Enterprise Risk Management

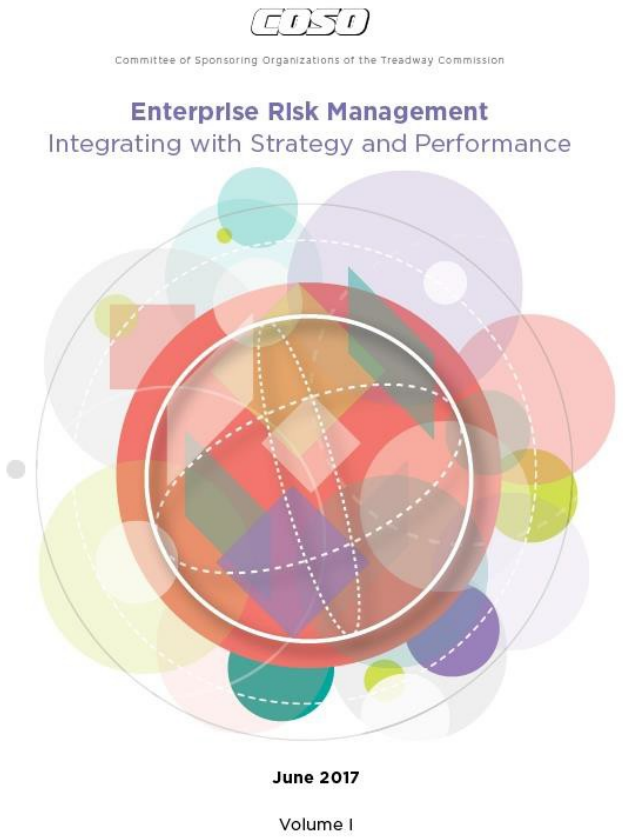
Integrating with Strategy and Performance

Sandra B. Richtermeyer, PhD
Former COSO Board Member &
Dean-Manning School of Business
University of Massachusetts Lowell

COSO's Enterprise Risk Management Framework

Refreshed in 2017

Original Release in 2004



COSO's Mission and Guiding Principle

Mission

- COSO's Mission is "To provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."

Fundamental Principle

- EFFECTIVE risk management and internal control are necessary for long term success of all organizations

About COSO…

> 600,000 professionals

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM) internal control and fraud deterrence

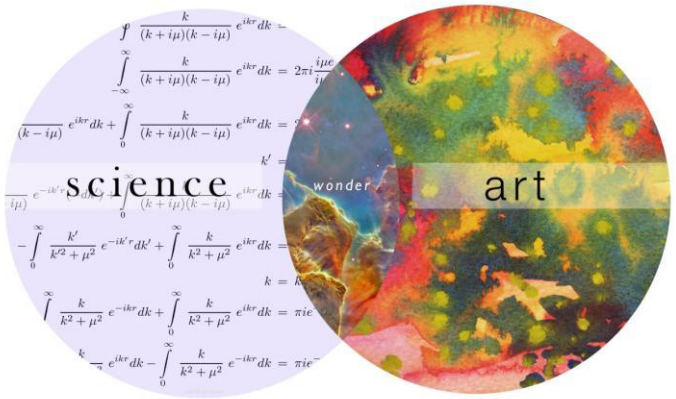
COSO Project to Update the Enterprise Risk Management Framework

- The COSO Board released in September 2017 an update to the 2004 Enterprise
- Risk Management–Integrated Framework
- That framework is used widely used by management to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase value
- This initiative enhanced the framework's content and relevance in an increasingly complex business environment so that organizations can attain better value from enterprise risk management

Key Reasons to Update the Framework

- Concepts and practices have evolved
- Lessons learned
- Bar raised with respect to enterprise risk management
- Business and operating environments more complex, technologically driven, and global in scale
- Stakeholders more engaged, seeking greater transparency and accountability
- Risk discussions increasingly prominent at the board level

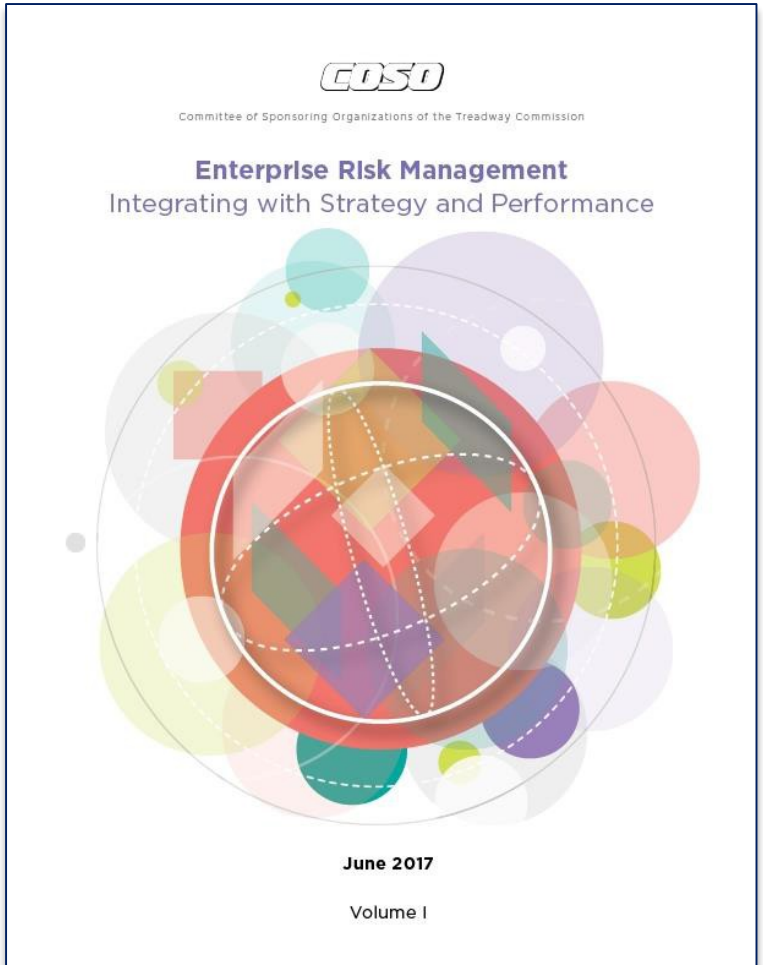
A Key Introduction…



Our understanding of the nature of risk, the art and science of choice lies at the core of our modern market economy

