Internal Controls to Assist with Anti-Corruption

Dr. Sandra B. Richtermeyer
Dean, Manning School of Business
University of Massachusetts Lowell

Use of COSO & 3 Lines of Defense Model

Full implementation of the COSO model helps with the following efforts to:

- Increase transparency
- Support efforts to improve organizational culture
- Implementation of management models
- More clearly define lines of authority
- Clarify roles and responsibilities
- Comply with laws, regulations and policies

Use of COSO & 3 Lines of Defense Model

Full implementation of the COSO model helps with the following efforts to:

- Balance expertise with roles and responsibilities
- Training
- Sharing of information and best practices
- Improve operational efficiencies
- Enable technology to assist with fraud detection

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.

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.

Emphasis on Responsibilities

We must remind our stakeholders, leaders and decision makers 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.

Key Roles and Responsibilities for Internal Controls and Risk Management

3 Lines of Defense Model

COSO Frameworks assist with Lines of Defense Implementation

- **1st Line of Defense** - operational management

- Focus on the "front-line" and process owners

- Roles and responsibilities

  - Distinguish procedures from controls

  - Implement controls and procedures for day-to-day risk management

  - Supervise the execution of the controls and procedures

3 Lines of Defense Model

COSO Frameworks assist with Lines of Defense implementation

- **2nd Line of Defense** – functions that oversee or specialize in areas such as risk management, compliance, informational security

- Roles and responsibilities
    - Review policies and procedures
    - Analyze segregation of duties
    - Review user access and revisions to access
    - Analyze requests for special privileges or use cases
    - Review requests for termination processes or new processes
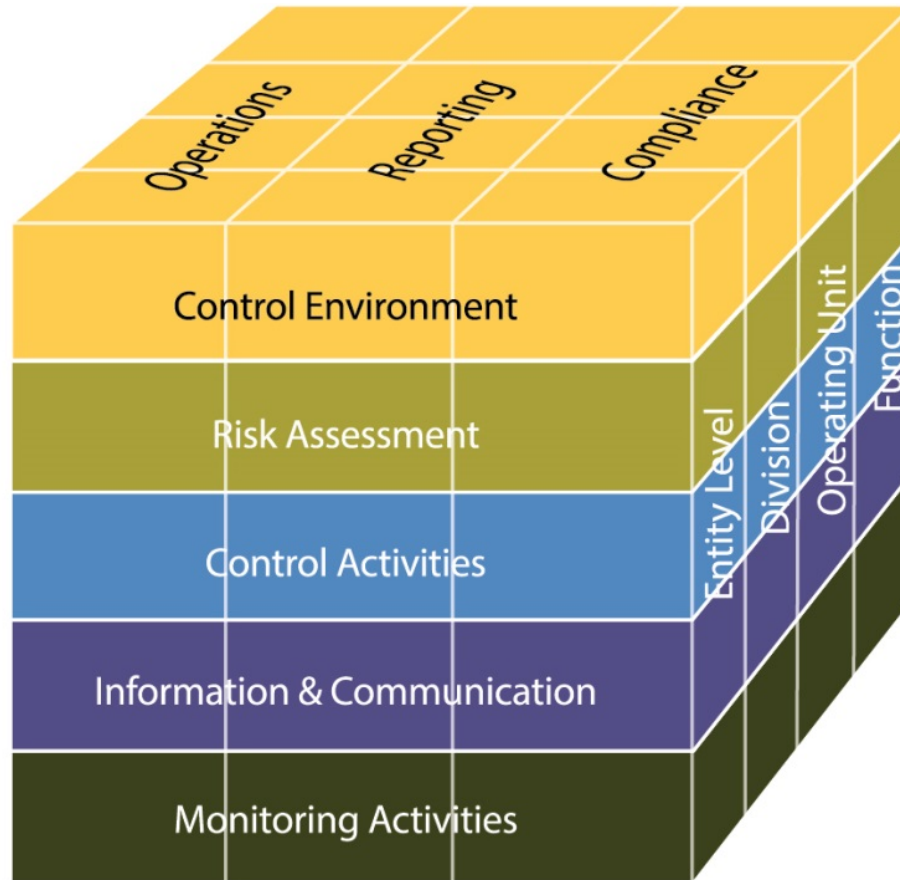
3 Lines of Defense Model

