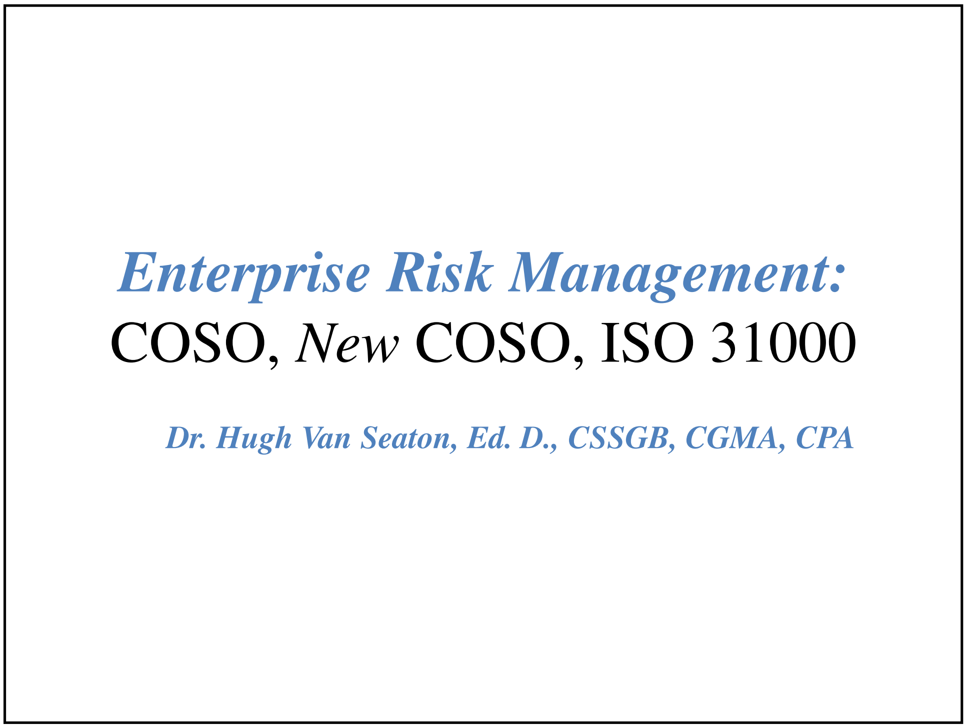
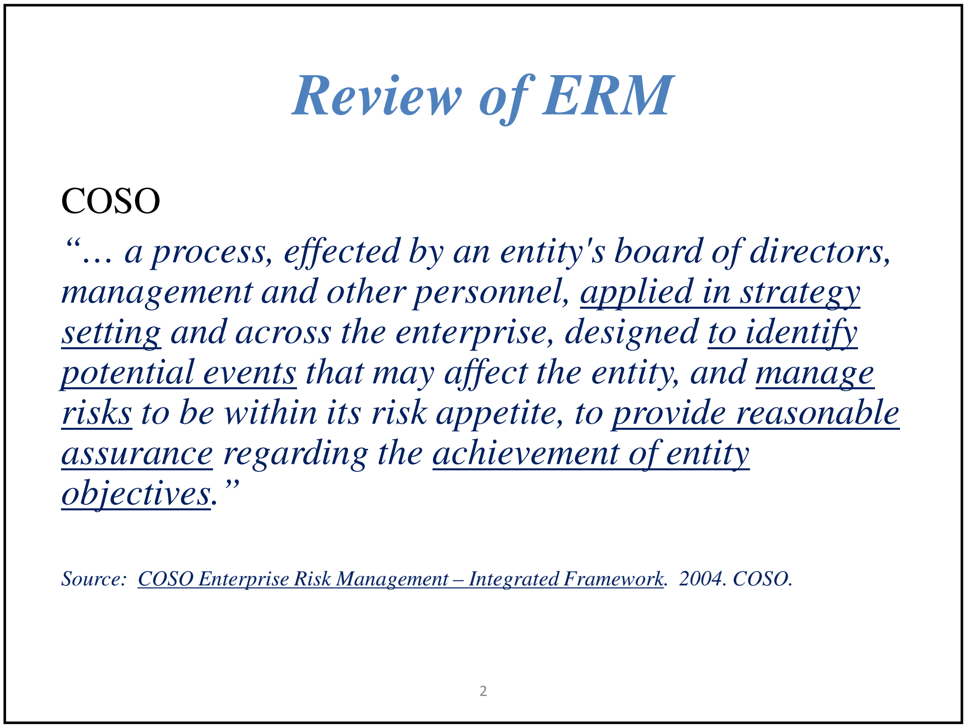


Enterprise Risk Management:

COSO, *New* COSO, ISO 31000

Dr. Hugh Van Seaton, Ed. D., CSSGB, CGMA, CPA



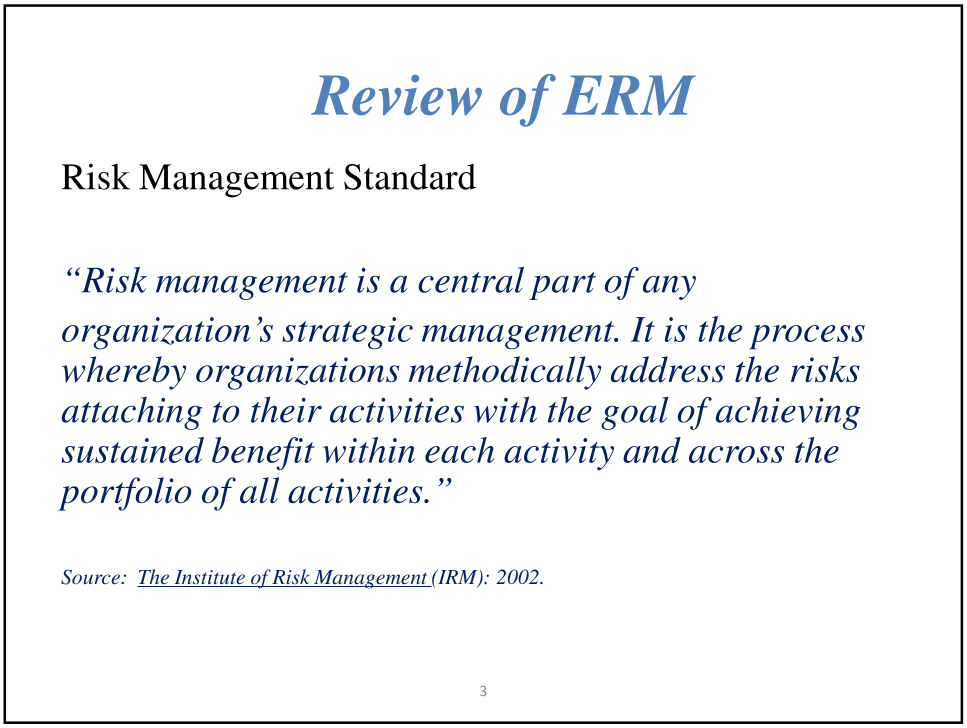
Review of ERM

COSO

"… 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.

2

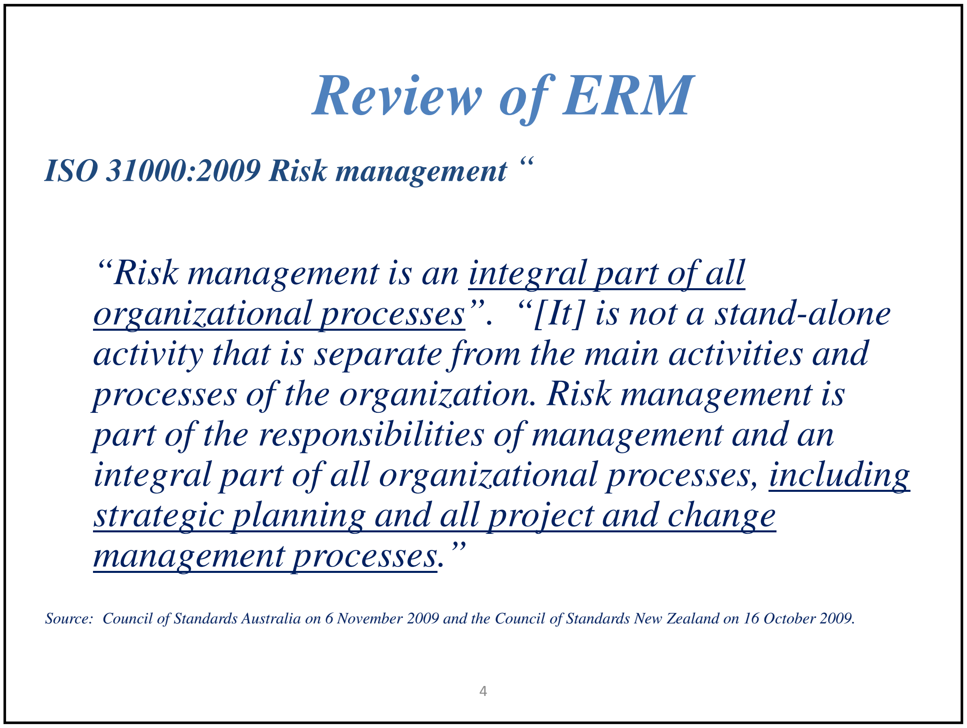


Review of ERM

Risk Management Standard

"Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities."

