A Practical Approach to Implementing the COSO Internal Control Integrated Framework

Dr. Sandra B. Richtermeyer, CPA, CMA
IMA's COSO Board Member
Professor of Accountancy & Associate Dean
Xavier University
Cincinnati, Ohio USA

Key Areas of Focus for Today's Session

- Determine how internal controls are important to the achievement of organizational mission, vision, values and strategic goals
- Identify how the COSO Internal Control Integrated Framework (ICIF) benefits for organizations of all types
- Examine the components and principles that are essential to systems of internal control
- Understand how components and principles can be applied with key questions
- Summarize the internal control systems function in an integrated manner

Who or what is COSO?

- COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission
- It all began in 1985
- First framework released in 1992, updated in 2013
- Nearly all publicly traded companies in the US use the COSO Internal Control Integrated Framework (ICIF)
- The ICIF is the most widely used internal control framework in the world

Who are the sponsoring organizations that represent COSO?

- **Five nonprofit accounting associations based in the U.S.**
- **Each association has a wide global reach**
- **Combined membership of over 600,000 professionals**
- **Each organization is viewed as a global leader in advancing accounting and finance professionals**

COSO's 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."

COSO's Fundamental Principle

Good risk management and internal control are necessary for long term success of all organizations.

What do we mean by *internal controls?*

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.

What do we mean by *risk management?*

COSO's Definition of Risk Management

"Risk management is 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."

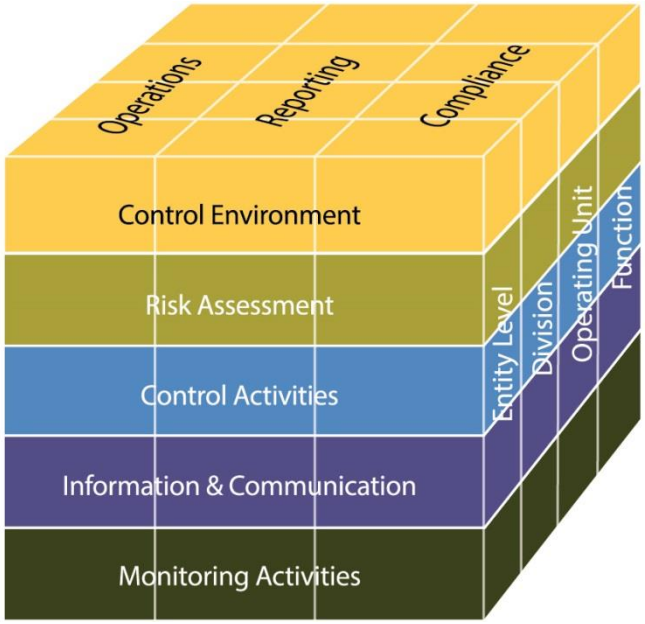
Who is responsible for internal controls and risk management?

Key Roles and Responsibilities for Internal Controls and Risk Management

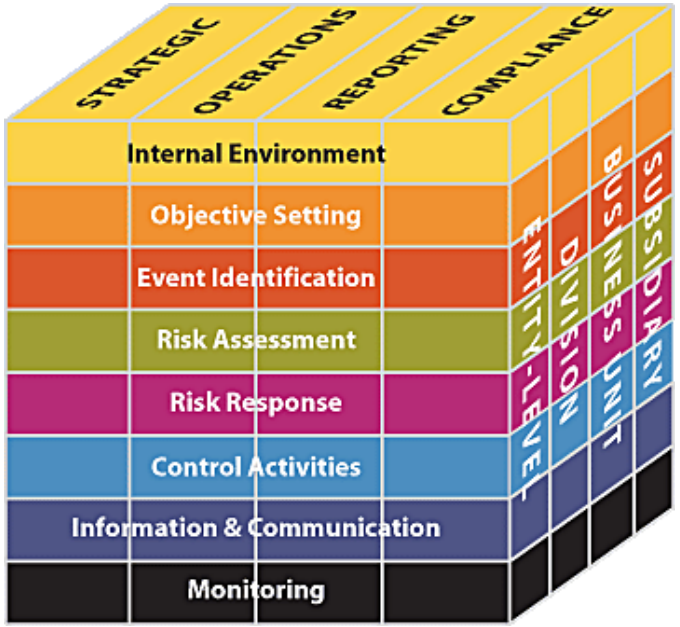
- ❑ Board of directors, board structure, board committees
- ❑ C-Suite
- ❑ Financial planning & analysis
- ❑ Risk and control personnel
- ❑ Other accounting and finance team members
- ❑ Internal and external audit
- ❑ Outsourced service providers
- ❑ Supply chain
- ❑ Legislators and regulators
- ❑ Analysts, bond rating agencies, news media, etc.