COSO Frameworks assist with Lines of Defense implementation

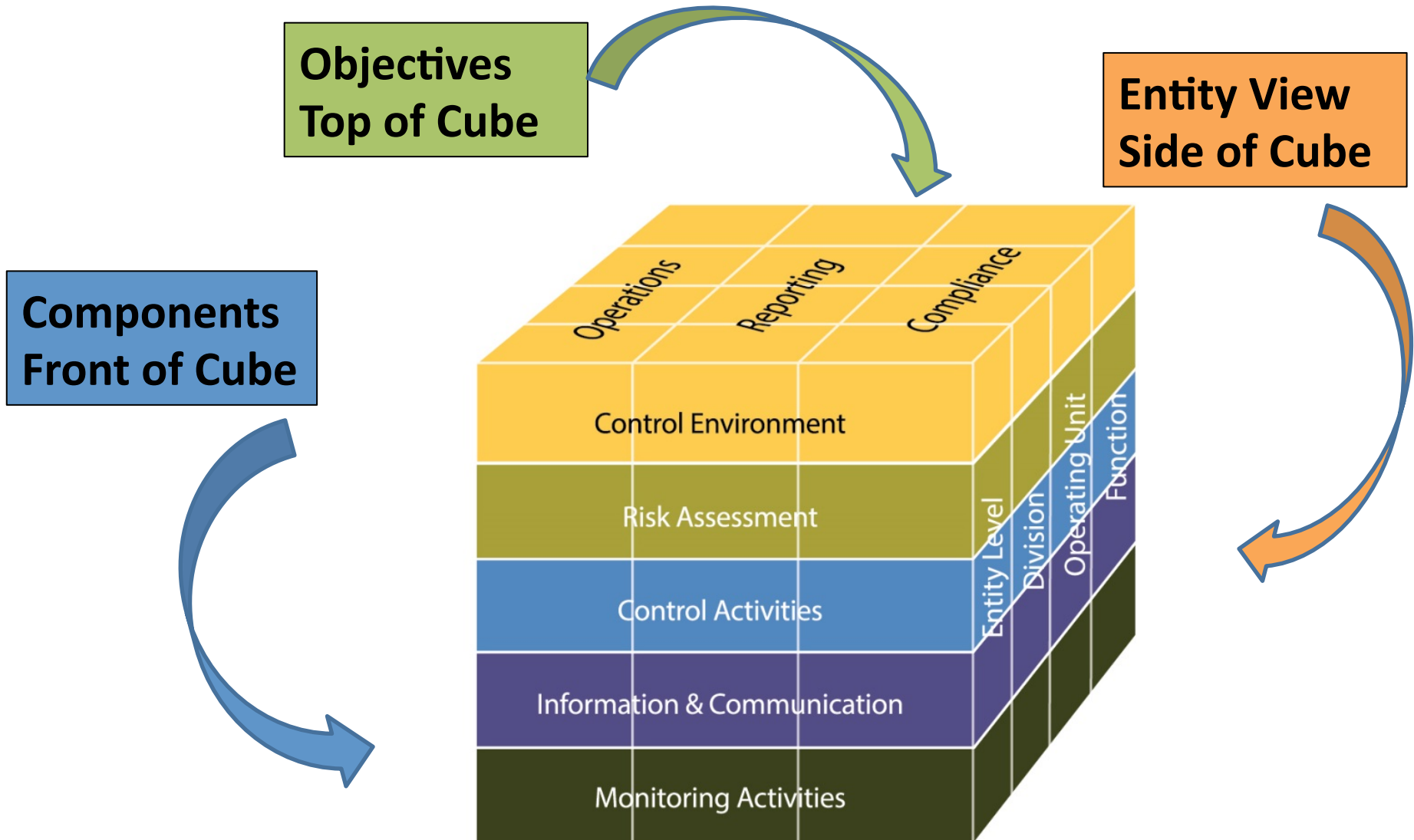**3rd Line of Defense** – internal audit function

Reporting to senior management or a governing body on items such as

- Effectiveness of operations
- All parts of risk management and internal control framework or model
- Overall organization and all operating units