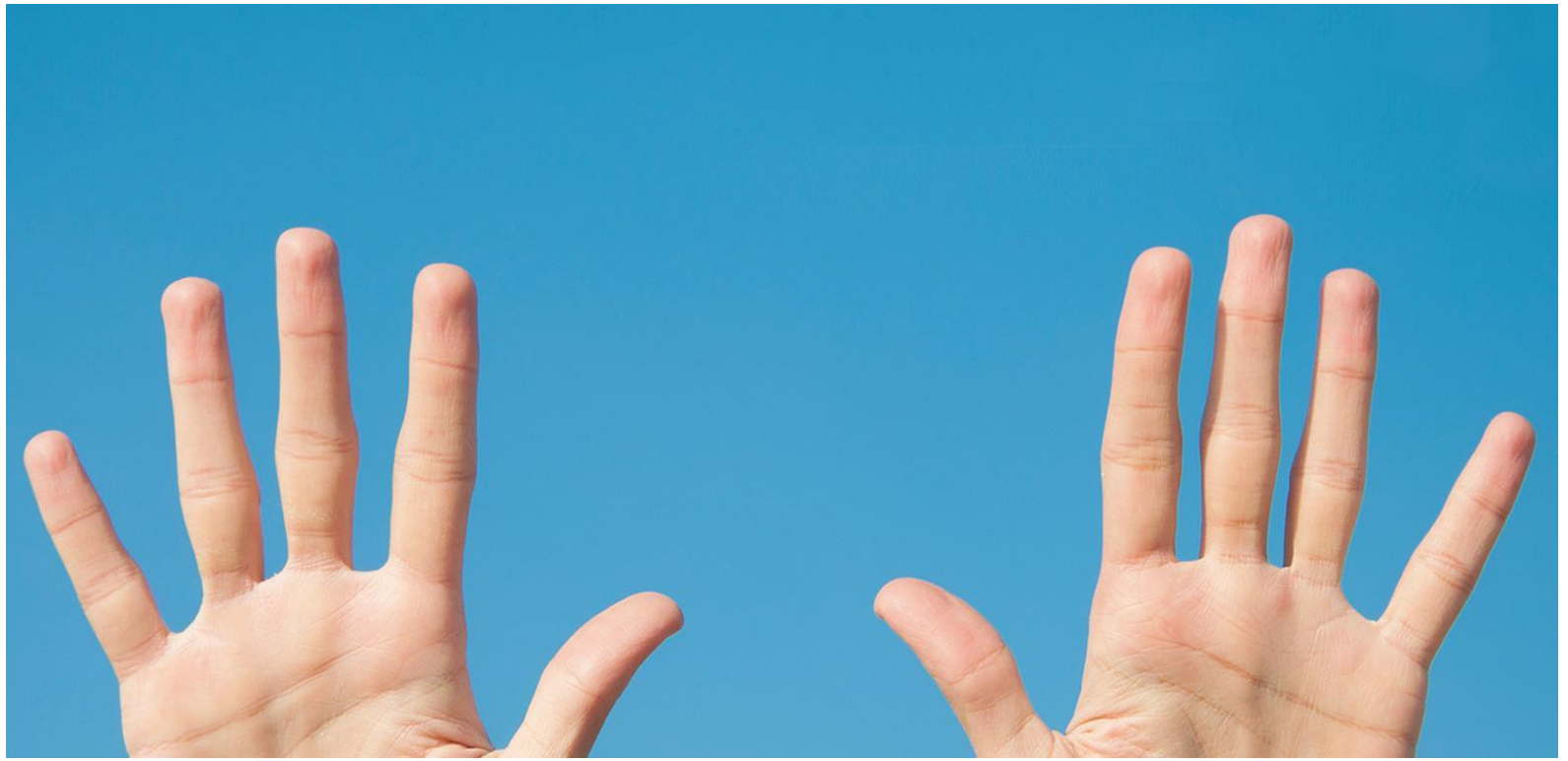
Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with uncertainly in these choices is a part of our organizational lives.

A New Title…



- Retitled as *Enterprise Risk Management—* ***Integrating*** *with Strategy and Performance*
- Recognizes the importance of strategy and entity performance
- Further delineates enterprise risk management from internal control

10 Key Things to Know about the ERM Framework



10 Key Things to Know about the ERM Framework

1) Provides a New Document Structure

- Framework focused on fewer components (five)

- Uses focused call-out examples to emphasize key points (> 30)
- Follows the business model versus an isolated risk management process

10 Key Things to Know about the ERM Framework

2) Introduces Principles

20 key principles within each of the five components

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

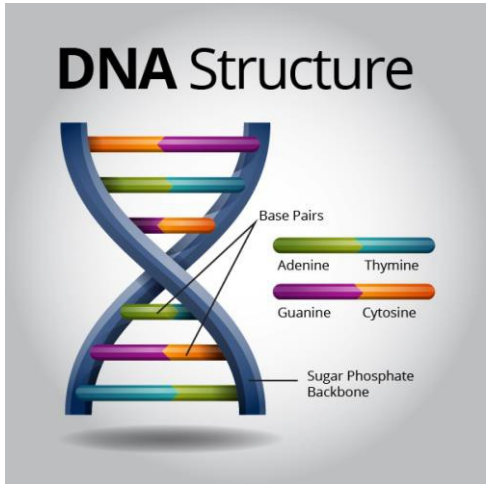
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

10 Key Things to Know about the ERM Framework

3) Incorporates New Graphics/Concepts

Graphic has stronger ties to the business model



10 Key Things to Know about the ERM Framework

4) Focuses on Integration

Integrating ERM with business practices results in better information that support improved decision-making and leads to enhanced performance

It helps organizations to:

- Anticipate risks earlier or more explicitly, opening up more options for managing the risks
- Identify and pursue existing and new opportunities
- Respond to deviations in performance more quickly and consistently
- Develop and report a more comprehensive and consistent portfolio view of risk
- Improve collaboration, trust, and information sharing

10 Key Things to Know about the ERM Framework

5) Emphasizes Value

- Enhances the focus on value – how entities **create, preserve, and realize value**
- Embeds value throughout the framework, as evidenced by its:
  - Prominence in the core definition of enterprise risk management
  - Extensive discussion in principles
  - Linkage to risk appetite
  - Focus on the ability to manage risk to acceptable levels

10 Key Things to Know about the ERM Framework

6) Links to Strategy

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy

10 Key Things to Know about the ERM Framework

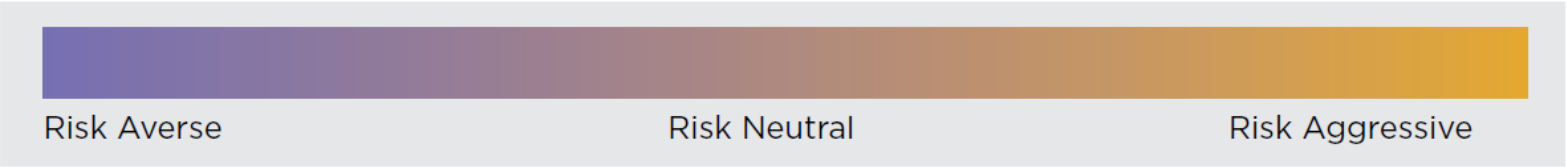
7) Links to Performance

- Enables the achievement of strategy by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives – not as individual risks

10 Key Things to Know about the ERM Framework

8) Recognizes Importance of Culture

- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core values
- Depicts culture behavior within a risk spectrum



- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior

10 Key Things to Know about the ERM Framework

9) Focuses on Decision-Making

- Explores how enterprise risk management drives risk aware decision making
- Highlights how risk awareness optimizes and aligns decisions impacting performance
- Explores how risk aware decisions affect the risk profile

10 Key Things to Know about the ERM Framework

9) Decision-Making Uncertainty/Certainty

- Selecting SAP or Oracle
- Setting the quarterly revenue plan for $20 million
- Hiring a new VP of_____
- Not developing a new product
- Making a new investment
- Opening a new office
- Closing an office

10 Key Things to Know about the ERM Framework

10) Builds Links to Internal Control

- The document does not replace the *Internal Control – Integrated Framework (more later)*
- The two frameworks are distinct and complementary
- Both use a components and principles structure
- Aspects of internal control common to enterprise risk management are not repeated
- Some aspects of internal control are developed further in this framework

Culture, ERM, Controls, or ALL?