Source: The Institute of Risk Management (IRM): 2002.

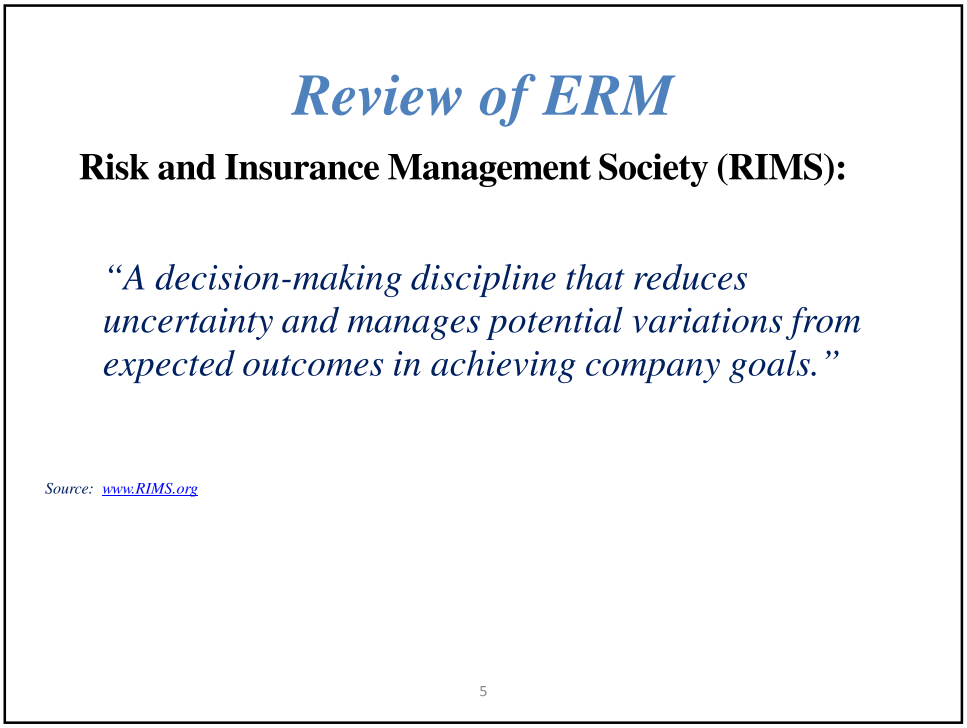


Review of ERM

ISO 31000:2009 Risk management "

"Risk management is an integral part of all organizational processes". "[It] 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."

Source: Council of Standards Australia on 6 November 2009 and the Council of Standards New Zealand on 16 October 2009.

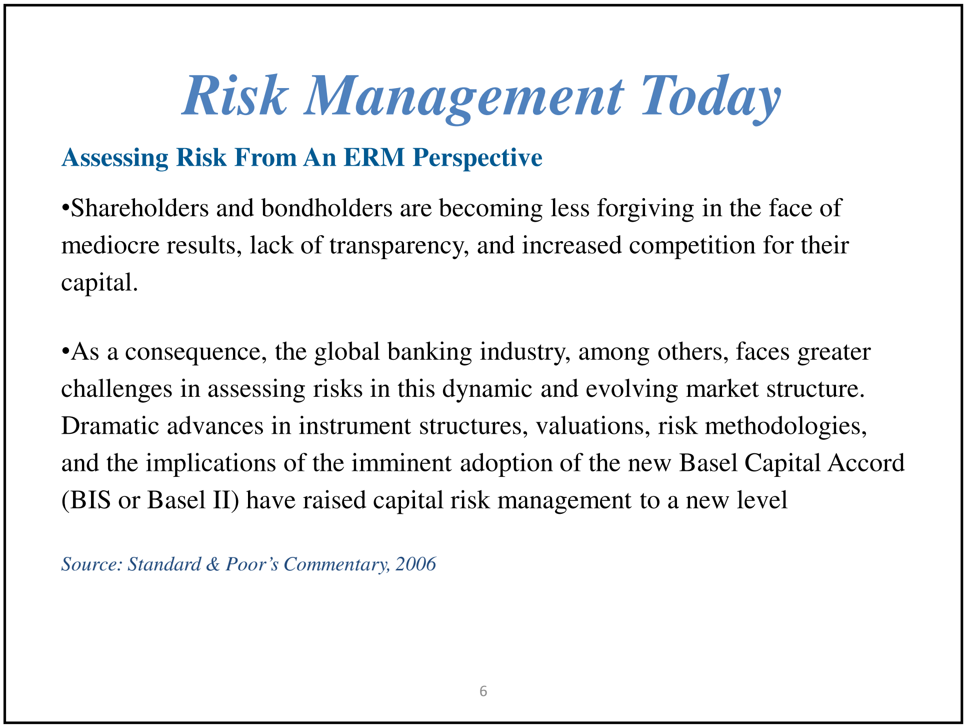


Review of ERM

Risk and Insurance Management Society (RIMS):

"A decision-making discipline that reduces uncertainty and manages potential variations from expected outcomes in achieving company goals."

Source: www.RIMS.org



Risk Management Today

Assessing Risk From An ERM Perspective

•Shareholders and bondholders are becoming less forgiving in the face of mediocre results, lack of transparency, and increased competition for their capital.

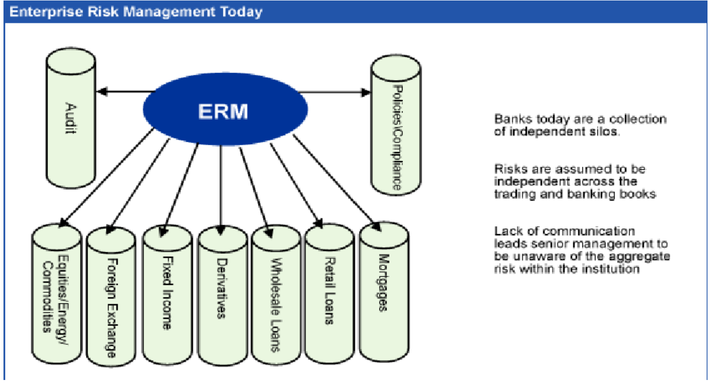
•As a consequence, the global banking industry, among others, faces greater challenges in assessing risks in this dynamic and evolving market structure. Dramatic advances in instrument structures, valuations, risk methodologies, and the implications of the imminent adoption of the new Basel Capital Accord (BIS or Basel II) have raised capital risk management to a new level

Source: Standard & Poor's Commentary, 2006

Risk Management Today

Assessing Risk From An ERM Perspective

The silo-based approach of the risk management function today



Banks today are a collection of independent silos.