COSO Internal Control Integrated Framework

Key Parts of Internal Control Framework

Objectives
Top of Cube

Entity View
Side of Cube

Components
Front of Cube

Operations

Reporting

Compliance

Control Environment

Risk Assessment

Control Activities

Information & Communication

Monitoring Activities

Entity Level

Division

Operating Unit

Function

COSO Enterprise Risk Management Framework
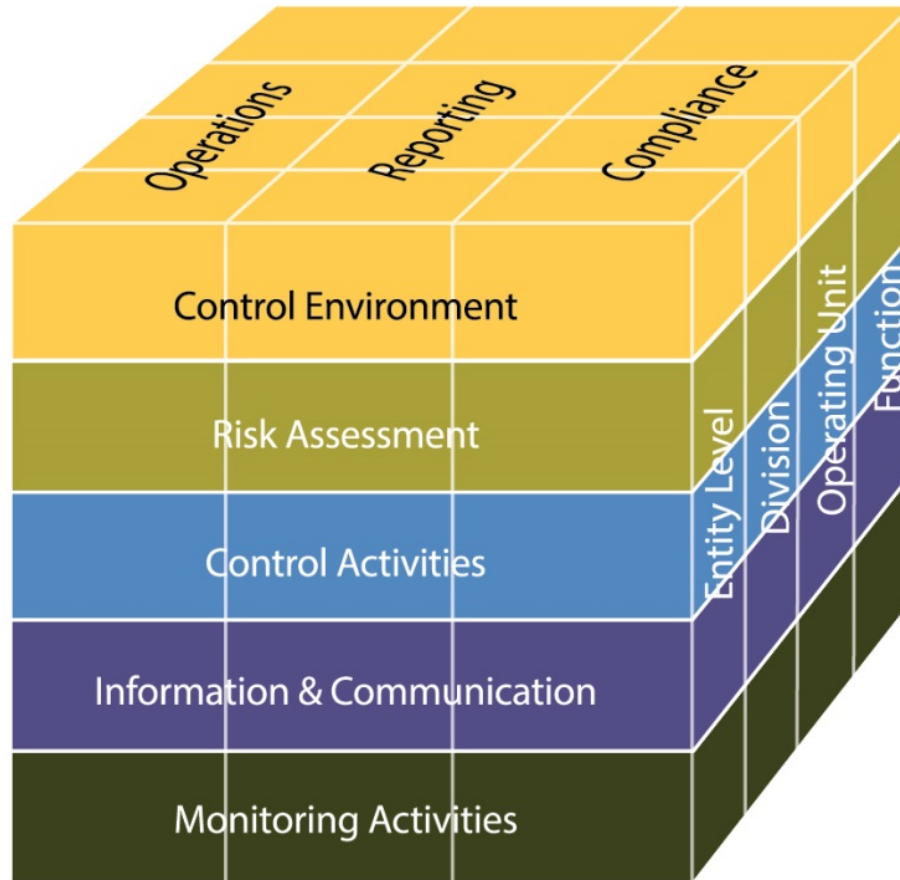
COSO ERM Focus

Reminder on Order of Key Relationships

Governance

Risk Management

Internal Control

COSO Internal Control Integrated Framework

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
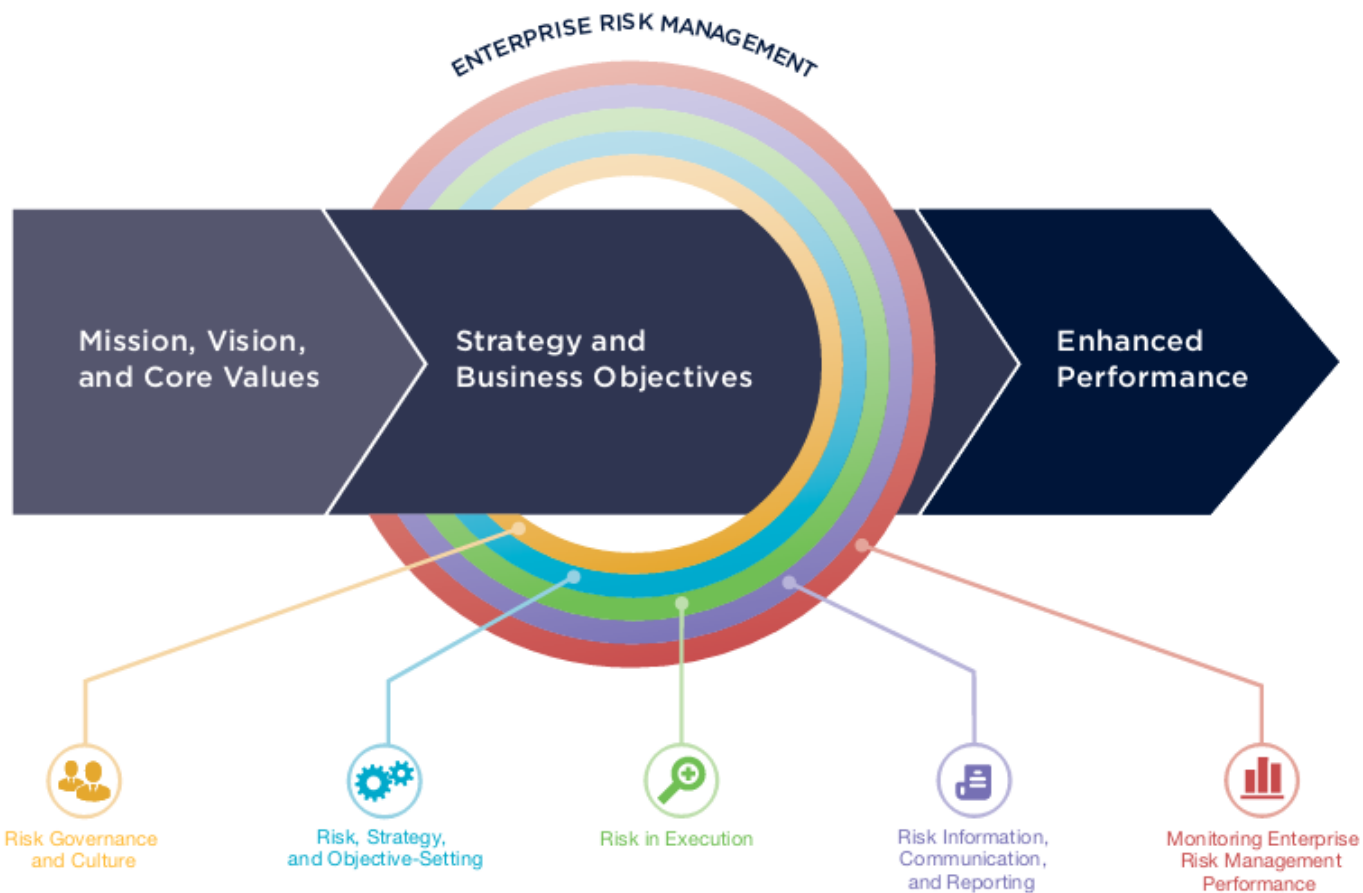12. Deploys through policies and procedures