The Two COSO Frameworks

Internal Control Integrated Framework (ICIF)

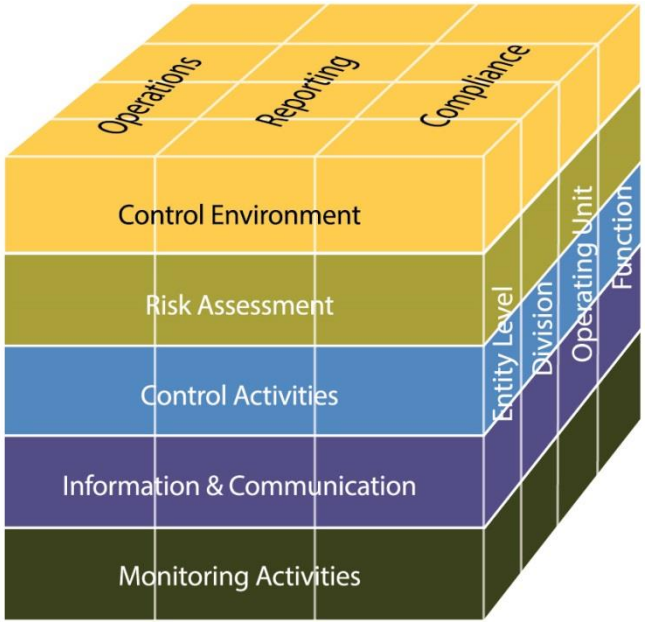


Enterprise Risk Management Framework (ERM)

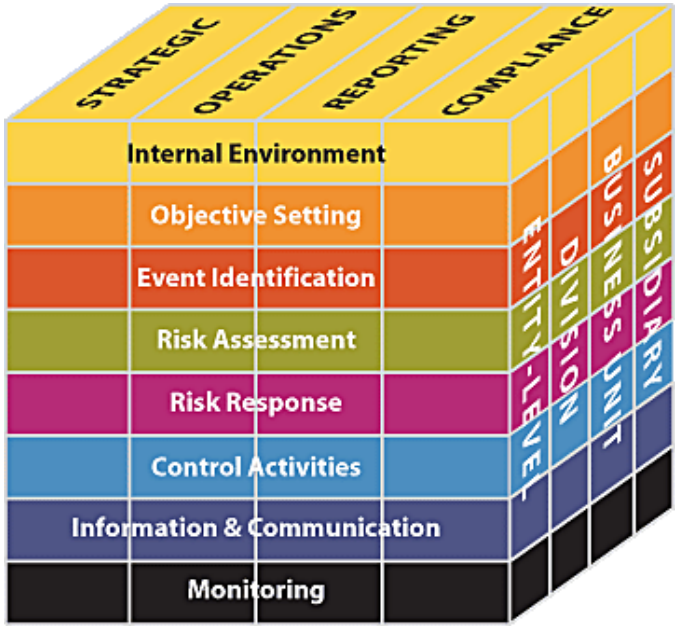


How do the Frameworks Fit Together?