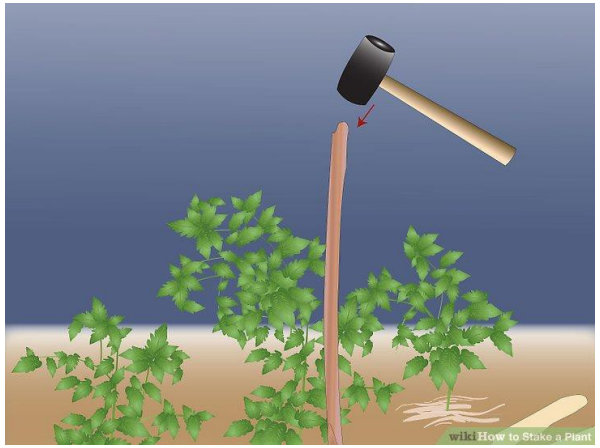
Putting A Stake in the Ground…

Risk

The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur)

Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value



You May Already be “Doing ERM”…

- Strong, Articulated Mission, Clear Vision and Values
- Commitment to the concept of ERM activities and integration
- Strategy as the best alternative, Risk vs. Reward, linked to objectives
- Understand uncertainly of our world and decisions we make
- Big focus on Change, so what, what do we do
- Focus and measurement on Objectives
- Going through the “WHAT IF” process
- Knowing what you won’t do and why
- Evaluating if ERM is adding value

ERM Myth Busting and Motivations

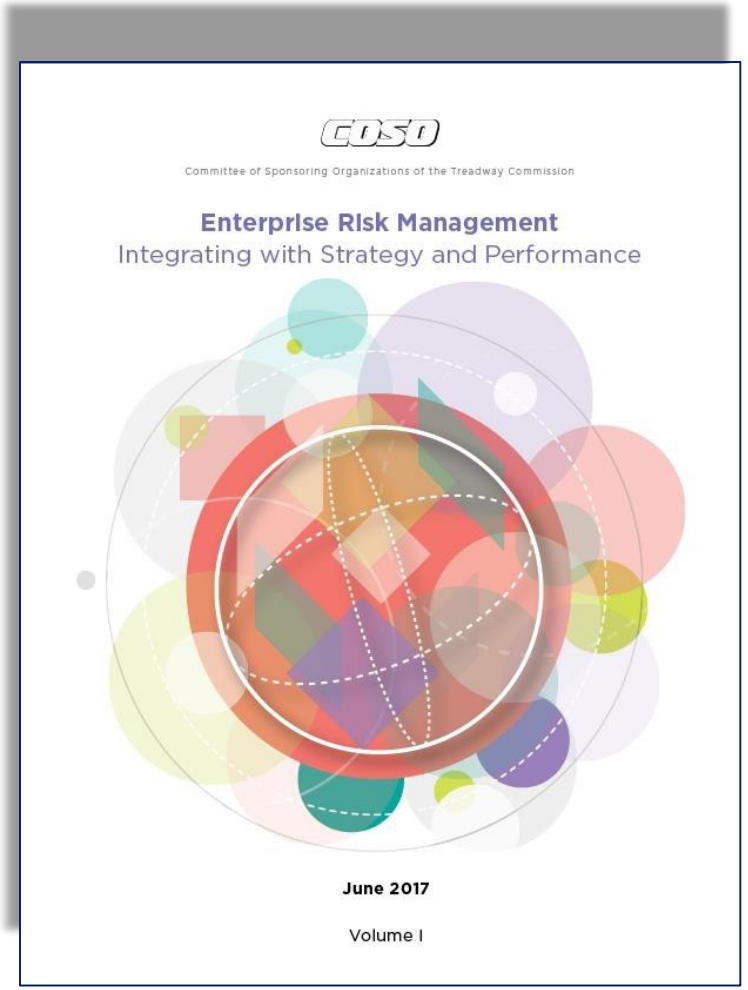
- It’s not a function or software application
- It’s not a long list, too long to try and conquer
- CRO’s don’t own risks, they facilitate ERM activities
- Everyone is a risk manager, kind of
- Its’ not an “add-on”- put it in a blender, build it in
- Risk isn’t all bad – it can be great!
- COSO can’t make you do anything
- Make better decisions
- #*&% still happens

- It’s gotta make you better!

Compendium of Examples

- A compendium of examples is also being developed, illustrating:
  - All principles
  - A variety of entity sizes from global through to national, regional, and local entities
  - A variety of industry types
  - Actual company practices and be augmented with expected practices in select areas, as needed
- Written from the perspective of the business

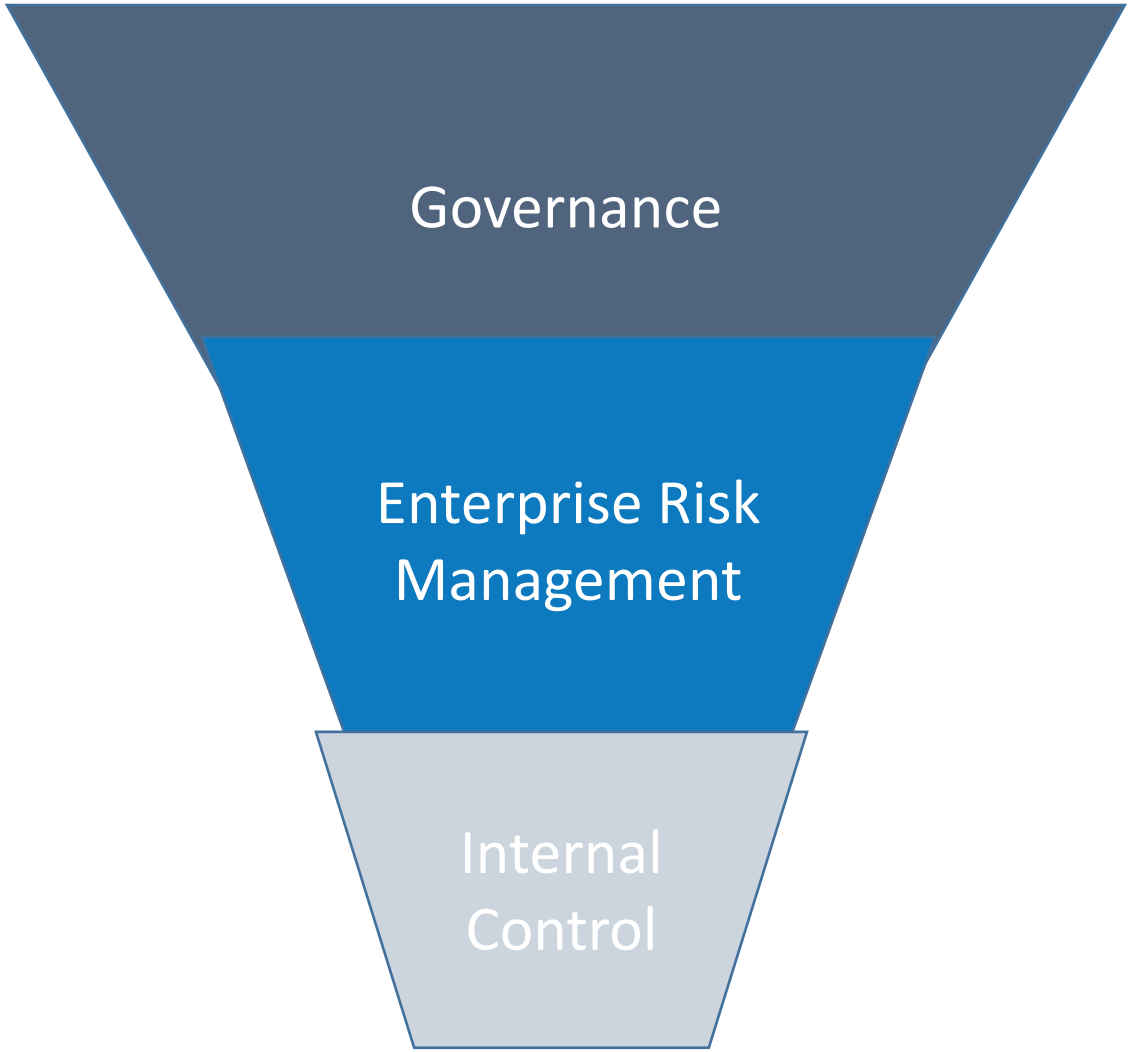
Let's Transition to the Internal Control Integrated Framework