Risks are assumed to be independent across the trading and banking books

Lack of communication leads senior management to be unaware of the aggregate risk within the institution

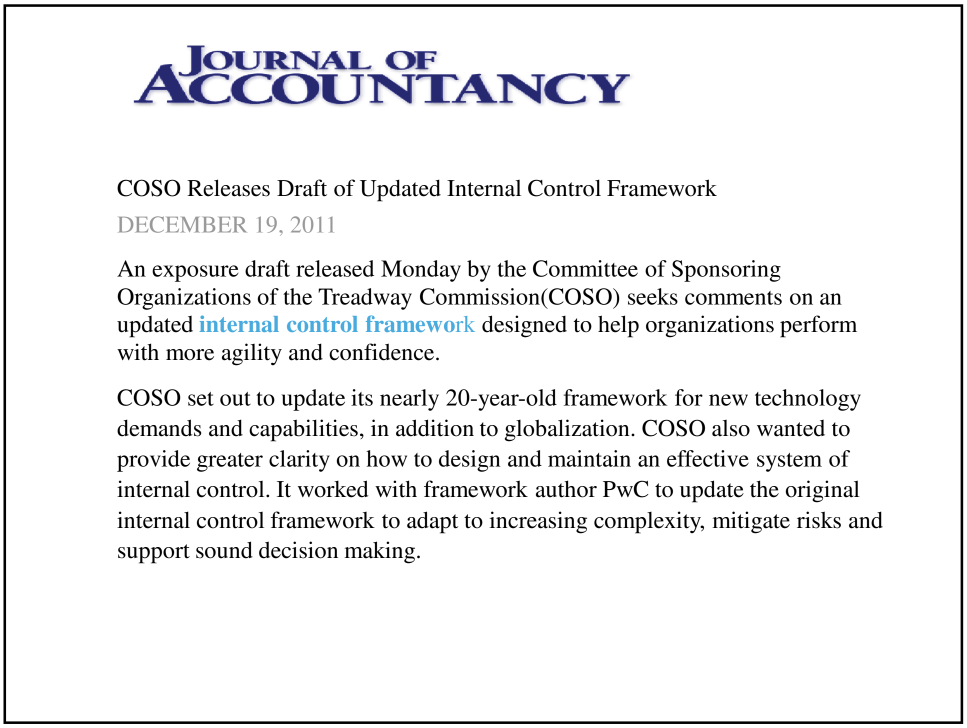
Source: Standard & Poor's Commentary, 2006

Risk Management Fundamentals

The COSO ERM framework is

- a three-dimensional model for understanding enterprise risk, applicable to all industries and encompassing all types of risks.
- The three dimensions are:
  1. The strategic, operational, reporting, and compliance objectives of the enterprise, which are to be evaluated for risk management considerations.
  2. The risk components of the model: the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.
  3. The organizational levels of the business entity, from top to bottom: entity, business unit, subsidiary, and division..

Source: http://www.coso.org/



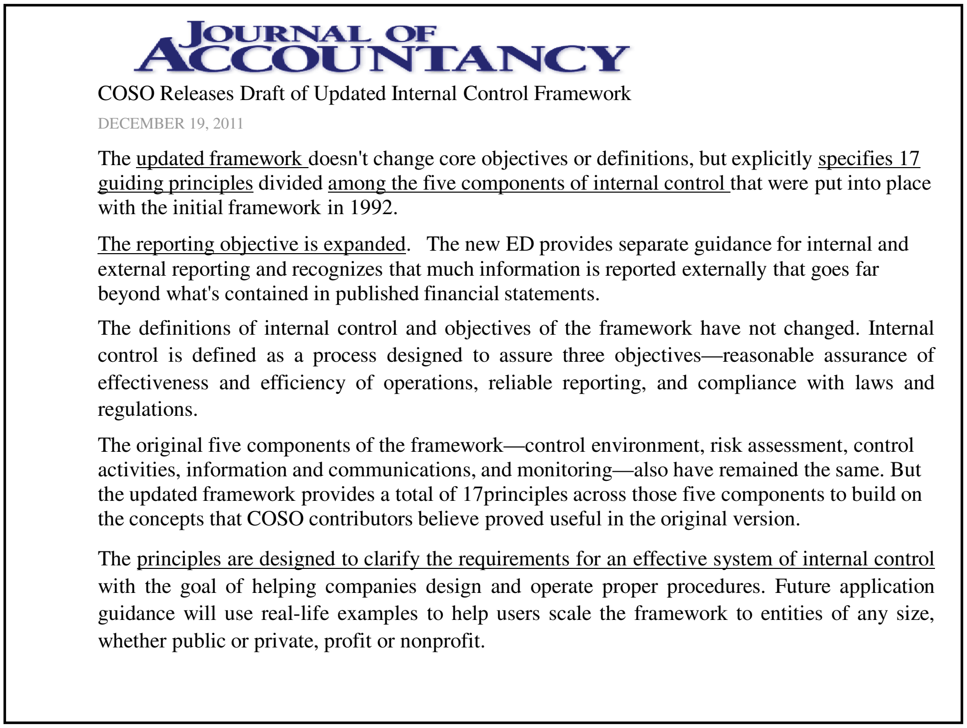
JOURNAL OF ACCOUNTANCY

COSO Releases Draft of Updated Internal Control Framework

DECEMBER 19, 2011

An exposure draft released Monday by the Committee of Sponsoring Organizations of the Treadway Commission(COSO) seeks comments on an updated **internal control framework** designed to help organizations perform with more agility and confidence.

COSO set out to update its nearly 20-year-old framework for new technology demands and capabilities, in addition to globalization. COSO also wanted to provide greater clarity on how to design and maintain an effective system of internal control. It worked with framework author PwC to update the original internal control framework to adapt to increasing complexity, mitigate risks and support sound decision making.



JOURNAL OF ACCOUNTANCY

COSO Releases Draft of Updated Internal Control Framework

DECEMBER 19, 2011

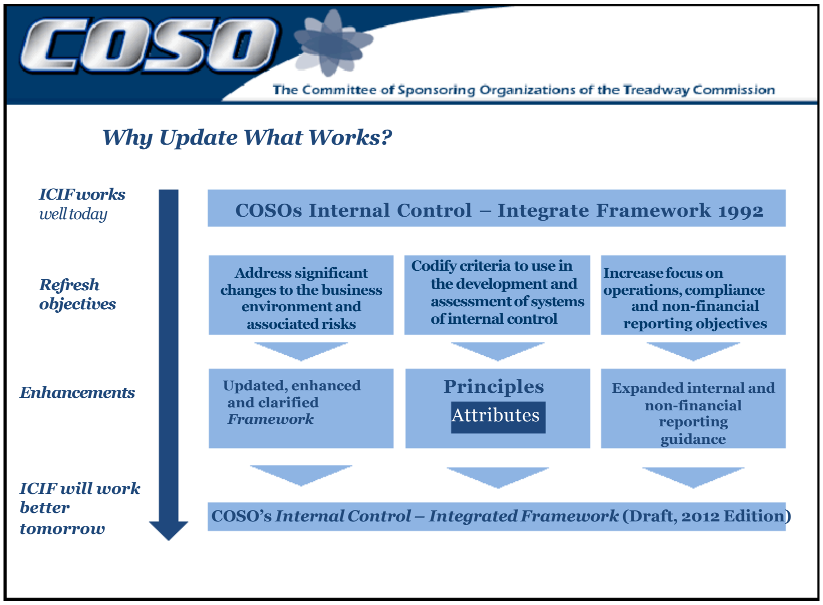
The updated framework doesn't change core objectives or definitions, but explicitly specifies 17 guiding principles divided among the five components of internal control that were put into place with the initial framework in 1992.

The reporting objective is expanded. The new ED provides separate guidance for internal and external reporting and recognizes that much information is reported externally that goes far beyond what's contained in published financial statements.

The definitions of internal control and objectives of the framework have not changed. Internal control is defined as a process designed to assure three objectives—reasonable assurance of effectiveness and efficiency of operations, reliable reporting, and compliance with laws and regulations.

The original five components of the framework—control environment, risk assessment, control activities, information and communications, and monitoring—also have remained the same. But the updated framework provides a total of 17principles across those five components to build on the concepts that COSO contributors believe proved useful in the original version.

The principles are designed to clarify the requirements for an effective system of internal control with the goal of helping companies design and operate proper procedures. Future application guidance will use real-life examples to help users scale the framework to entities of any size, whether public or private, profit or nonprofit.



COSO The Committee of Sponsoring Organizations of the Treadway Commission

Why Update What Works?

ICIF works *well today*

COSOs Internal Control – Integrate Framework 1992

Refresh objectives

Address significant changes to the business environment and associated risks

Codify criteria to use in the development and assessment of systems of internal control

Increase focus on operations, compliance and non-financial reporting objectives

Enhancements

Updated, enhanced and clarified *Framework*

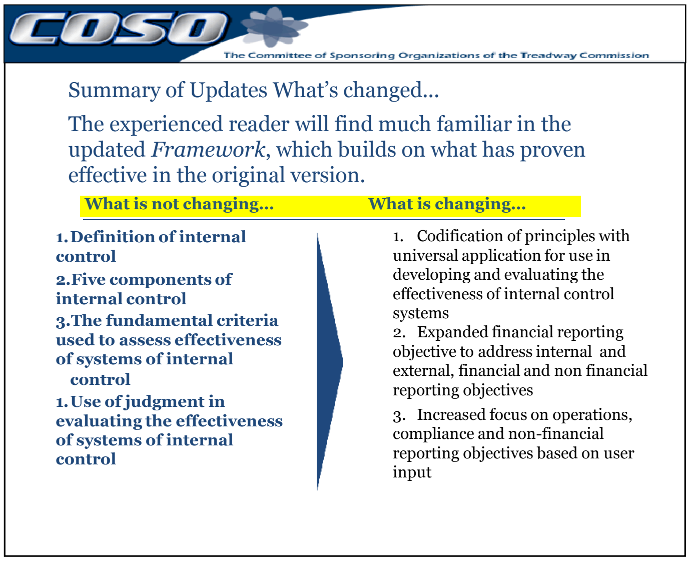
Principles

Attributes

Expanded internal and non-financial reporting guidance

ICIF will work better tomorrow

COSO's *Internal Control – Integrated Framework* (Draft, 2012 Edition)



COSO The Committee of Sponsoring Organizations of the Treadway Commission

Summary of Updates What's changed…

The experienced reader will find much familiar in the updated *Framework*, which builds on what has proven effective in the original version.