Internal Control Integrated Framework



Enterprise Risk Management Framework

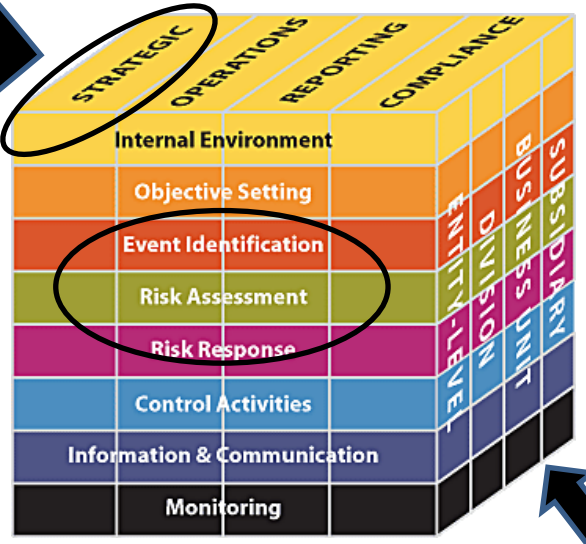


Linking the COSO Frameworks

Internal Control Integrated Framework

Strategic added to objectives

Enterprise Risk Management Framework



Risk Assessment in ICIF is Expanded into Three Components: 1) Event Identification 2) Risk Assessment and 3) Risk Response

Currently Under Renovation!

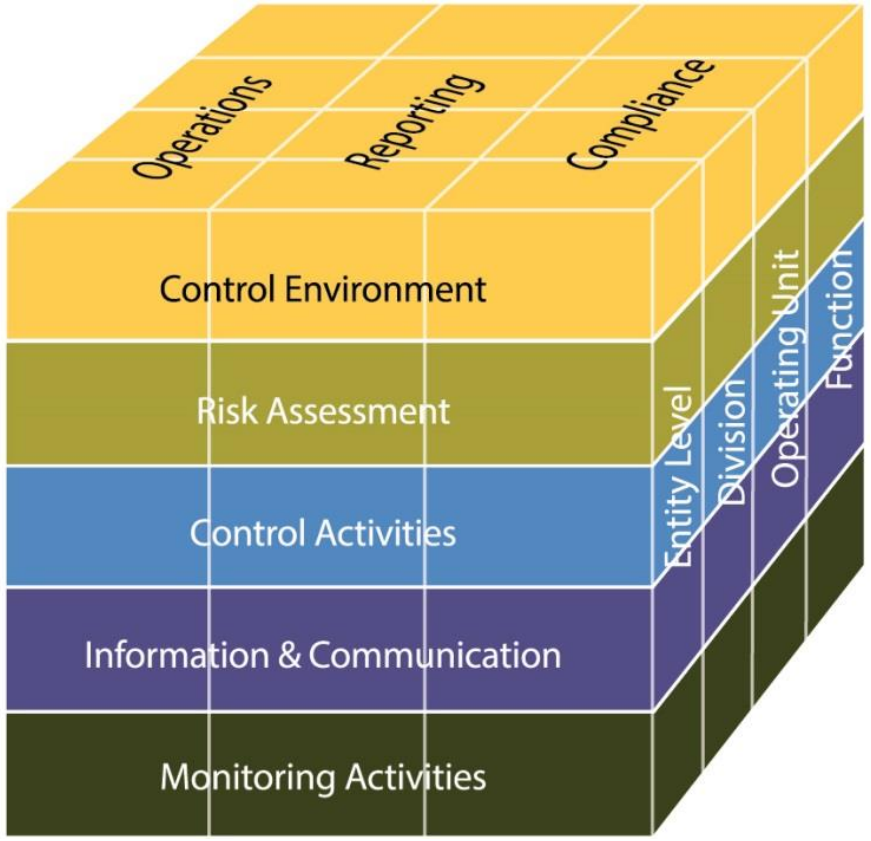
Today's Focus is on the Internal Control Integrated Framework (ICIF)