Key Considerations

How does the ERM Framework Link to the Internal Control Integrated Framework (ICIF)?

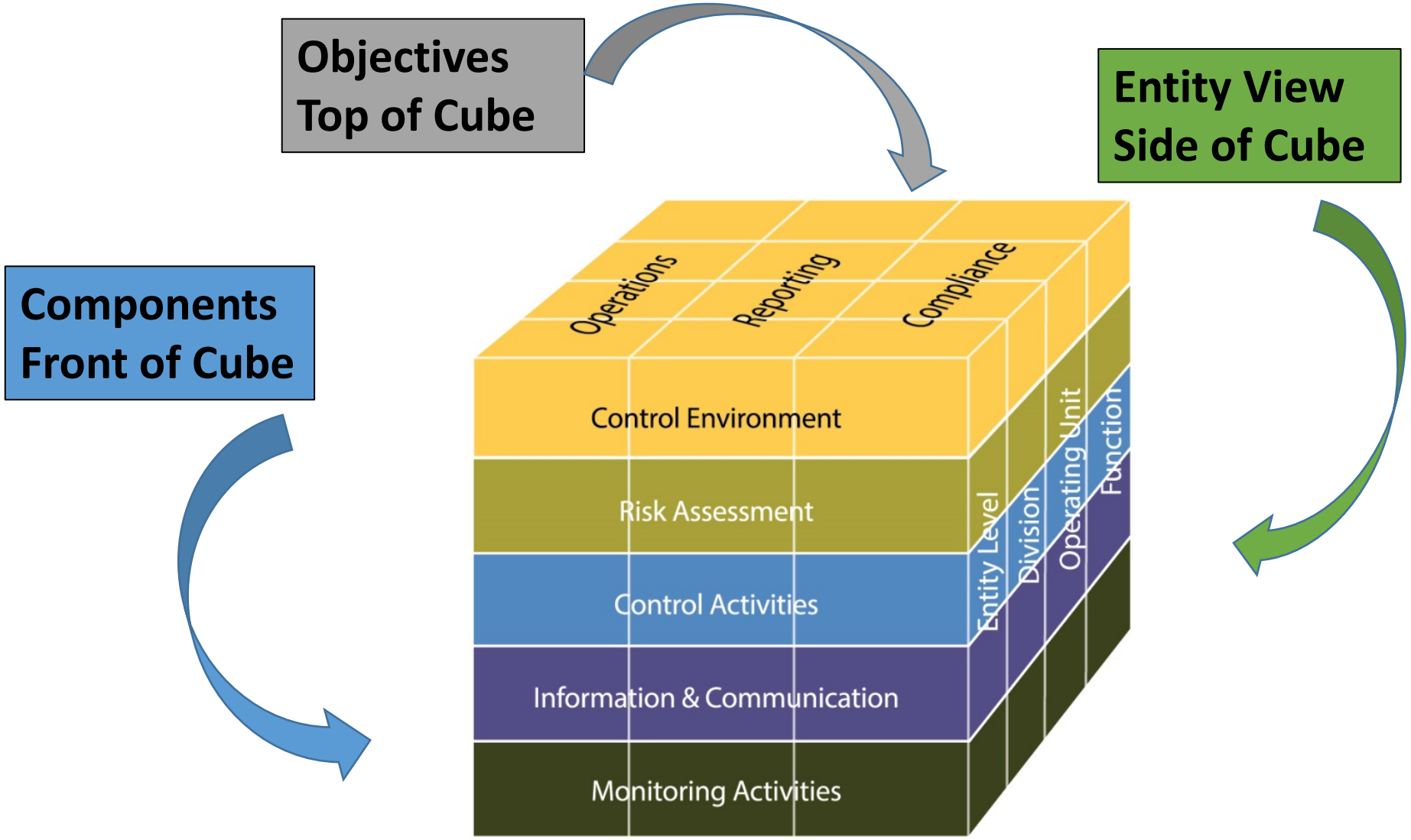
Key Relationships



COSO's Definition of Internal Controls

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 relating to operations, reporting and compliance.