What is not changing… **What is changing…**

1. Definition of internal control

2. Five components of internal control

3. The fundamental criteria used to assess effectiveness of systems of internal control

1. Use of judgment in evaluating the effectiveness of systems of internal control

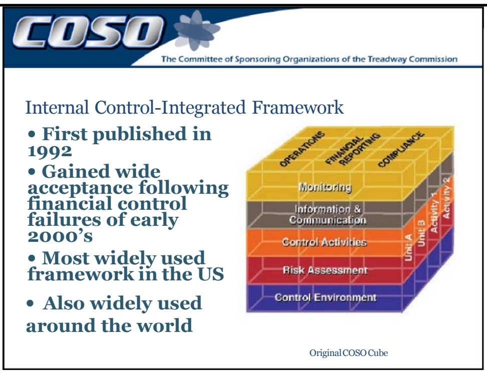
1. Codification of principles with universal application for use in developing and evaluating the effectiveness of internal control systems

2. Expanded financial reporting objective to address internal and external, financial and non financial reporting objectives

3. Increased focus on operations, compliance and non-financial reporting objectives based on user input

The *Framework's* important <u>enhancements</u> include the <u>codification of internal control concepts into principles and attributes</u>. These principles and attributes provide clarity in the design and development of systems of internal control., and can also be used to support the assessment of the effectiveness of internal controls. Other updates and enhancements to the *Framework* help the user address changes in business and operating environments, including:

- **Expectations for *governance oversight*.**
- ***Globalization* of markets and operations.**
- **Changes in business models.**
- **Demands and complexities in laws, rules, regulations, and standards.**
- **Expectations for competencies and accountabilities.**
- **Use of, and reliance on, evolving technologies.**
- **Expectations relating to preventing and detecting corruption.**



COSO

The Committee of Sponsoring Organizations of the Treadway Commission

Internal Control-Integrated Framework

- **First published in 1992**
- **Gained wide acceptance following financial control failures of early 2000's**
- **Most widely used framework in the US**
- **Also widely used around the world**

Original COSO Cube

Five components of the COSO Internal Control framework: *Control Environment*

This is the foundation for all other components of internal control, providing discipline, process and structure as established by the board and senior management. There are *five principles* relating to control environment:

1.Commitment to integrity and ethics.

2.Oversight for internal control by the board of directors, independent of management.

3.Structures, reporting lines and appropriate responsibilities in the pursuit of objectives established by management and overseen by the board.

4.A commitment to attract, develop and retain competent individuals in alignment with objectives.

5.Holding individuals accountable for their internal control responsibilities in pursuit of objectives.

Components of Internal Control

Internal Control consists of five integrated components.

Control Environment

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization.

The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance.

The resulting control environment has a pervasive impact on the overall system of internal control.

The five components of the COSO Internal Control framework:

Risk Assessment

The basis for how risks should be managed involves a dynamic process. Management must consider possible changes in the external environment and within the business that may be obstacles to its objectives. There are *four principles* of risk assessment:

6.Specifying objectives clearly enough for risks to be identified and assessed.

7.Identifying and analyzing risks in order to determine how they should be managed.

8.Considering the potential of fraud.

9.Identifying and assessing changes that could significantly impact the system of internal control.

Components of Internal Control

Risk Assessment

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and *adversely* affect the achievement of objectives.

Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity.

Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives.

Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

The five components of the COSO Internal Control framework:

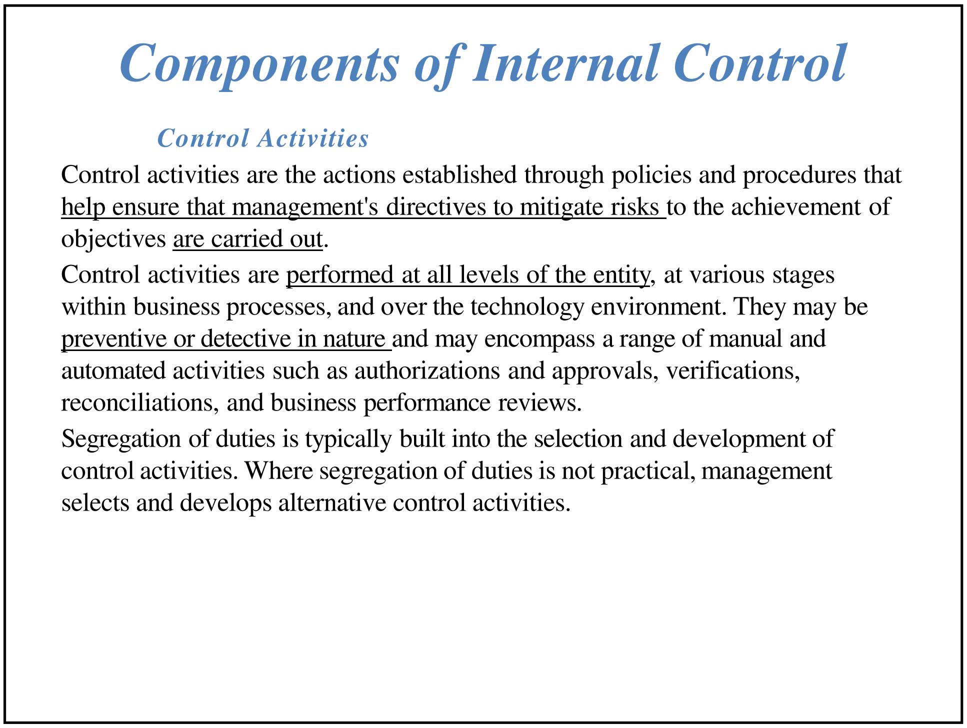
Control Activities

These are established to help ensure management's directives to mitigate risks get carried out. Control activities are performed at all levels and at various stages within the business process and over technology. There are *three principles* of control activities:

10.Selecting and developing controls that help mitigate risks to an acceptable level.

11.Selecting and developing general control activities over technology.

12.Deploying control activities as specified in policies and relevant procedures.



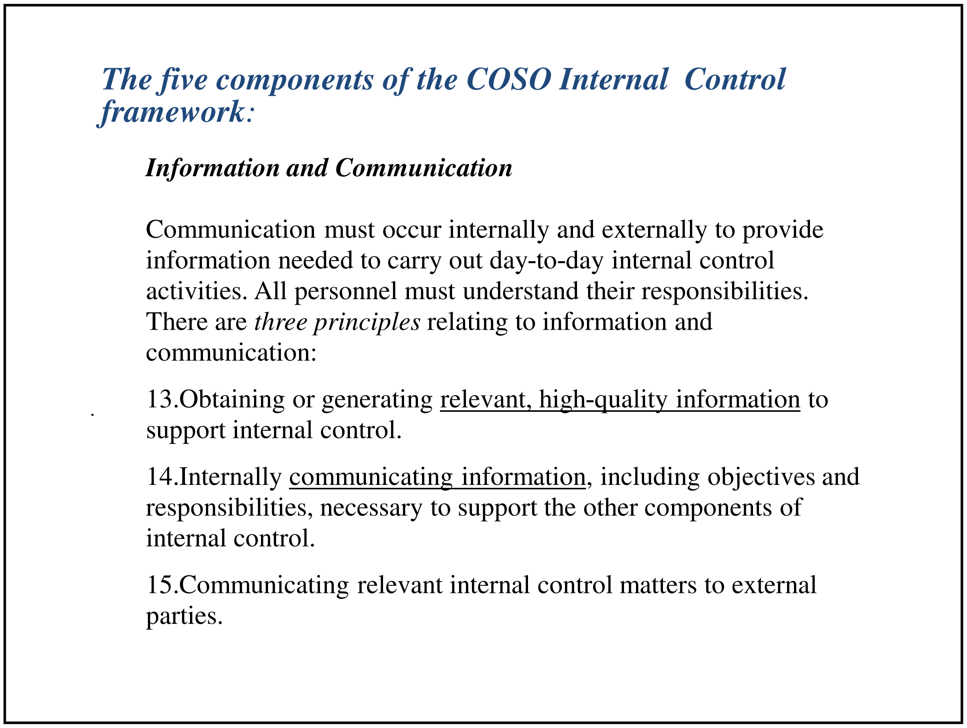
Components of Internal Control

Control Activities

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.