The Cube Representation of the ICIF

Objectives
Top of Cube

Entity View
Side of Cube

Components
Front of Cube



Three Types of Objectives

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

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

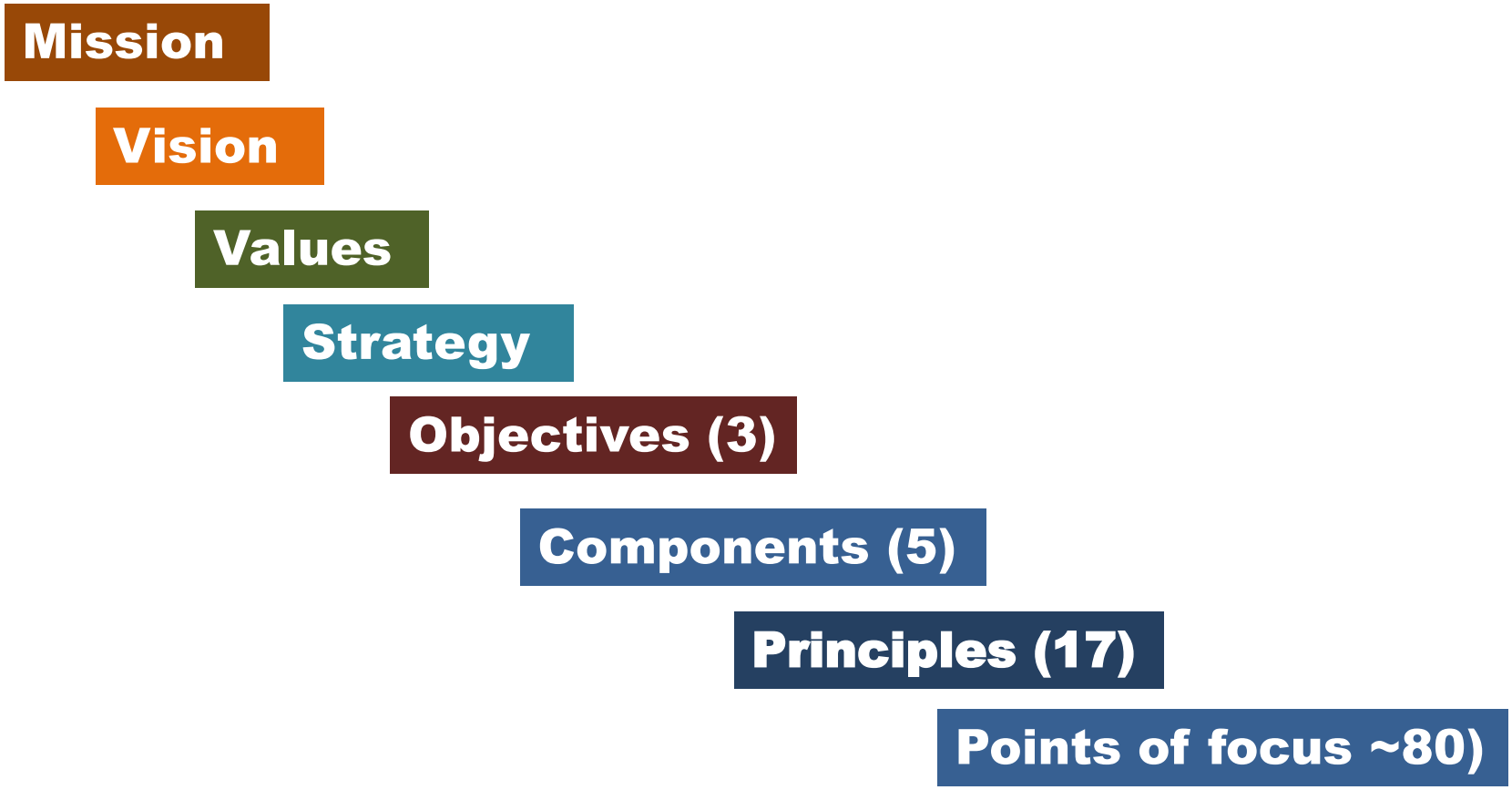
Compliance – laws, regulations

Five Types of Components

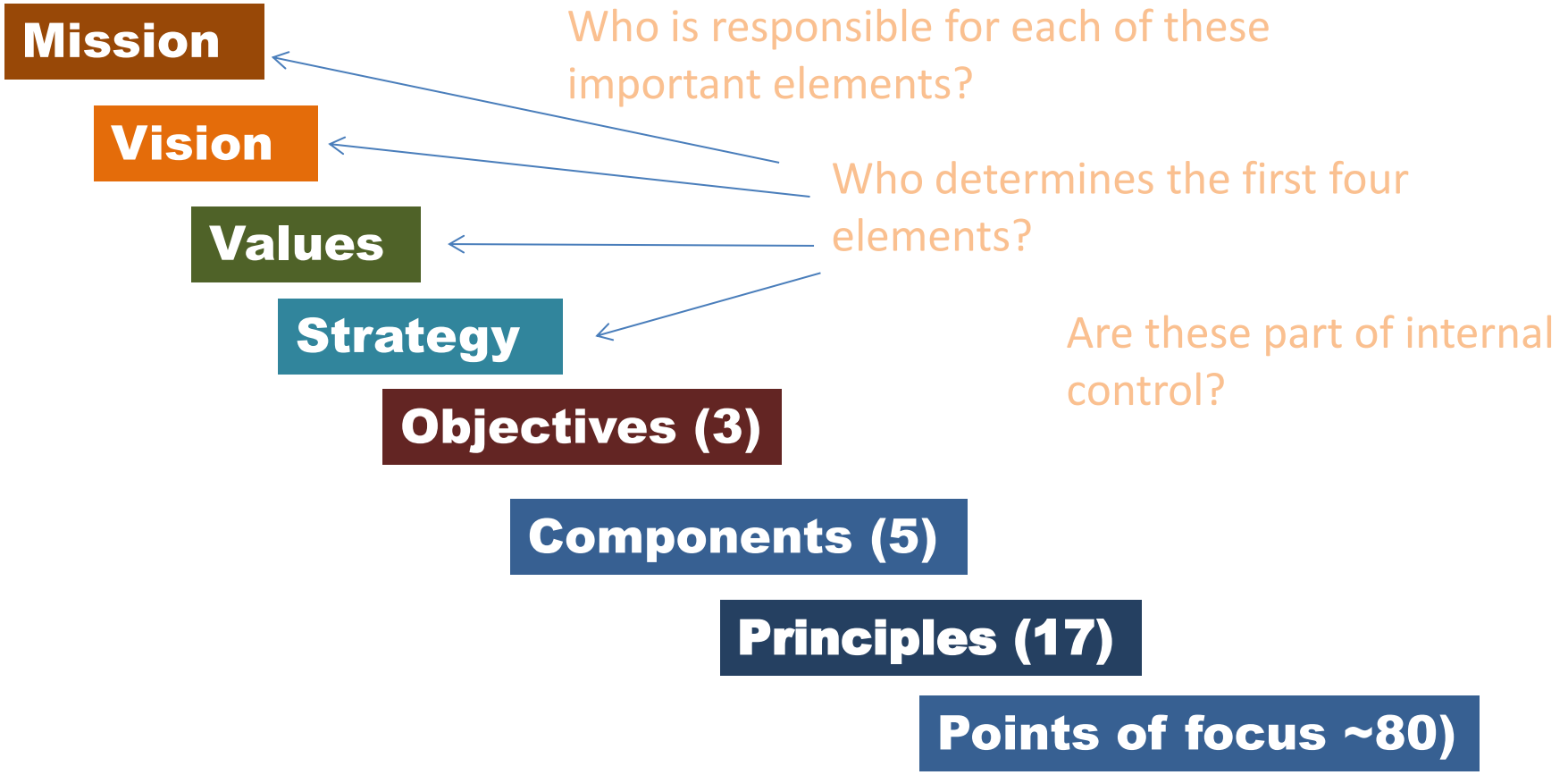
- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Each component is associated with key principles
There are 17 total principles