The COSO Cube



Three Types of Objectives

Operations – achievement of an entity's basic mission, vision & strategies

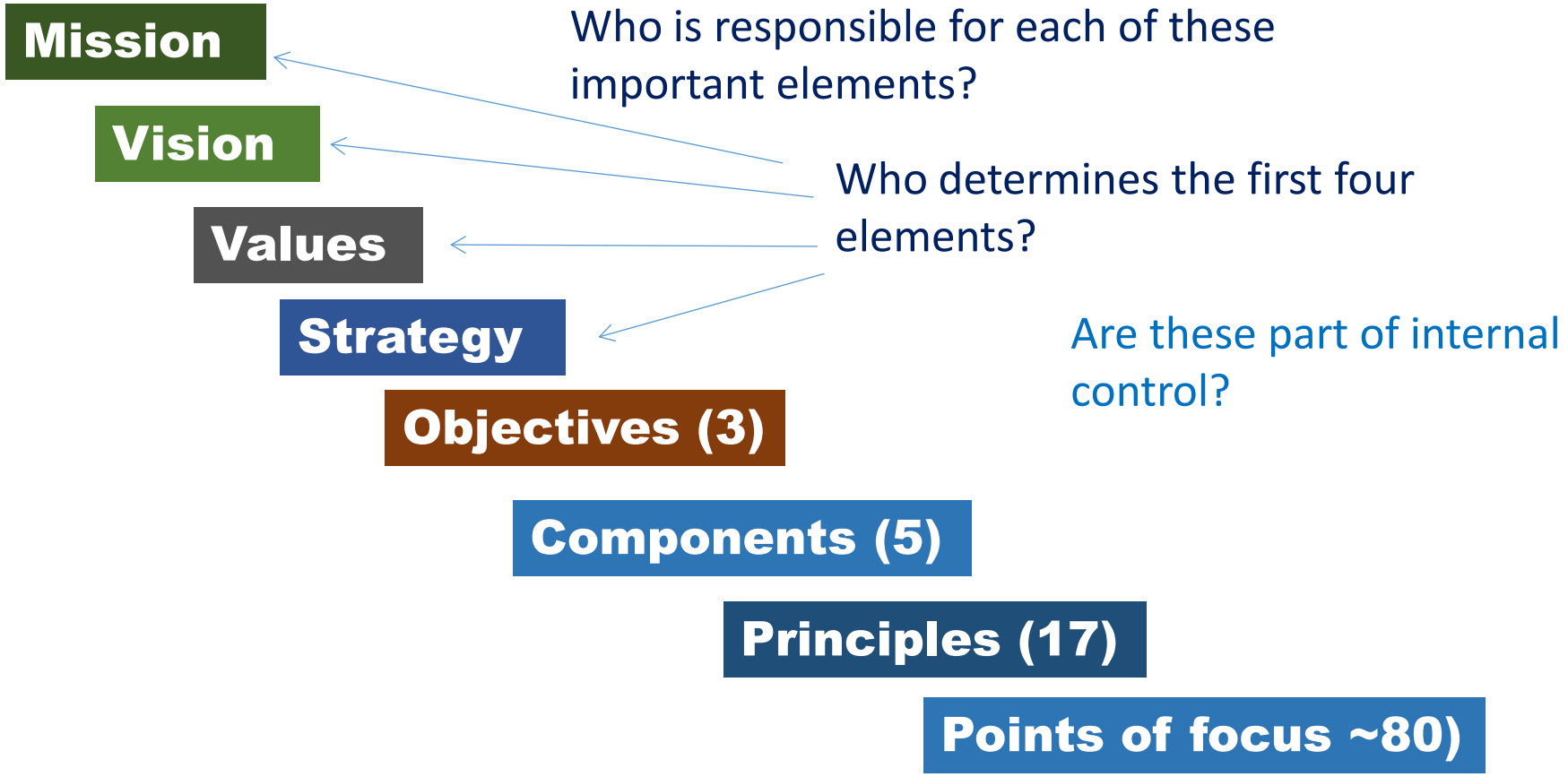
Reporting – external financial & non-financial, internal financial & non-financial

Compliance – laws, regulations

5 Components & 17 Principles of the ICIF

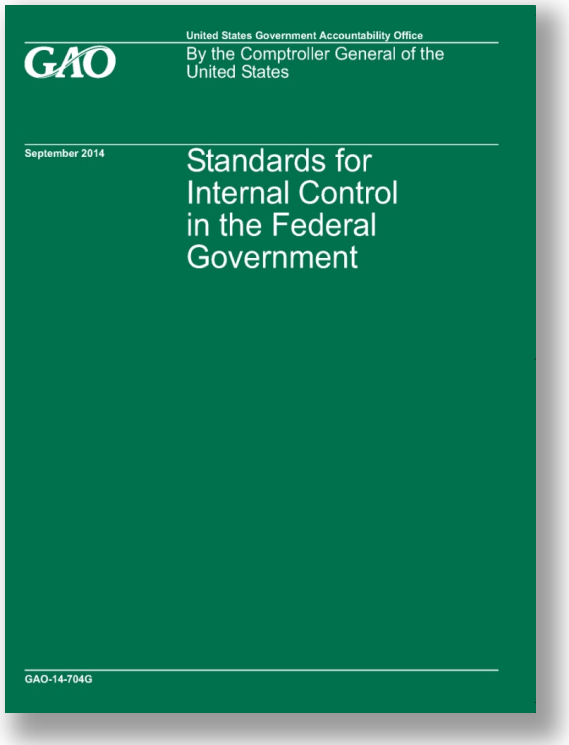
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Linking Organization Essentials with Main Parts of the COSO ICIF



Public Sector Use of COSO

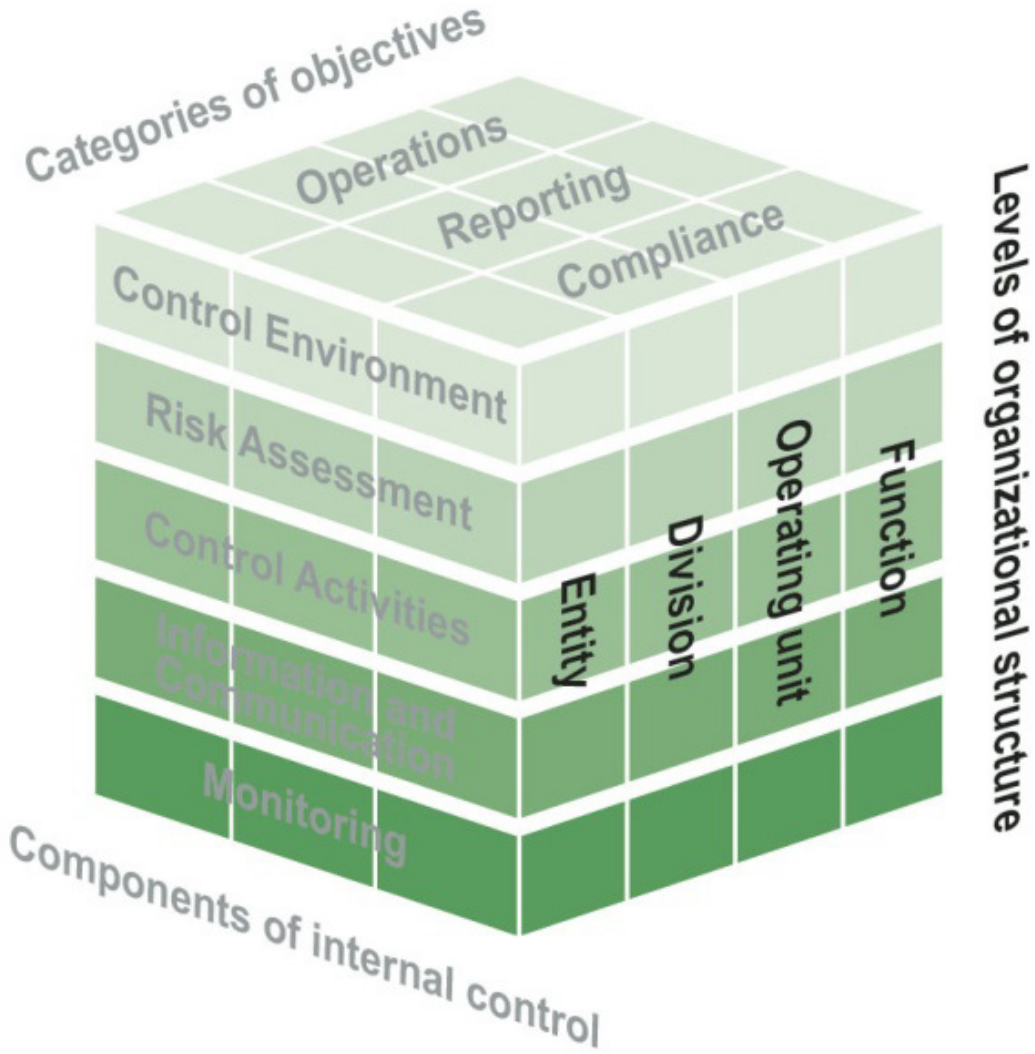
The Green Book



The COSO Internal Control Integrated Framework is Embedded in U.S. GAO's Green Book

