Internal Controls

Agenda:

- Basics of Internal Controls – what are they?
- COSO framework
- Practical applications to your current processes

Created: February 2014
Updated: April 2023

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Internal Control Basics

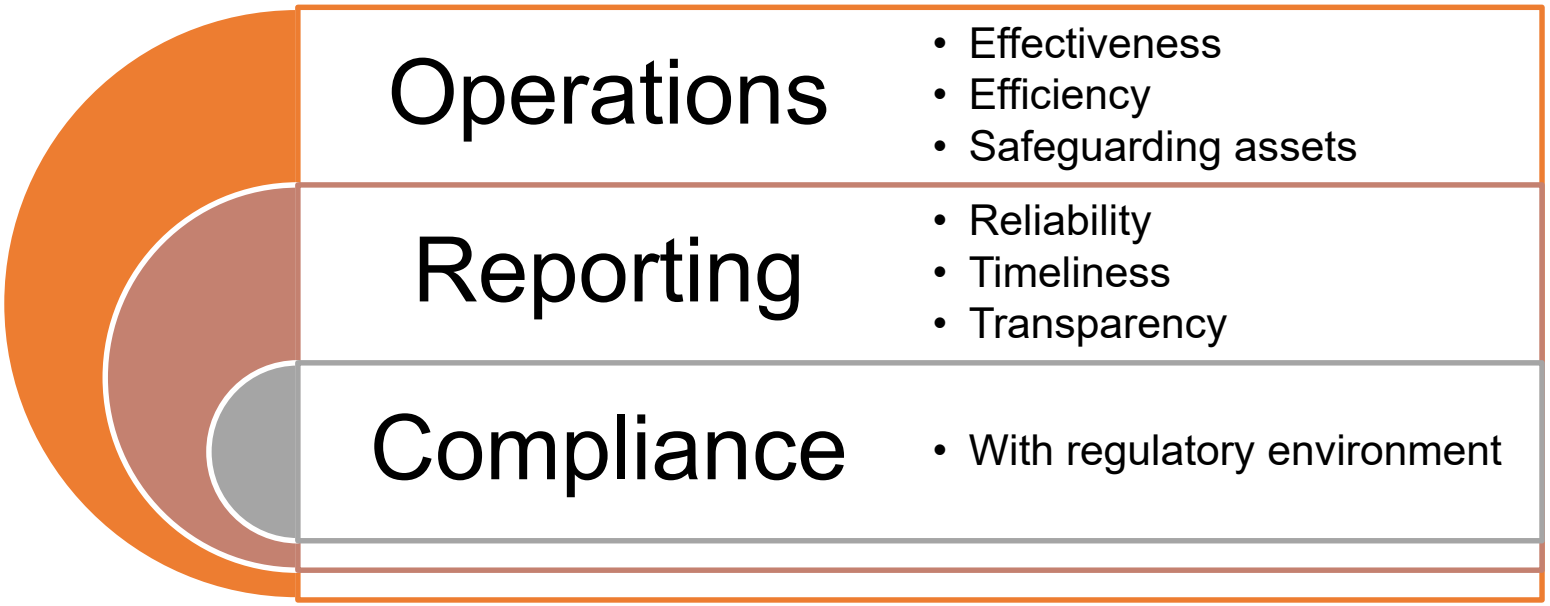
What are internal controls?

Connect


Objectives
What are you trying to achieve?
What might thwart our efforts?
Risks
Controls
How can we manage risk?