Linking Organization Essentials with Main Parts of the COSO ICIF



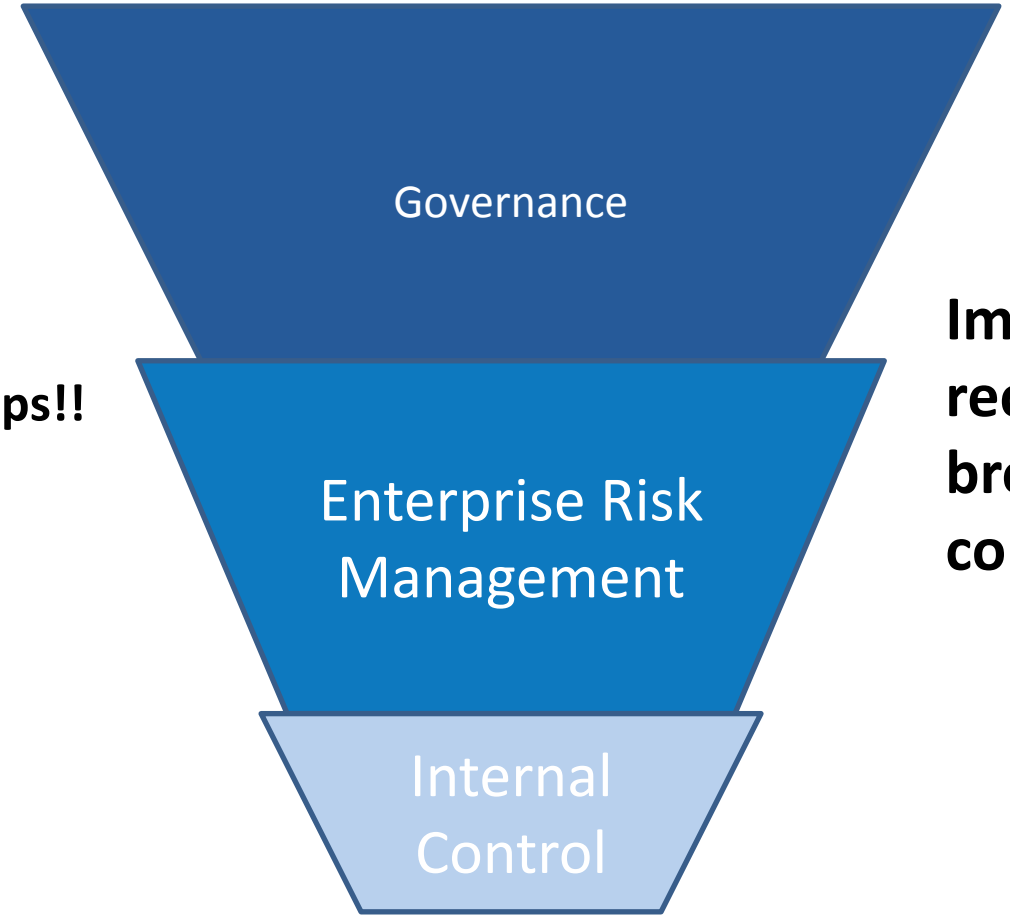
Linking Organization Essentials with Main Parts of the COSO ICIF



Setting the Backdrop: Key Organizational Elements

- Governance
- Enterprise risk management
- Internal control
- Linking organizational essentials with the COSO ICIF
- Roles and responsibilities for internal control

The Big Picture



Key Relationships!!

Important to recognize the broader concepts!!

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

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 1 – activities and examples

- ✓ Establish a set of core values
- ✓ Define and illustrate lines of communication
- ✓ Use company communications to reinforce commitment to ethics, values, integrity
- ✓ Evaluate key partners in your supply chain in terms of their ethics, values and standard of conduct
- ✓ Evaluate ethical climate throughout the organization
- ✓ Evaluate how you take action when deviations occur

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 2 – activities and examples

- ✓ Review the descriptions of board committees
- ✓ Review roles and responsibilities for board members
- ✓ Prepare formal criteria for evaluation of board candidates (identifying new, assessing existing directors)
- ✓ Document activities of audit committee
- ✓ Establish policies and practices for communication between board and management
- ✓ Establish policies and practices for communication between levels of management
- ✓ Create a meetings calendar (and a meeting budget)
- ✓ Operates independently
- ✓ Provides oversight for the system of internal control

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 3 – activities and examples

