internal Control

A strong system of internal control is essential to effective enterprise risk management.

Relationship to *Internal Control — Integrated Framework*

- Expands and elaborates on elements of internal control as set out in COSO's "control framework."
- Includes objective setting as a separate component. Objectives are a "prerequisite" for internal control.
- Expands the control framework's "Financial Reporting" and "Risk Assessment."

ERM Roles & Responsibilities

- Management
- The board of directors
- Risk officers
- Internal auditors

Internal Auditors

- Play an important role in monitoring ERM, but do NOT have primary responsibility for its implementation or maintenance.

- Assist management and the board or audit committee in the process by:
  - Monitoring - Evaluating
  - Examining - Reporting
  - Recommending improvements

Internal Auditors

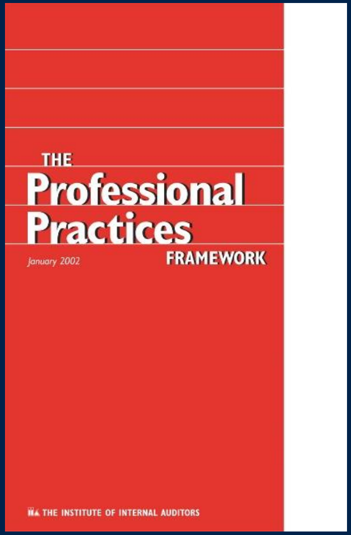
Visit the guidance section of The IIA’s Web site for The IIA’s position paper, “Role of Internal Auditing’s in Enterprise Risk Management.”

Standards

- **2010.A1** – The internal audit activity’s plan of engagements should be based on a risk assessment, undertaken at least annually.

- **2120.A1** – Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization’s governance, operations, and information systems.

- **2210.A1** – When planning the engagement, the internal auditor should identify and assess risks relevant to the activity under review. The engagement objectives should reflect the results of the risk assessment.



Key Implementation Factors

1. Organizational design of business
2. Establishing an ERM organization
3. Performing risk assessments
4. Determining overall risk appetite
5. Identifying risk responses
6. Communication of risk results
7. Monitoring
8. Oversight & periodic review by management

Organizational Design

- Strategies of the business
- Key business objectives
- Related objectives that cascade down the organization from key business objectives
- Assignment of responsibilities to organizational elements and leaders (linkage)

Example: Linkage

- **Mission** – To provide high-quality accessible and affordable community-based health care

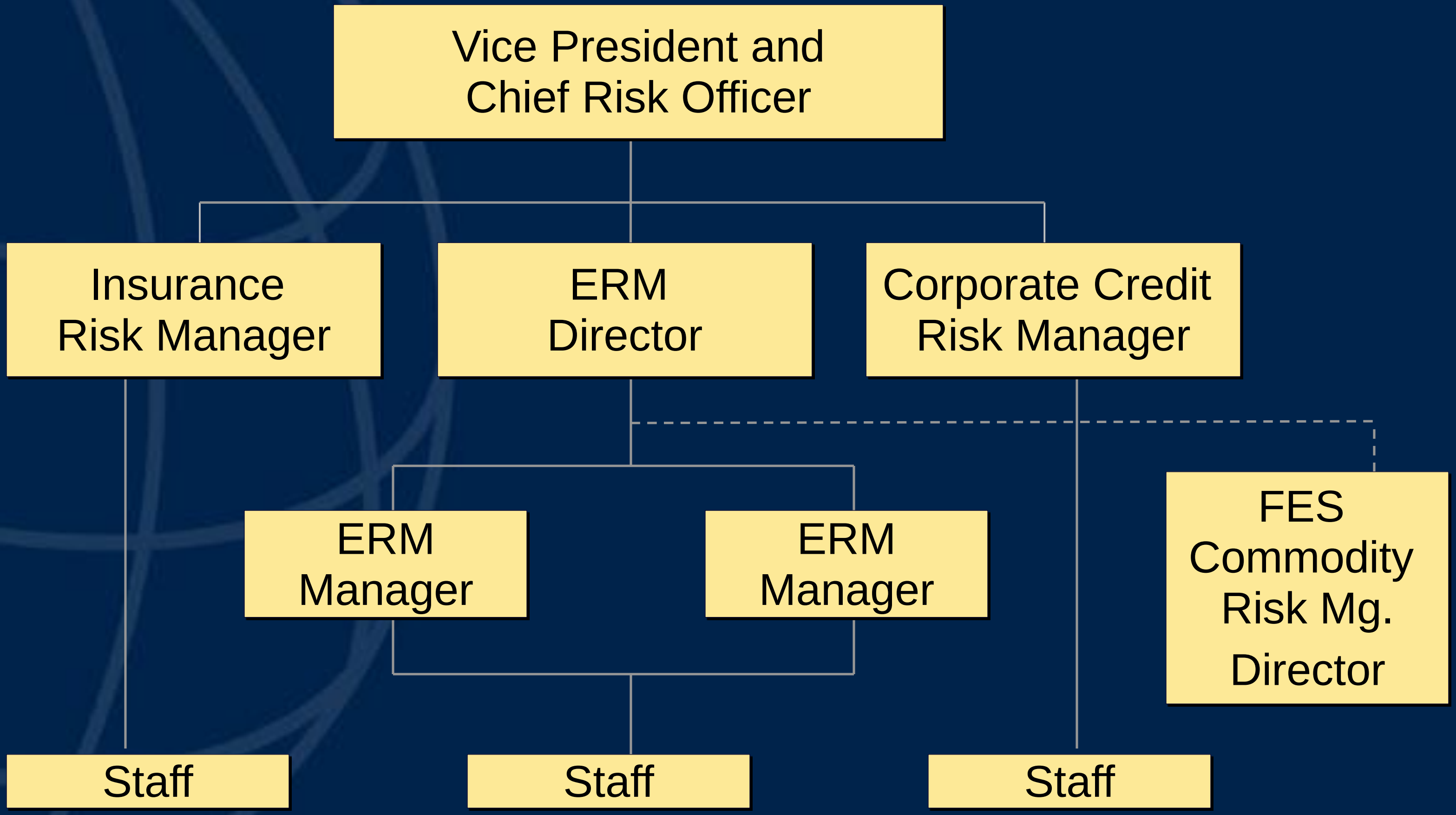
- **Strategic Objective** – To be the first or second largest, full-service health care provider in mid-size metropolitan markets