Information & Communication

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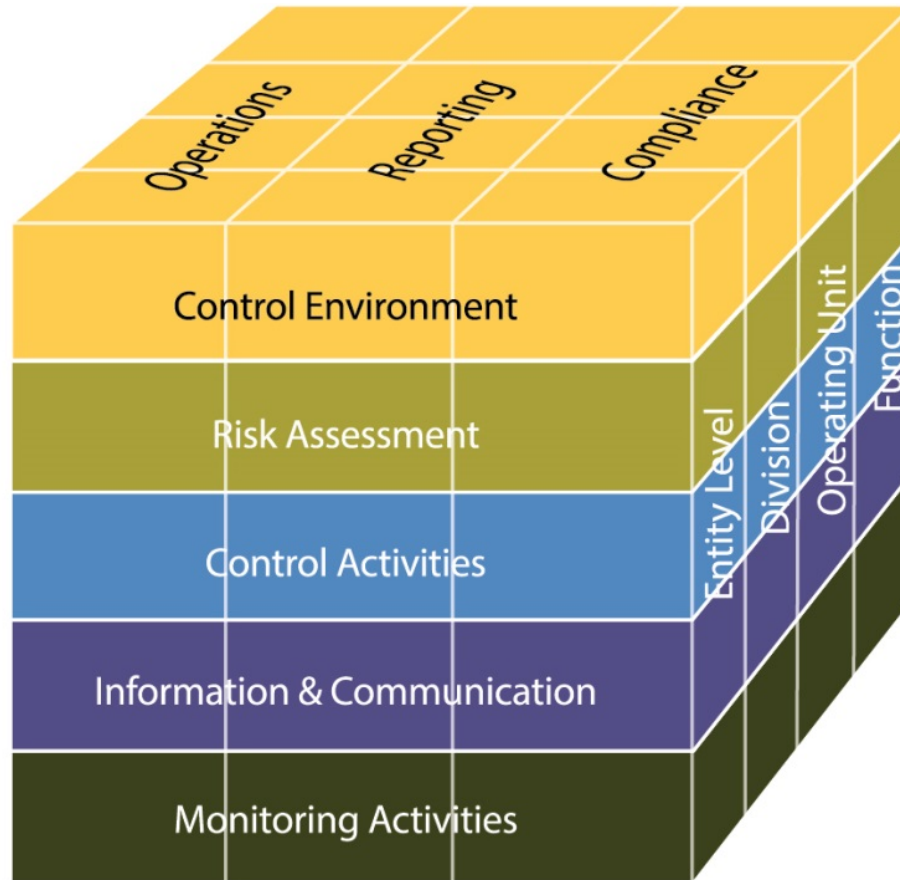14. Communicates internally
15. Communicates externally

Monitoring Activities

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

COSO ERM 2017

COSO Internal Control Integrated Framework

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

Thank you!

My contact information:
Sandra_Richtermeyer@uml.edu