- ✓ Evaluate lines of authority
- ✓ Consider how representative your org chart is in terms of reality
- ✓ Look at organizational hierarchy in terms of relevance and appropriate segregation of duties
- ✓ Create (or review) an authority and approval matrix
- ✓ Link roles and responsibilities with key strategic goals and objectives
- ✓ Evaluate agreements with your supply chain partners and/or outside service providers

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 4 – activities and examples

- ✓ Determine a calendar for policy review
- ✓ Link competency standards to hiring, training and retention activities
- ✓ Look for gaps in knowledge, skills and expertise
- ✓ Define performance expectations
- ✓ Create a training plan
- ✓ Evaluate your ability to implement complex regulations, accounting standards, tax matters
- ✓ Review (or create) succession plan

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

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

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 6 – activities and examples

- ✓ Assess materiality for financial statements
- ✓ Review financial accounting policies against standards (GAAP or IFRS)
- ✓ Review internal accounting reporting policies
- ✓ Benchmark policies with peer groups or supply chain partners, strategic partners
- ✓ Review all aspects or ranges of business and consider how they are represented in reports

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 7 – activities and examples

- ✓ Assess and link risk to significant financial statement accounts

Impact on financial statements

Character of accounts

Link accounts to business processes

Examine fraud risk

Evaluate account across entity

- ✓ Analyze risk across functions
- ✓ Create a risk identification and analysis matrix
- ✓ Rate processes or accounts by risk categories (high medium, low)
- ✓ Establish meeting schedule between accounting and finance personnel and leaders in other functional areas
- ✓ Create plan of analysis of technology risk
- ✓ Create benchmarks to address significance and response to risk

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

Component – Control Activities

Principle 10

The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Key questions…

- How do control activities integrate with risk assessment?
- Have entity-specific factors been appropriately considered?
- Has management determined how internal control activities affect relevant business processes?
- Have a mix of control activity types been considered?
- How have you considered how control activities affect various levels of the organization?
- How may segregation of duties be important?

Component – Control Activities

Principle 10 – activities and examples

- ✓ Use a workshop to link risks to control activities
- ✓ Create and/or maintain a risk and controls matrix
- ✓ Evaluate controls in outsourced
- ✓ Evaluate preventive vs. detective controls
- ✓ Control and evaluate the use of estimates
- ✓ Develop plans when adequate segregation of duties is not possible

Component – Control Activities

Principle 11

The organization selects and develops general control activities over technology to support the achievement of objectives.

Key questions…

- How can you evaluate the dependency between the use of technology in business processes and technology general controls?

Component – Control Activities

Principle 11- activities and examples

- ✓ Use walkthroughs to gain understanding of technology dependencies
- ✓ Evaluate use of spreadsheets
- ✓ Compare enterprise system capability with off-system activities
- ✓ Examine technology access controls
- ✓ Manage changes or customizations to purchased software
- ✓ Manage changes or customizations to internally developed software
- ✓ Create a plan for software upgrades

Component – Control Activities

Principle 12

The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Key questions…

- Have policies and procedures to support deployment of management's directives been established?
- Is authority for executing policies and procedures clear?
- Are control activities performed in a timely manner?
- Do those responsible takes corrective action when necessary?
- Are control activities overseen performed by competent personnel?
- Are policies and procedures reassessed as appropriate?

Component – Control Activities

Principle 12 - activities and examples

- ✓ Develop documentation policies and procedures
- ✓ Use templates to or standards for documentation
- ✓ Establish responsibilities for reviewing internal financial statements
- ✓ Create a deployment plan with business unit leaders for internal control activities and policy review
- ✓ Regularly assess policies and procedures
- ✓ Evaluate corrective actions

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

Component – Information & Communication

Principle 13

The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Key questions…

- Have you identified key information requirements?
- Have internal and external sources of data been captured?
- Has relevant data been processed into information?
- Has quality been maintained throughout processing?
- What are the costs vs. benefits?