The five components of the COSO Internal Control framework:

Information and Communication

Communication must occur internally and externally to provide information needed to carry out day-to-day internal control activities. All personnel must understand their responsibilities. There are *three principles* relating to information and communication:

13.Obtaining or generating relevant, high-quality information to support internal control.

14.Internally communicating information, including objectives and responsibilities, necessary to support the other components of internal control.

15.Communicating relevant internal control matters to external parties.

Components of Internal Control

Information and Communication

Information is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control.

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information.

Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously.

External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

The five components of the COSO Internal Control framework:

Monitoring Activities

Evaluations ascertain whether each component of internal control is present and functioning. Deficiencies are communicated in a timely manner, with serious matters reported to senior management and the board. There are two principles relating to monitoring activities:

16. Selecting, developing and performing ongoing or separate evaluations of the components of internal control.
17. Evaluating and communicating deficiencies to those responsible for corrective action, including senior management and the board of directors, where appropriate.

Components of Internal Control

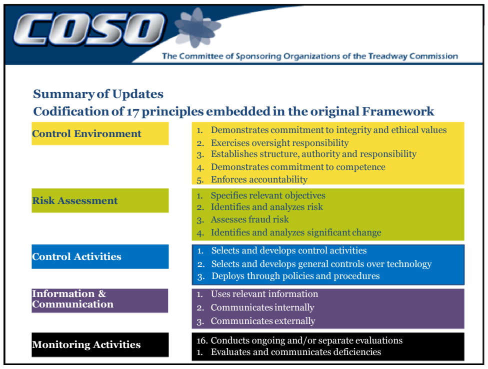
Monitoring Activities

Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component are present and functioning.

Ongoing evaluations built into business processes at different levels of the entity, provide timely information.

Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations.

Findings are evaluated against management's criteria and deficiencies are communicated to management and the board of directors as appropriate.



COSO

The Committee of Sponsoring Organizations of the Treadway Commission

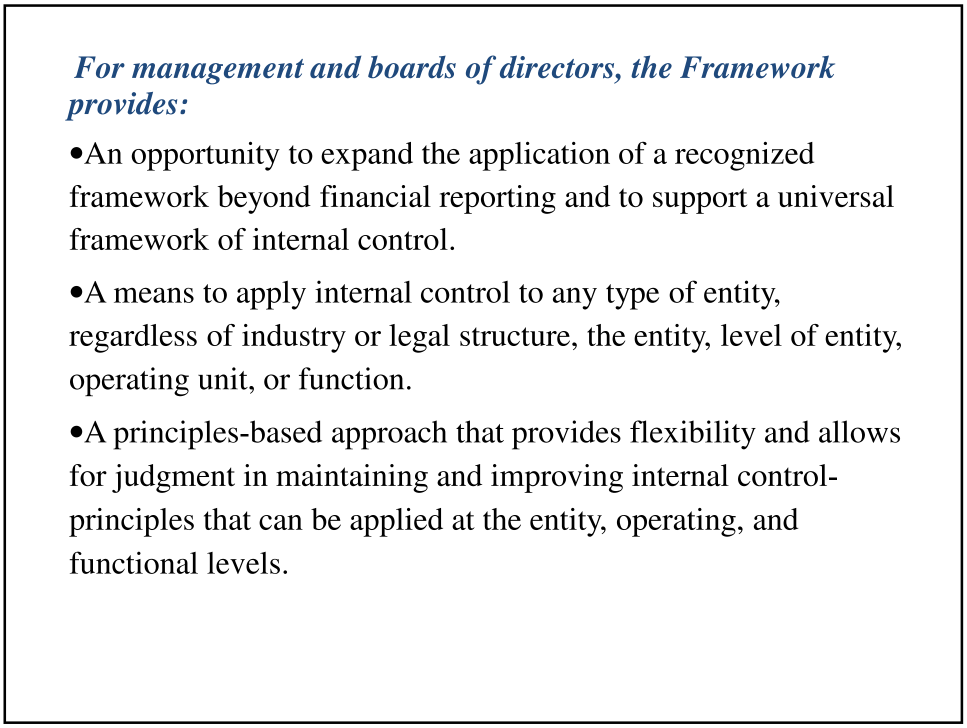
Summary of Updates

Codification of 17 principles embedded in the original Framework

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	1. Specifies relevant objectives 2. Identifies and analyzes risk 3. Assesses fraud risk 4. Identifies and analyzes significant change
Control Activities	1. Selects and develops control activities 2. Selects and develops general controls over technology 3. Deploys through policies and procedures
Information & Communication	1. Uses relevant information 2. Communicates internally 3. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 1. Evaluates and communicates deficiencies

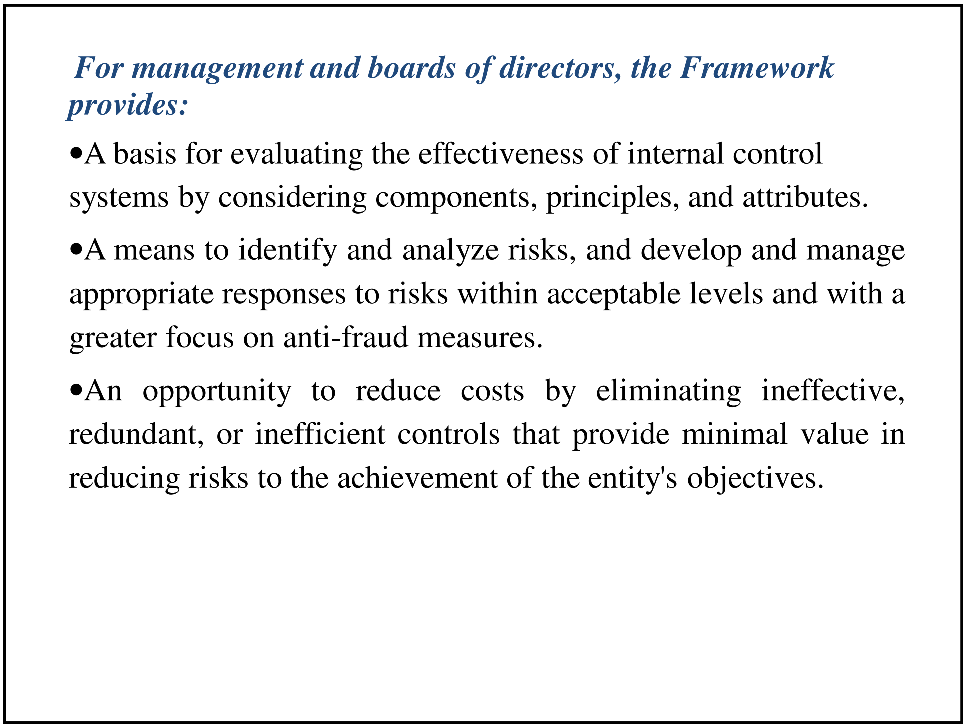
Benefits of the Updated *Framework*

- **Improve governance**
- **Expand use beyond financial reporting**
- **Improve quality of risk assessment**
- **Strengthen anti-fraud efforts**
- **Adapt controls to changing business needs**
- **Greater applicability for various business models**



For management and boards of directors, the Framework provides:

- An opportunity to expand the application of a recognized framework beyond financial reporting and to support a universal framework of internal control.
- A means to apply internal control to any type of entity, regardless of industry or legal structure, the entity, level of entity, operating unit, or function.
- A principles-based approach that provides flexibility and allows for judgment in maintaining and improving internal control-principles that can be applied at the entity, operating, and functional levels.



For management and boards of directors, the Framework provides:

- A basis for evaluating the effectiveness of internal control systems by considering components, principles, and attributes.
- A means to identify and analyze risks, and develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures.
- An opportunity to reduce costs by eliminating ineffective, redundant, or inefficient controls that provide minimal value in reducing risks to the achievement of the entity's objectives.

Benefits to Stakeholders

For external stakeholders of an entity and others that interact with the entity, the *Framework* provides:

•Greater confidence in the board of directors' oversight over internal control systems.

•Greater confidence in the organization's ability to respond to risk and changes in the business and operating environments.

•A greater understanding of the criteria used to design, implement, and evaluate internal control.