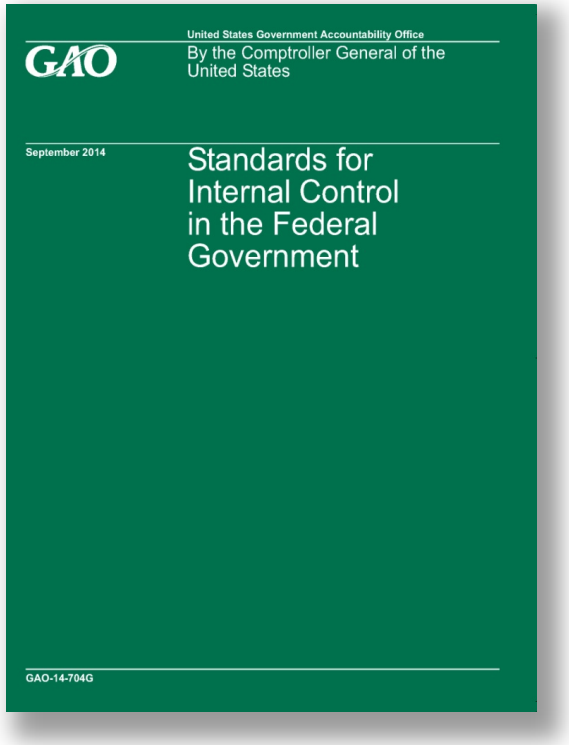
GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Green Book Cube



Source: COSO, GAO

The Green Book



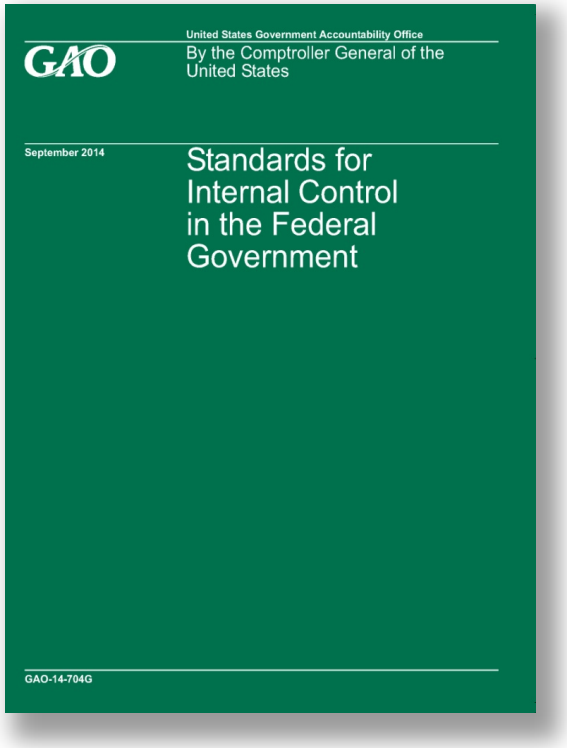
A required standard for all Federal agencies and departments

Use is on the rise for many states and local governments

Available for free download

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

The Green Book

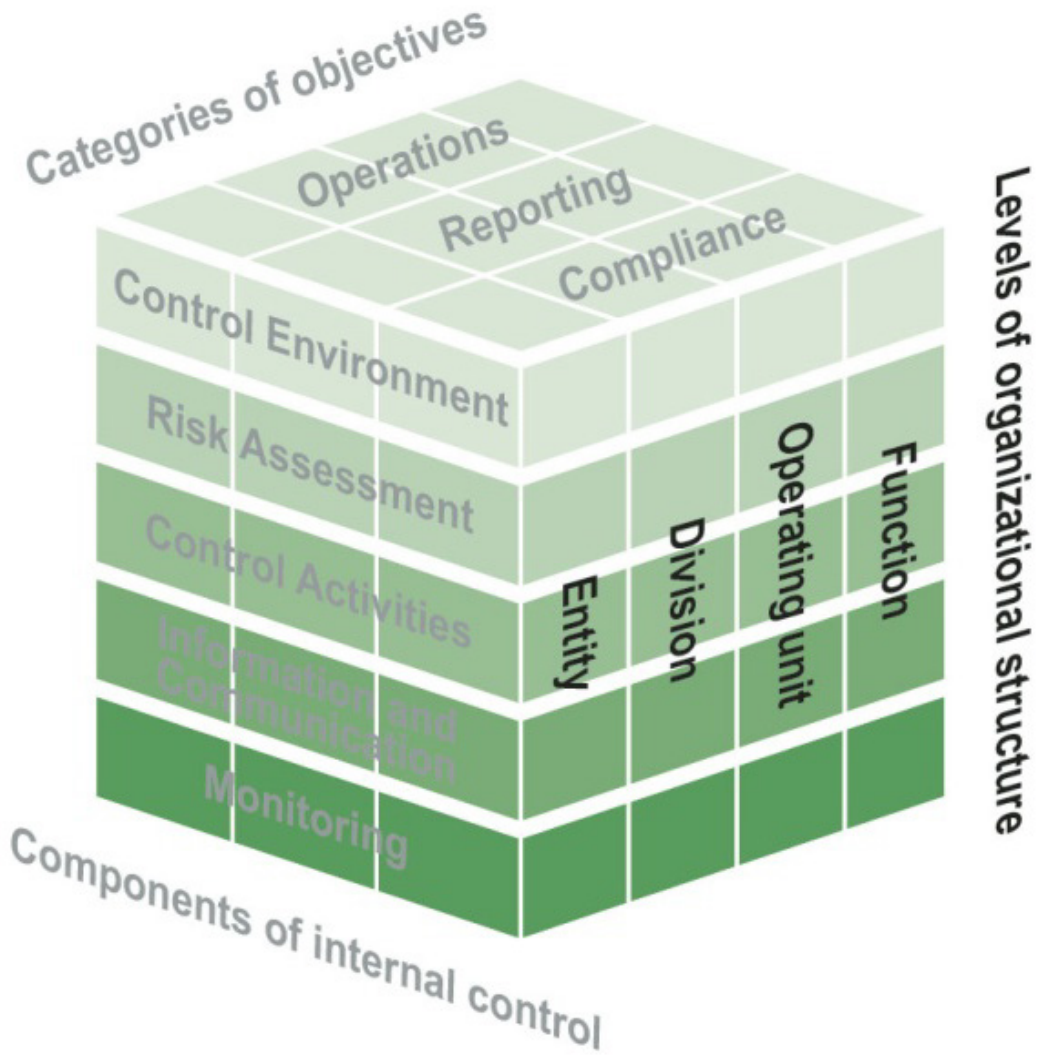


Reflects federal internal control standards required per Federal Managers' Financial Integrity Act (FMFIA)