Component – Information & Communication

Principle 14

The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Key questions…

- Is a process in place to communicates internal control information?
- How is this communicated to the governing body or board of directors?
- Are separate lines of communication available?
- How have relevant methods of communication been determined?

Component – Information & Communication

Principle 14 – activities and examples

- ✓ Developing guidelines for communications to board of directors
- ✓ Evaluate technology used to supply information to board of directors
- ✓ Communicating activities of whistleblower and ethics hotlines to employees
- ✓ Evaluate the need for cross-functional teams
- ✓ Establish a cross-functional internal control committee
- ✓ Create a mentoring program

Component – Information & Communication

Principle 15

The organization communicates with external parties regarding matters affecting the functioning of internal control.

Key questions…

How does the organization

- Communicate to external parties?
- Enable inbound communications?
- Communicate with the board of directors?
- Provide separate communication lines?
- Select relevant methods of communication?

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

Component – Monitoring Activities

Principle 16

The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Key questions…

How does the organization…

- Consider a mix of ongoing and separate evaluations?
- Consider a rate of change?
- Establish a baseline understanding?
- Use knowledgeable personnel?
- Integrate with business processes?
- Adjust scope and frequency?
- Objectively evaluate?

Component – Monitoring Activities

Principle 17

The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Key questions…

- How are results of deficiencies assessed?
- Ho are deficiencies communicated?
- How does management and relevant personnel monitor corrective actions?

Now what?

- We’ve reviewed the basic elements of the Framework
  - Questions?
  - Concerns?
- What should you do next?
- Roles and responsibilities to enable a healthy system of internal control
- Conclusion and wrap-up

Suggested Next Steps

- Read, understand, and train others
- Meet with your audit team
- Take 17 **Principles** inventory
- Map your controls to **Principles**, consider **Points of Focus**
- Evaluate results and plan change
- Meet with your audit firm again
- Execute the transition plan, monitor change

Questions?

Thank you!

My contact information:
richtermeyer@xavier.edu

The following slides are meant to be helpful after you get back to the office and dig deeper into internal controls and risk management.

Important Items to Emphasize Regarding Definition of Internal Control

- Geared to accomplishing objectives in one or more separate but overlapping categories – operations, reporting and compliance
- A process that includes ongoing tasks and activities – it is a means to an end, not an end to itself
- Effected by people (not affected)…internal control isn't just about policy and procedure manuals – culture is key!
- Able to provide reasonable assurance – keep in mind the word reasonable – not absolute!
- Adaptable to the entity structure – it is important that it is able to apply across the entire organization, not just certain departments, divisions or locations.

What are the **limitations** of internal control systems?

- Are the objectives that drive the system of internal control appropriate?
- Humans are involved and we are inherently prone to error
- Breakdowns can occur due to failure and error
- Management can override internal control
- Management, other personnel or external parties can break down the system individually or in a collusive manner
- External events that are beyond the organization's control may occur at any time

What is **Effective** Internal Control?

- An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective relating to one, two or all three categories (operations, reporting, compliance). It requires that:
- Each of the five components on internal control and relevant principles is present and functioning
- The five components are operating together in an integrated manner

What is **present and functioning**?

- Present – the components and relevant principles exist in the system of internal control
- Functioning – the components and relevant principles continue to work in the system of internal control to achieve the organization's objectives

What do we mean by **operating together**?

- The concept of integration in the application of the COSO ICIF is important!
- The components must work together in an integrated manner. All five components, working together, have an important role to play in terms of reducing the risk of not achieving an objective.
- The components are interdependent
- If components are not present and functioning, then they can't be working together in an integrative manner!

What are **deficiencies** in a system of internal control?

- A deficiency in general – a component(s) and relevant principle(s) has shortcomings that reduce the likelihood of an organization achieving its objectives.
- A major deficiency – the likelihood that an organization will achieve its objectives is severely reduced.
- If a major deficiency exists, the organization cannot conclude that it has an effective system of internal control.
- If management determines that a component and one or more relevant principles are not present and functioning and working together → major deficiency.

Please check out the many free resources provided by COSO including an executive summary of the COSO Framework

www.coso.org

Also www.imanet.org