Benefits to Stakeholders

For external stakeholders of an entity and others that interact with the entity, the *Framework* provides:

•Recognition that through the use of appropriate judgment, management may be able to reduce costs by eliminating ineffective, redundant, or inefficient controls.

•A means to align internal control with other standards to develop an integrated view of specific functions and other areas of focus.

Benefits to Stakeholders

For external stakeholders of an entity and others that interact with the entity, the *Framework* provides:

The above considerations are compelling reasons why organizations—regardless of the entity's legal structure, size, complexity, or purpose—will want to apply the *Framework* in designing, implementing, conducting, and evaluating their systems of internal control.

Defining Internal Control

Internal control is defined as follows:

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations.*
- *Reliability of reporting.*
- *Compliance with applicable laws and regulations.*

This definition reflects certain fundamental concepts. Internal control is:

- *A process consisting of ongoing tasks and activities. It is a means to an end, not an end in itself.*
- *Effected by people. It is not merely about policy manuals, systems, and forms, but people at every level of an organization that impact internal control.*
- *Able to provide reasonable assurance, not absolute assurance, to an entity's senior management and board.*
- *Geared to the achievement of objectives in one or more categories—operations, reporting, and compliance.*
- *Adaptable to the entity structure.*

Objectives

The *Framework* sets forth three categories of objectives, which allow organizations to focus on differing aspects of internal control:

•*Operations Objectives—These pertain to effectiveness and efficiency of the entity's operations, including operations and financial performance goals and safeguarding assets against loss.*

•*Reporting Objectives—These pertain to the reliability of reporting. They include internal and external financial and non-financial reporting.*

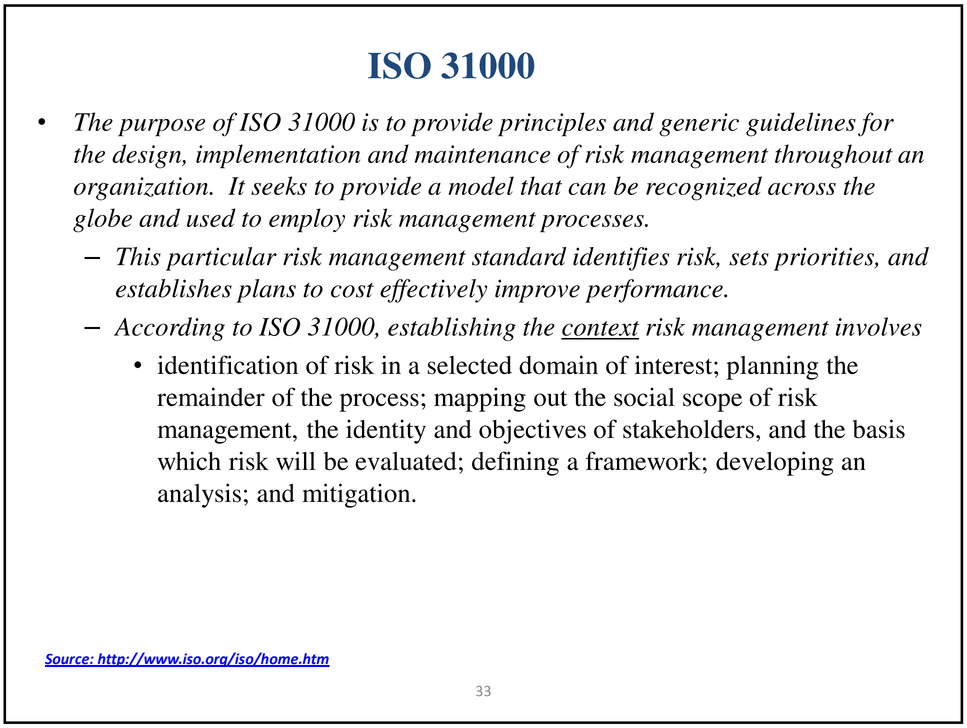
•*Compliance Objectives—These pertain to adherence to laws and regulations to which the entity is subject.*

ISO 31000

- *A set of principle based standards for enterprise risk management by the International Organization for Standardization.*
- *ISO is made up of 161 member country organizations, which are divided into three categories.*
  - A member body *of ISO is the national body "most representative of standardization in its country". Only one such body for each country is accepted for membership of ISO. Member bodies are entitled to participate and exercise full voting rights on any technical committee and policy committee of ISO.*
  - A correspondent member *is usually an organization in a country which does not yet have a fully-developed national standards activity. Correspondent members do not take an active part in the technical and policy development work, but are entitled to be kept fully informed about the work of interest to them.*
  - Subscriber membership *has been established for countries with very small economies. Subscriber members pay reduced membership fees that nevertheless allow them to maintain contact with international standardization.*

Source: http://www.iso.org/iso/home.htm

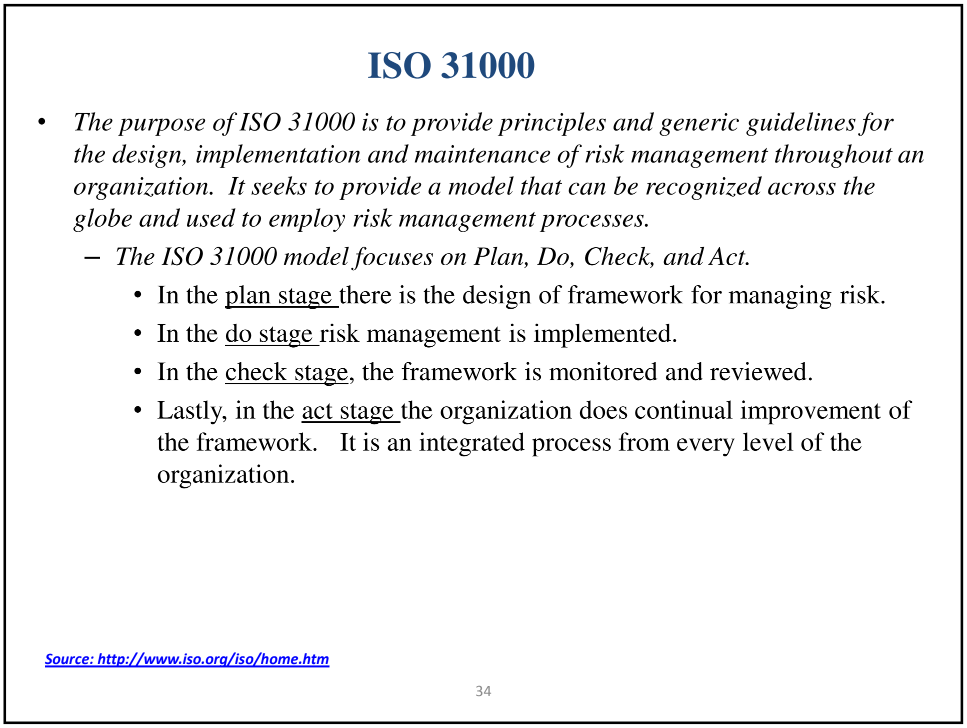
32



ISO 31000

- *The purpose of ISO 31000 is to provide principles and generic guidelines for the design, implementation and maintenance of risk management throughout an organization. It seeks to provide a model that can be recognized across the globe and used to employ risk management processes.*
  - *This particular risk management standard identifies risk, sets priorities, and establishes plans to cost effectively improve performance.*
  - *According to ISO 31000, establishing the context risk management involves*
    - identification of risk in a selected domain of interest; planning the remainder of the process; mapping out the social scope of risk management, the identity and objectives of stakeholders, and the basis which risk will be evaluated; defining a framework; developing an analysis; and mitigation.

Source: http://www.iso.org/iso/home.htm



ISO 31000

- *The purpose of ISO 31000 is to provide principles and generic guidelines for the design, implementation and maintenance of risk management throughout an organization. It seeks to provide a model that can be recognized across the globe and used to employ risk management processes.*
  - *The ISO 31000 model focuses on Plan, Do, Check, and Act.*
    - In the plan stage there is the design of framework for managing risk.
    - In the do stage risk management is implemented.
    - In the check stage, the framework is monitored and reviewed.
    - Lastly, in the act stage the organization does continual improvement of the framework. It is an integrated process from every level of the organization.