- **Related Objective** – To initiate dialogue with leadership of 10 top under-performing hospitals and negotiate agreements with two this year

Establish ERM

- Determine a risk philosophy
- Survey risk culture
- Consider organizational integrity and ethical values
- Decide roles and responsibilities

Example: ERM Organization



Vice President and Chief Risk Officer

Insurance Risk Manager

ERM Director

Corporate Credit Risk Manager

ERM Manager

ERM Manager

FES Commodity Risk Mg. Director

Staff

Staff

Staff

Assess Risk

Risk assessment is the identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed.

Example: Risk Model

Environmental Risks

- Capital Availability
- Regulatory, Political, and Legal
- Financial Markets and Shareholder Relations

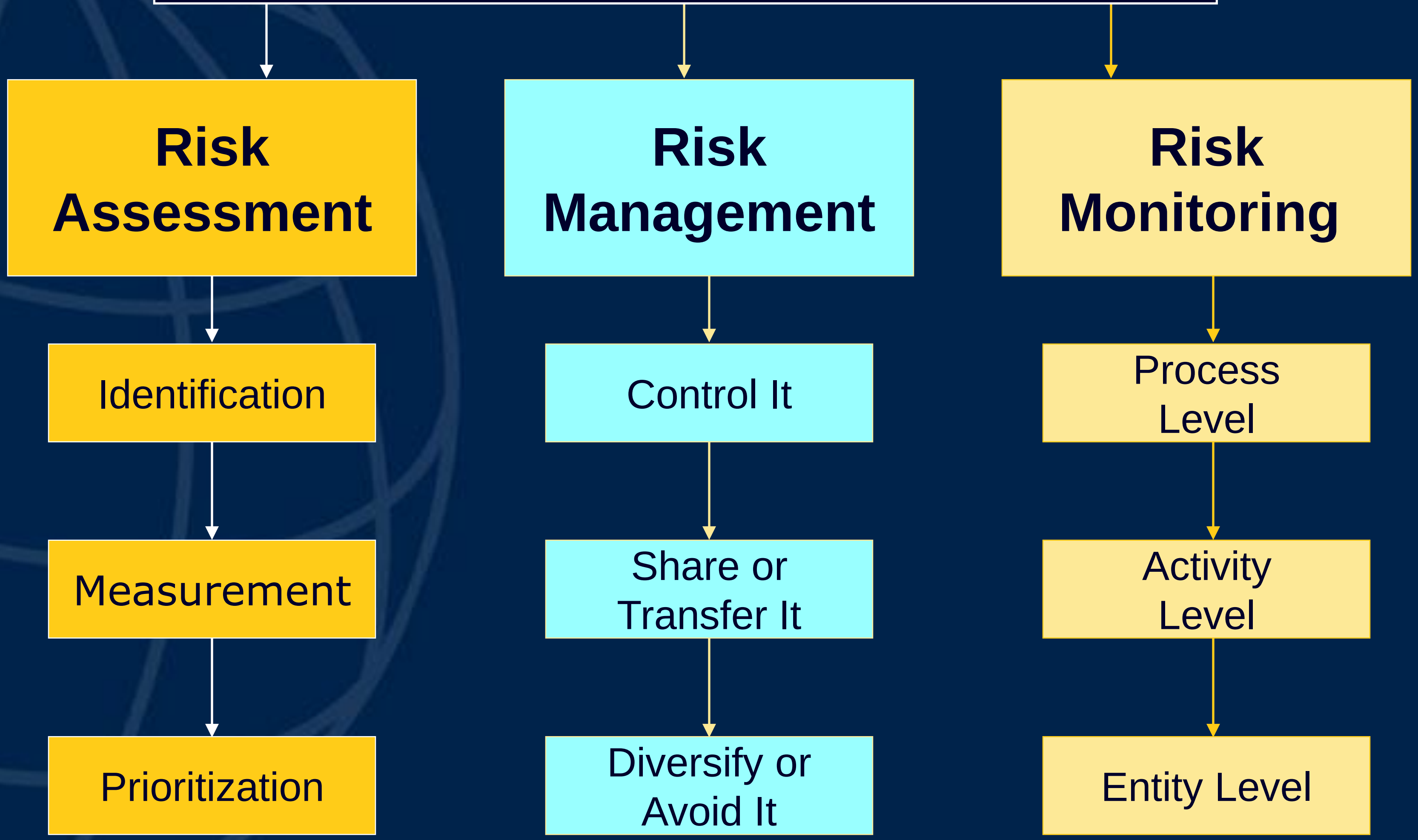
Process Risks

- Operations Risk
- Empowerment Risk
- Information Processing / Technology Risk
- Integrity Risk
- Financial Risk

Information for Decision Making

- Operational Risk
- Financial Risk
- Strategic Risk

Risk Analysis



Risk Assessment

Identification

Measurement

Prioritization

Risk Management

Control It

Share or Transfer It

Diversify or Avoid It

Risk Monitoring

Process Level

Activity Level

Entity Level

Source: Business Risk Assessment. 1998 – The Institute of Internal Auditors

DETERMINE RISK APPETITE

- Risk appetite is the amount of risk — on a broad level — an entity is willing to accept in pursuit of value.

- Use quantitative or qualitative terms (e.g. earnings at risk vs. reputation risk), and consider risk tolerance (range of acceptable variation).

DETERMINE RISK APPETITE

Key questions:

- What risks will the organization not accept?
  (e.g. environmental or quality compromises)
- What risks will the organization take on new initiatives?
  (e.g. new product lines)
- What risks will the organization accept for competing objectives?
  (e.g. gross profit vs. market share?)

IDENTIFY RISK RESPONSES

- Quantification of risk exposure

- Options available:
  - Accept = monitor
  - Avoid = eliminate *(get out of situation)*
  - Reduce = institute controls
  - Share = partner with someone *(e.g. insurance)*

- Residual risk *(unmitigated risk – e.g. shrinkage)*

Impact vs. Probability

High IMPACT	*Medium Risk* ***Share***	*High Risk* ***Mitigate & Control***
	Low Risk ***Accept***	*Medium Risk* ***Control***
Low	**PROBABILITY**	High