Internal Control

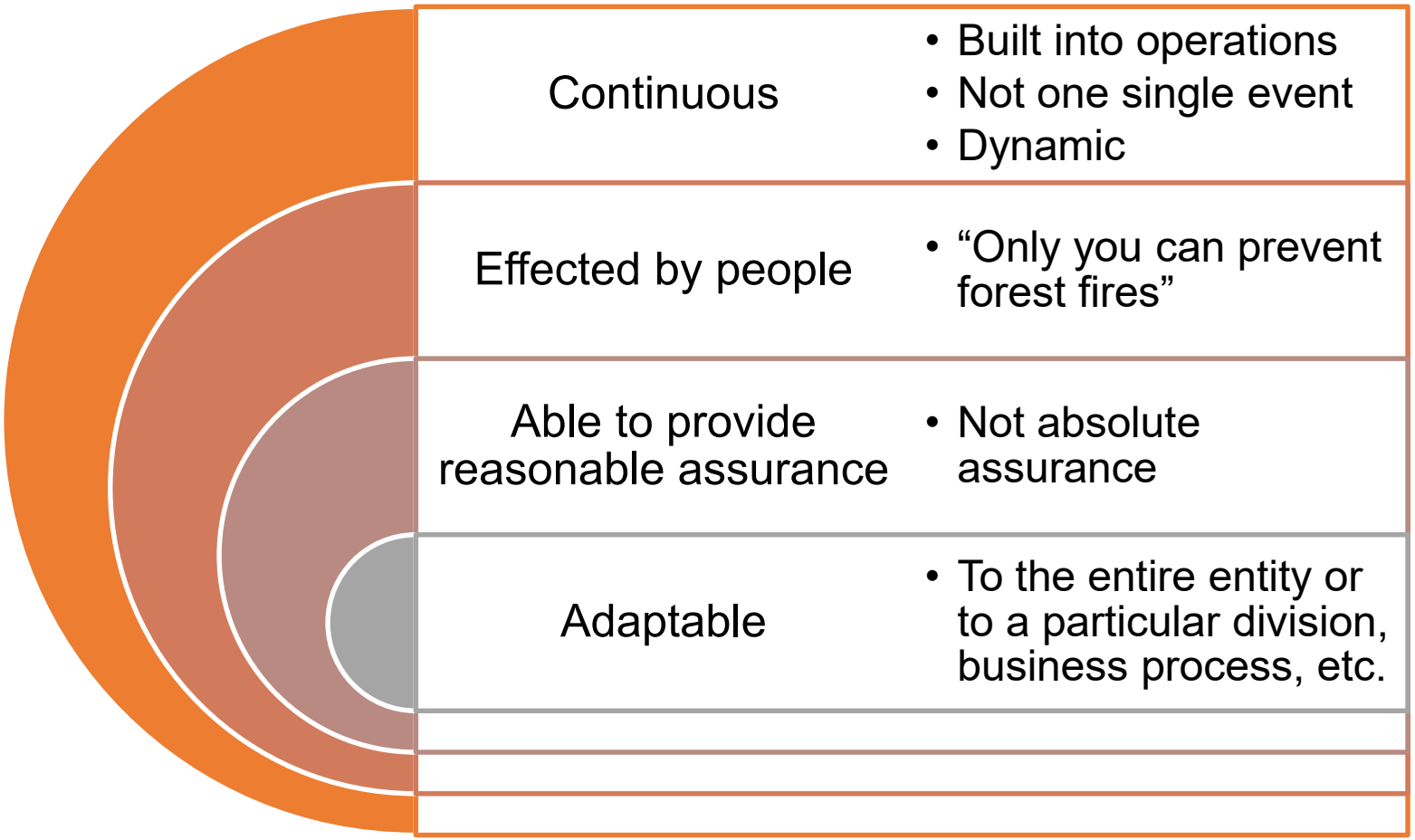
INTERNAL CONTROL is a ***process***, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to:



Management has a fundamental responsibility to develop and maintain effective internal control.

Internal Control

INTERNAL CONTROLS are



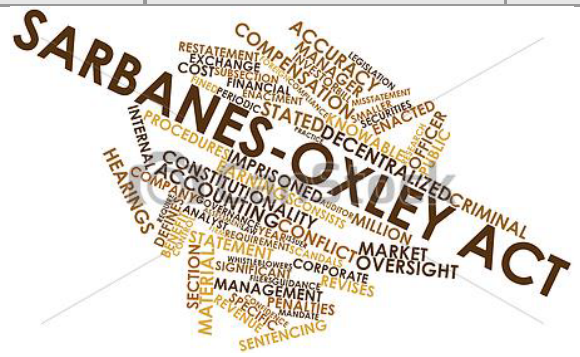
Risks of Weak Internal Controls

- Financial misstatements
- Business loss
- Loss of funds or materials
- Incorrect or untimely management information
- Fraud or collusion
- Tarnished reputation with the public
- Program Sustainability compromised
- Missed goals

COSO Framework

What are the five integrated components of internal control?