Source: http://www.iso.org/iso/home.htm

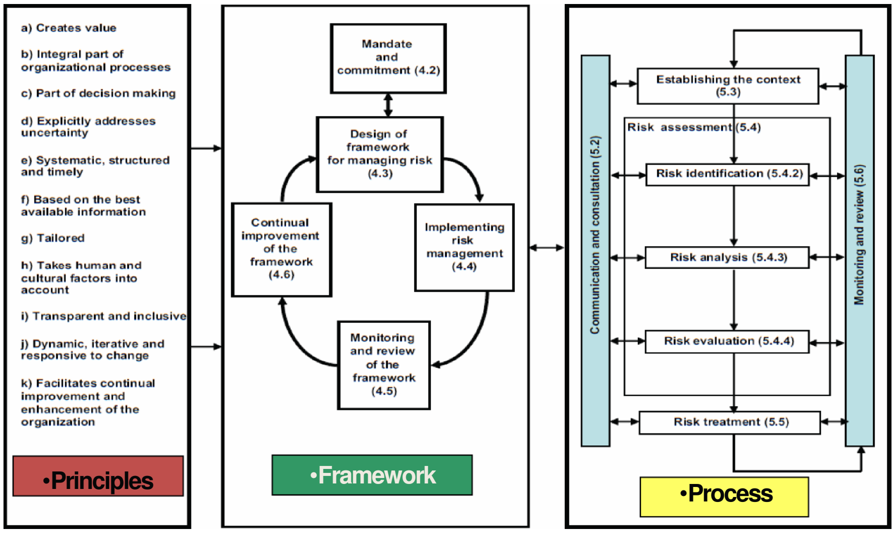
ISO 31000

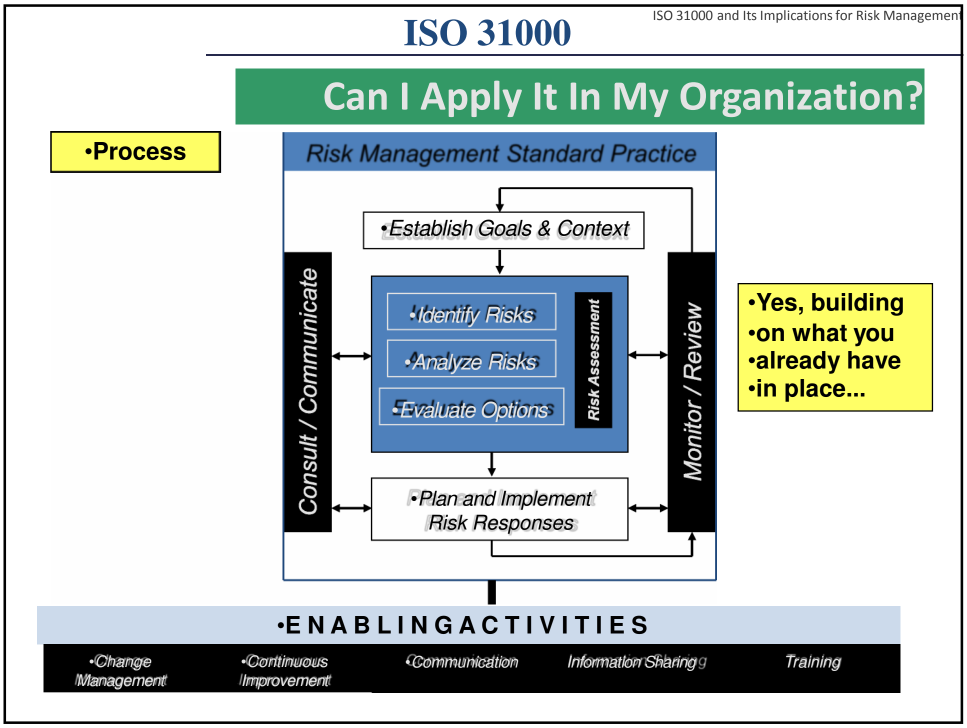
- For the United States, *the American National Standards Institute (ANSI), founded in 1918, has coordinated the development of voluntary consensus standards in the United States and has represented the needs and views of U.S. stakeholders in standardization forums around the globe.*
  - *ANSI is the U.S. member body to ISO and, via its U.S. National Committee, the International Electrotechnical Commission (IEC). ANSI is also a member of the International Accreditation Forum (IAF).*

Source: http://www.iso.org/iso/home.htm

ISO 31000

•ISO 31000 - Risk Management (At-A-Glance)


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
•Principles
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
•Framework
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
•Process



ISO 31000 and Its Implications for Risk Management

ISO 31000

Can I Apply It In My Organization?

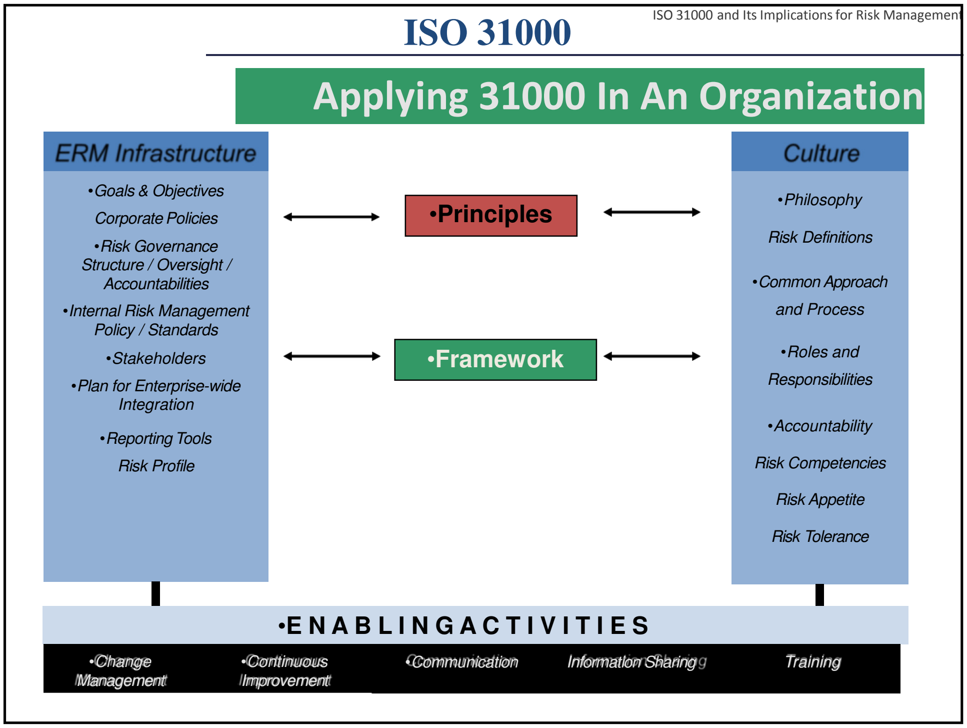
- Process

Risk Management Standard Practice

- Yes, building
- on what you
- already have
- in place…

- ENABLING ACTIVITIES

•Change Management	•Continuous Improvement	•Communication	Information Sharing	Training



ISO 31000 and Its Implications for Risk Management

ISO 31000

Applying 31000 In An Organization

ERM Infrastructure

- Goals & Objectives
- Corporate Policies
- Risk Governance Structure / Oversight / Accountabilities
- Internal Risk Management Policy / Standards
- Stakeholders
- Plan for Enterprise-wide Integration
- Reporting Tools
- Risk Profile

Culture

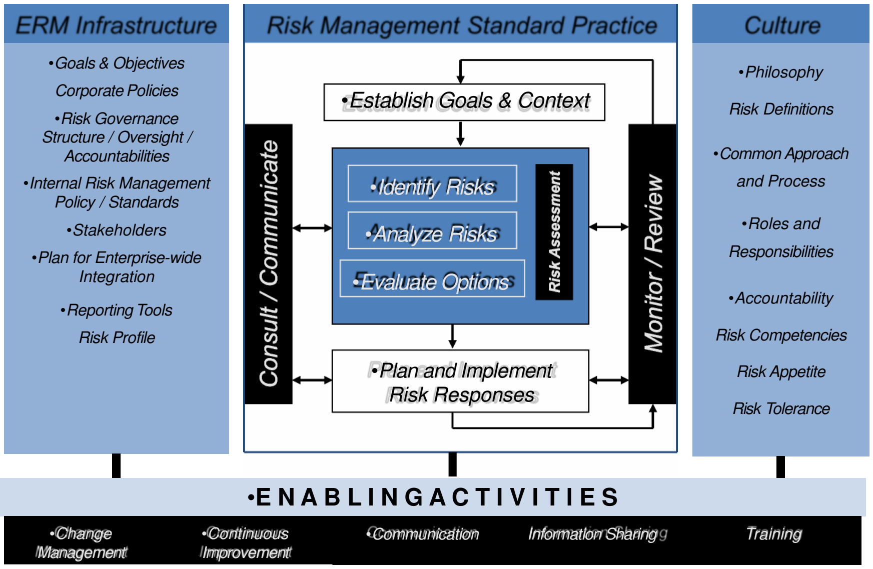
- Philosophy
- Risk Definitions
- Common Approach and Process
- Roles and Responsibilities
- Accountability
- Risk Competencies
- Risk Appetite
- Risk Tolerance