Serves as a base for OMB Circular A-123

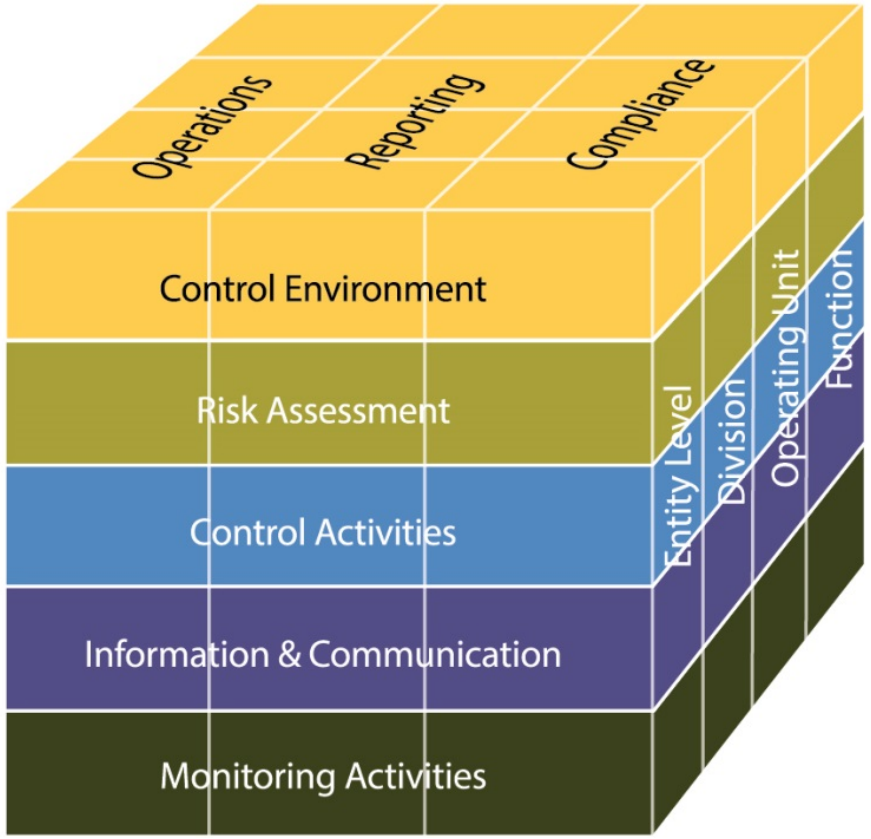
GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Both Cubes


Categories of objectives
Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information and Communication
Monitoring
Entity
Division
Operating unit
Function
Levels of organizational structure
Components of internal control


Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity Level
Division
Operating Unit
Function

COSO Cube


Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity Level
Division
Operating Unit
Function

Green Book as a Base for OMB Circular No. A-123

- Office of Management and Budget (OMB) released Circular No. A-123 in July 2016
- Focuses on Management's Responsibility for Risk Management and Internal Control
- Implements the Federal Financial Managers' Financial Integrity Act (FMFIA)
- Focus is on improving accountability in Federal programs and operations

OMB Circular No. A-123

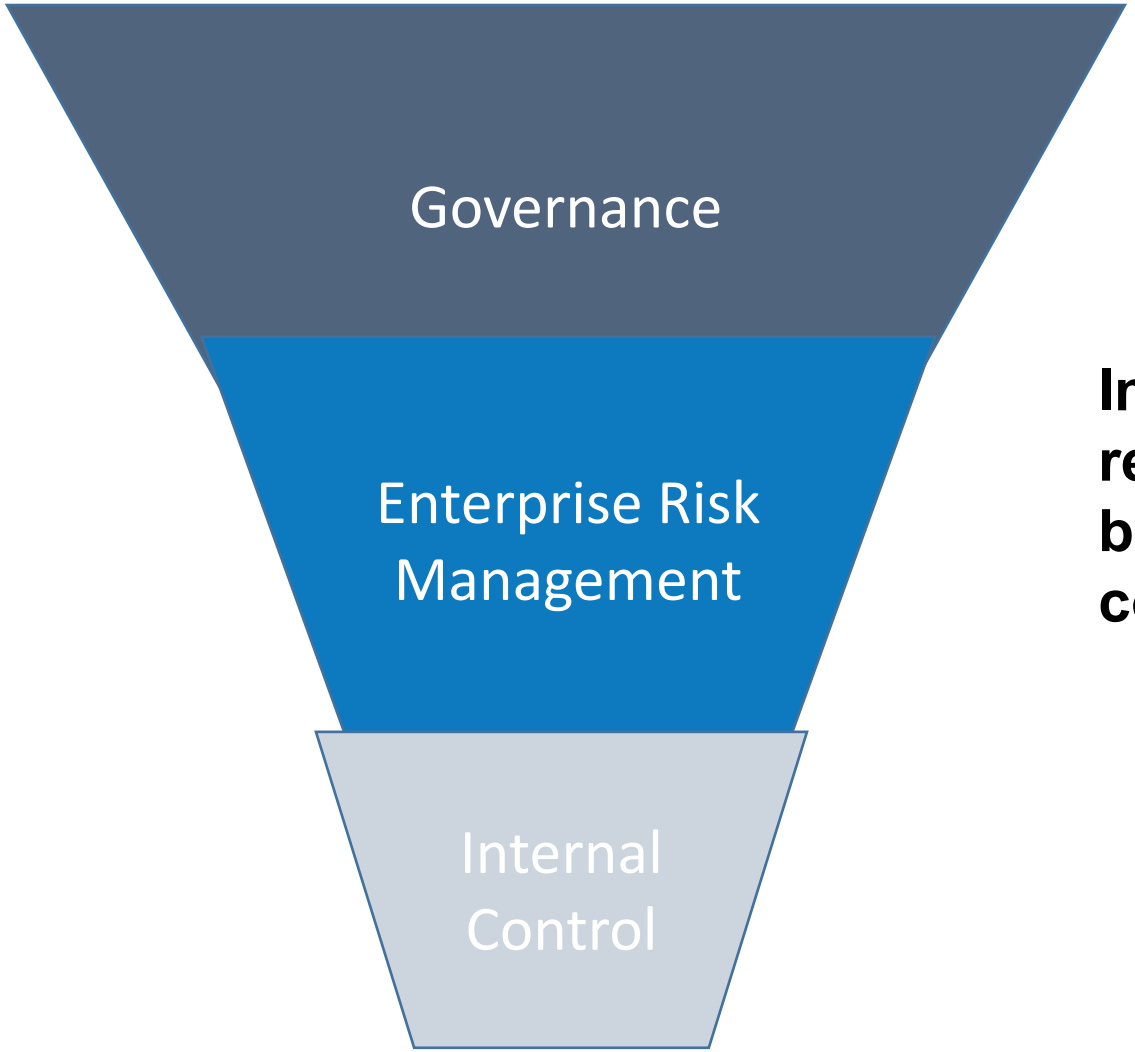
- Specifies internal control requirements
- Links with Green Book
- Agencies should follow a risk based approach to integrate and coordinate internal controls across their organization
- All agencies should establish a senior management council to implement requirements