Example: Call Center Risk Assessment

High

IMPACT

Low

Medium Risk

- Loss of phones
- Loss of computers

High Risk

- Credit risk
- Customer has a long wait
- Customer can’t get through
- Customer can’t get answers

Low Risk

- Fraud
- Lost transactions
- Employee morale

Medium Risk

- Entry errors
- Equipment obsolescence
- Repeat calls for same problem

PROBABILITY High

Example: Accounts Payable Process

Control Objective	Risk	Control Activity
Completeness	Material transaction not recorded	Accrual of open liabilities Invoices accrued after closing

Issue: Invoices go to field and AP is not aware of liability.

Communicate Results

- Dashboard of risks and related responses (visual status of where key risks stand relative to risk tolerances)
- Flowcharts of processes with key controls noted
- Narratives of business objectives linked to operational risks and responses
- List of key risks to be monitored or used
- Management understanding of key business risk responsibility and communication of assignments

Monitor

- Collect and display information
- Perform analysis
  - Risks are being properly addressed
  - Controls are working to mitigate risks

Management Oversight & Periodic Review

- Accountability for risks
- Ownership
- Updates
  - Changes in business objectives
  - Changes in systems
  - Changes in processes

Internal auditors can add value by:

- Reviewing critical control systems and risk management processes.

- Performing an effectiveness review of management's risk assessments and the internal controls.

- Providing advice in the design and improvement of control systems and risk mitigation strategies.

Internal auditors can add value by:

- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal auditing's resources are directed at those areas most important to the organization.
- Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk treatment strategies.

Internal auditors can add value by:

- Facilitating ERM workshops.
- Defining risk tolerances where none have been identified, based on internal auditing's experience, judgment, and consultation with management.

For more information

On COSO's

Enterprise Risk Management — Integrated Framework,

visit

www.coso.org

or

www.theiia.org

Applying COSO's

Enterprise Risk Management — Integrated Framework

This presentation
was produced
by

The Institute of
Internal Auditors