- ENABLING ACTIVITIES

•Change Management	•Continuous Improvement	•Communication	Information Sharing	Training

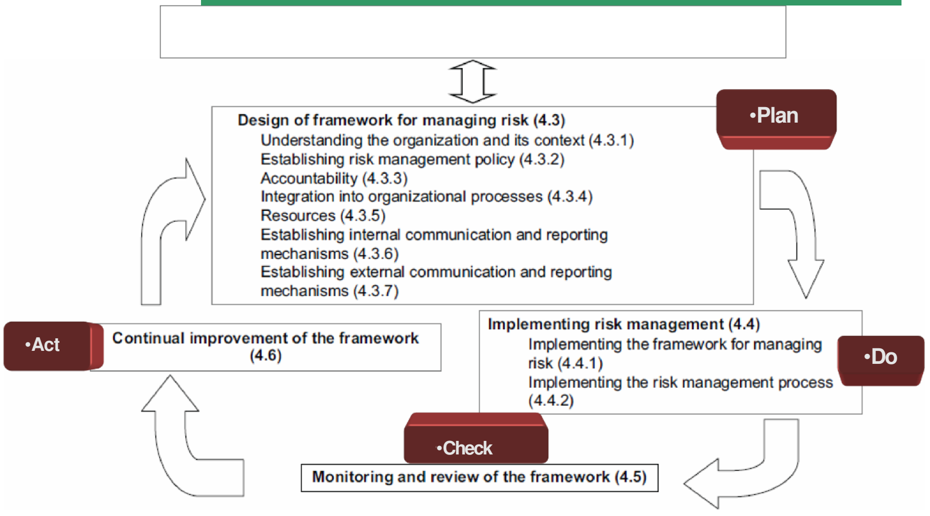
ISO 31000

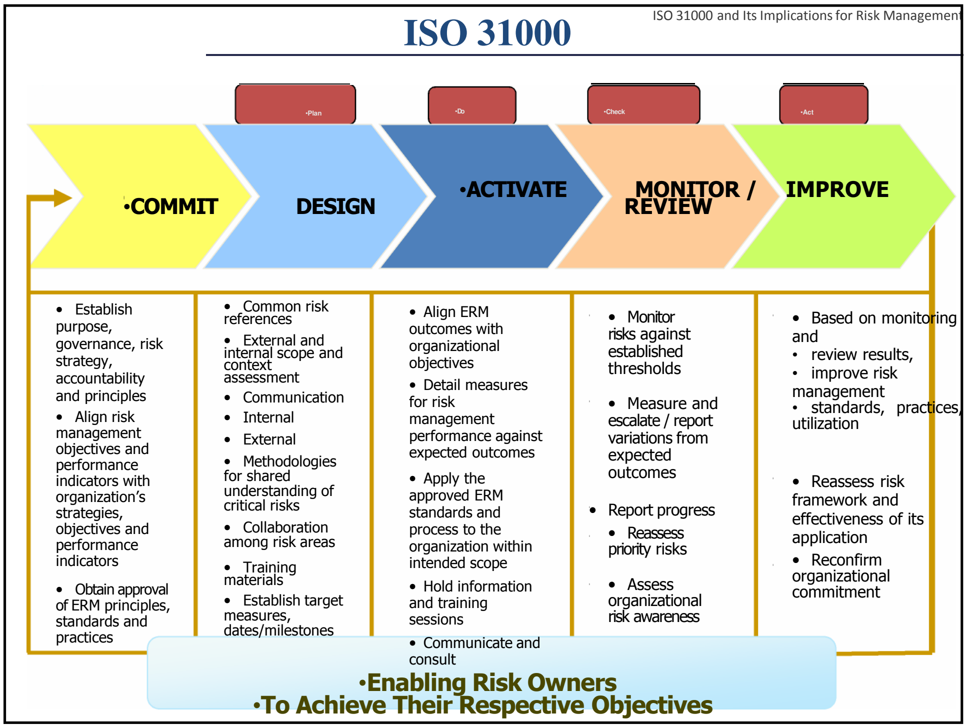
Bringing It All Together



ISO 31000

ISO 31000 - Risk Management Framework Process Overview


•Plan
Design of framework for managing risk (4.3)
Understanding the organization and its context (4.3.1)
Establishing risk management policy (4.3.2)
Accountability (4.3.3)
Integration into organizational processes (4.3.4)
Resources (4.3.5)
Establishing internal communication and reporting mechanisms (4.3.6)
Establishing external communication and reporting mechanisms (4.3.7)
•Act
Continual improvement of the framework (4.6)
Implementing risk management (4.4)
Implementing the framework for managing risk (4.4.1)
Implementing the risk management process (4.4.2)
•Do
•Check
Monitoring and review of the framework (4.5)



ISO 31000 and Its Implications for Risk Management

ISO 31000

•COMMIT

- Establish purpose, governance, risk strategy, accountability and principles
- Align risk management objectives and performance indicators with organization’s strategies, objectives and performance indicators
- Obtain approval of ERM principles, standards and practices

DESIGN

- Common risk references
- External and internal scope and context assessment
- Communication
- Internal
- External
- Methodologies for shared understanding of critical risks
- Collaboration among risk areas
- Training materials
- Establish target measures, dates/milestones

•ACTIVATE

- Align ERM outcomes with organizational objectives
- Detail measures for risk management performance against expected outcomes
- Apply the approved ERM standards and process to the organization within intended scope
- Hold information and training sessions
- Communicate and consult

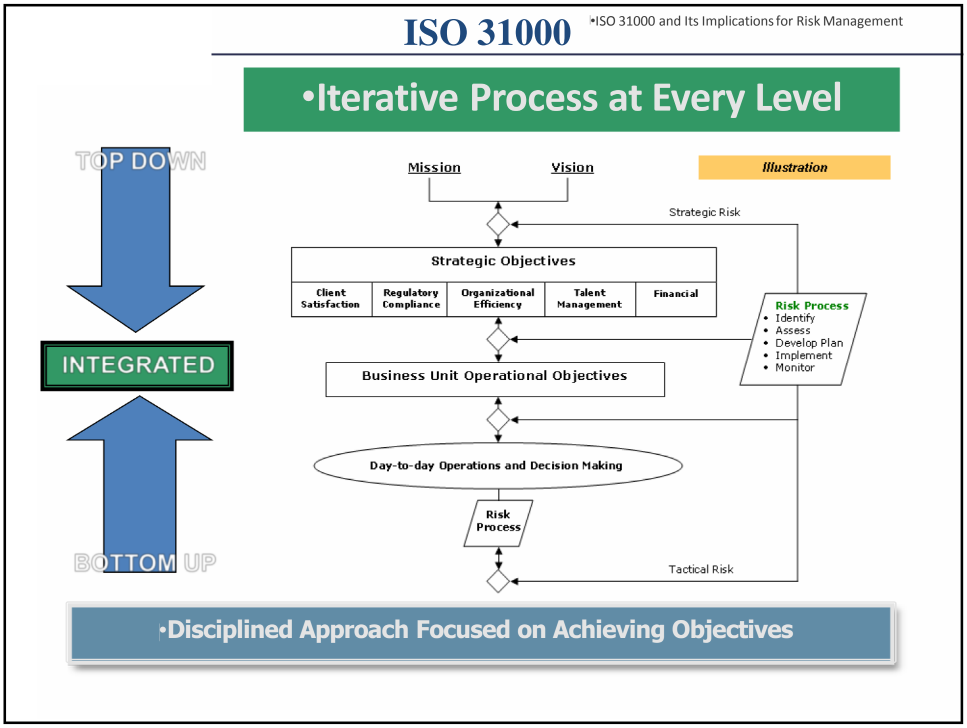
MONITOR / REVIEW

- Monitor risks against established thresholds
- Measure and escalate / report variations from expected outcomes
- Report progress
- Reassess priority risks
- Assess organizational risk awareness

IMPROVE

- Based on monitoring and
- review results,
- improve risk management
- standards, practices, utilization
- Reassess risk framework and effectiveness of its application
- Reconfirm organizational commitment

•Enabling Risk Owners
•To Achieve Their Respective Objectives



•ISO 31000 and Its Implications for Risk Management

ISO 31000

•Iterative Process at Every Level

•Disciplined Approach Focused on Achieving Objectives