OMB Circular No. A-123

- Focus on Enterprise Risk Management (ERM)
- All agencies are required to
  - Implement ERM
  - Develop a risk profile
- Agencies are encouraged to develop a Risk Management Council
- Focus on implementation across the agency
- Offers methods on streamlined reporting of internal control – a single assurance statement

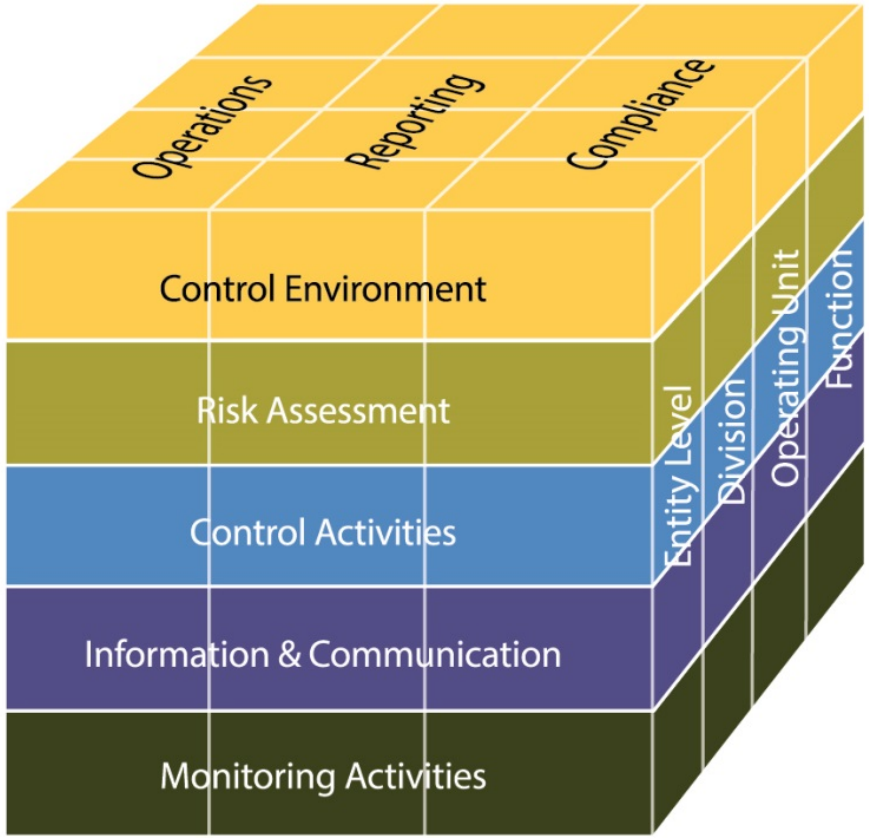
The Big Picture

Key Relationships



Important to recognize the broader concepts

COSO Cube


Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity Level
Division
Operating Unit
Function

5 Components & 17 Principles of the ICIF

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

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Relationship Between Components and Principles

COSO Relationships
Components, Principles, Points of Focus

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.

Points of Focus:
- Sets the Tone at the Top
- Establishes Standards of Conduct
- Evaluates Adherence to Standards of Conduct
- Addresses Deviations in a Timely Manner

- **Points of focus may not be suitable or relevant, and others may be identified**
- **Points of focus may facilitate designing, implementing, and conducting internal control**
- **There is *no* requirement to separately assess whether points of focus are in place**

Component - Control Environment

Principle 1

The organization demonstrates a commitment to integrity and ethical values.

Key questions…

- How would you describe the tone of organizational leaders?
- Are formal codes of conduct in place?
- How would employees describe the culture in the organization?
- When things go wrong, what actions follow?
- Are personnel evaluations consistent with expectations and cultural alignment?

Component - Control Environment

Principle 2

The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Key questions…

- Is there a governing body in place for oversight?
- If yes, do they understand and accept their oversight responsibilities?
- Is the governing body comprised of individuals with the right skills and expertise to provide oversight?

Component - Control Environment

Principle 3

Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Key questions…

- Is the entire organization considered in terms of the scope?
- Are the lines of authority clear throughout the organization from the governing body or board down to each level of management?
- Are the roles of outsourced providers clear in terms of lines of authority and the scope of their services?

Component - Control Environment

Principle 4

The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Key questions…

- Do adequate policies and procedures exist?
- Can the policies and procedures be linked to show support of objectives and strategic goals of the organization?
- How are any gaps in skill sets and competencies addressed?
- Are the right people working in the organization?
- How are personnel developed and retained?
- Are succession plans in place for members of the governing body and key personnel?

Component - Control Environment

Principle 5

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Key questions…

- How are personnel held accountable for internal control responsibilities?
- Are performance indicators or metrics linked to incentives and rewards?

Component - Control Environment

Principle 5

The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Key questions…

- Are any excessive pressures that may threaten the ability of management to accomplish organizational objectives considered?
- Are those responsible for the system of internal control evaluated?

Component - Control Environment

Principle 5 – activities and examples

- ✓Obtain sign-offs on goals mutually agreed upon with management and the board
- ✓Develop incentives that are properly linked to performance
- ✓Evaluate the appropriateness of awards
- ✓Establish clear ways to communicate the basis for rewards
- ✓Board and management periodic review of the appropriateness of incentives and rewards
- ✓Evaluate link between incentives and organizational values

Component – Risk Assessment

Principle 6

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Key questions…

How are the objectives related to:

- Operations
- External financial and non-financial reporting
- Internal financial and non-financial reporting
- Compliance

Component – Risk Assessment

Principle 7

The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Key questions…

- Are all aspects of the entity included? Subsidiary, division, operating unit, and functional levels?
- Are both internal and external factors considered?
- Are all appropriate levels of management involved?
- Have you evaluated how to estimate the significance of risks?
- Have you determined how to respond to risks?

Component – Risk Assessment

Principle 8

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Key questions…

- What are the types of fraud that can occur?
- What incentives and pressures exist that can impact fraudulent activity?
- How might you assess opportunity for fraud?
- Have you considered how inappropriate behaviors may be invoked by certain attitudes and rationalizations?

Component – Risk Assessment

Principle 8 – activities and examples

✓Look at historical fraud activities:

- Inventory theft
- Inventory shrinkage
- Whistle-blower reports
- Number of override entries
- Late reports
- Adjustment of estimates

✓Benchmark whistleblower program with supply chain and/or industry

✓Document how fraud risks are being managed

Component – Risk Assessment

Principle 9

The organization identifies and assesses changes that could significantly impact the system of internal control.

Key questions…

- What changes in the external environment may impact risk assessment?
- How may modifications to the business model assess change?
- How can changes in leadership affect our approach to risk?

Component – Risk Assessment

Principle 9 – examples and activities

Assess changes in external environment

- ✓Websites/disclosures
- ✓Social media
- ✓Newspaper clipping services
- ✓Search engines/alerts
- ✓Conferences
- ✓Professional organizations

- ✓Evaluate changes in international conditions
- ✓Preparing for leadership changes
- ✓Evaluate impact on culture after acquisitions
- ✓Evaluate impact on culture when strategic alliances are formed

5 Components & 17 Principles of the ICIF

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

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Questions/Conclusions

Thank you!

Contact:
Sandra Richtermeyer@uml.edu