WorldCom CHARGE SHEET		
Count I	Securities Fraud Conspiracy	Guilty
Count 2	Securities Fraud	Guilty
Count 3-9 (7 counts)	False Filing With the SEC	Guilty



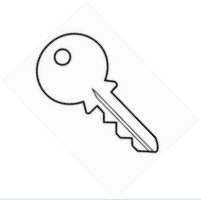
UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Updated COSO Framework

- Reflective of the current environment

- Applicable to more business objectives
  - Integrated approach to addressing organization-wide objectives

- Flexible and customizable
  - **Principles-based** rather than Rules-based
  - 17 principles – formalize fundamental concepts to help
    - Specify objectives
    - Assess risks
    - Deploy controls
  - Designed to help address objectives across the organization
    - E.g., addressing financial reporting fraud might help address compliance objectives

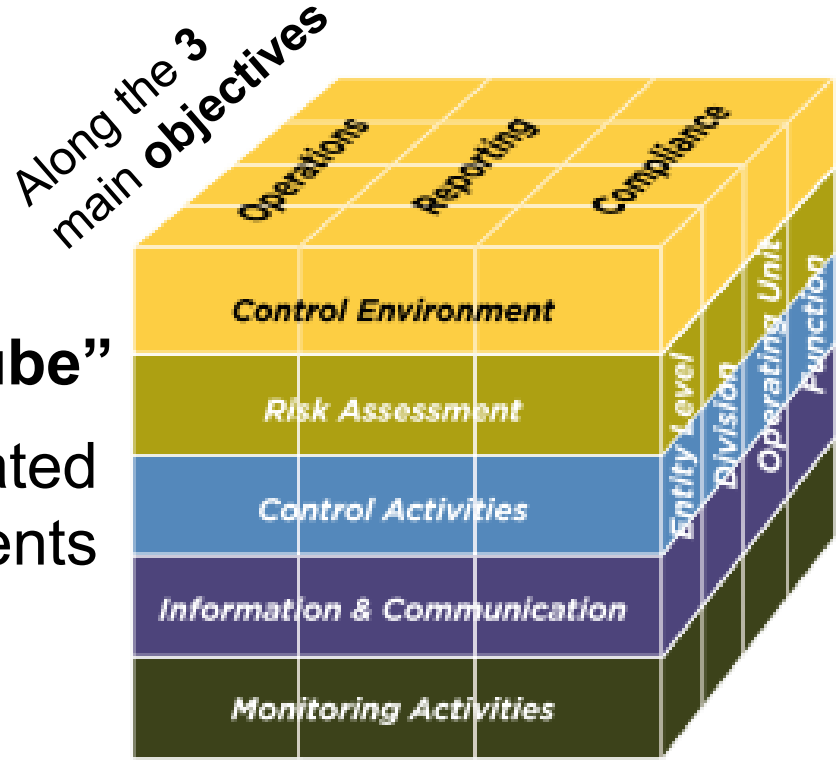


Key: Ramp it up in the "right" areas
- How to define right areas? Risk assessment.

Updated COSO Framework

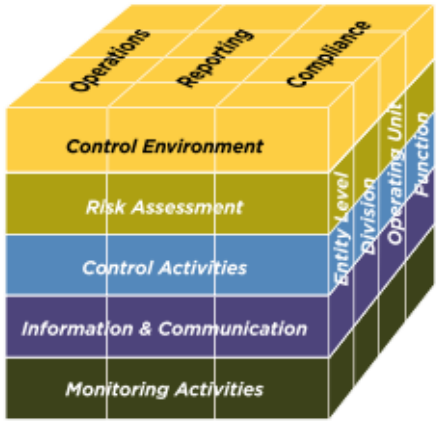
The COSO "cube"

5 integrated components



At **all** levels of the organization

COSO cube – 5 Integrated Components



1. Control Environment

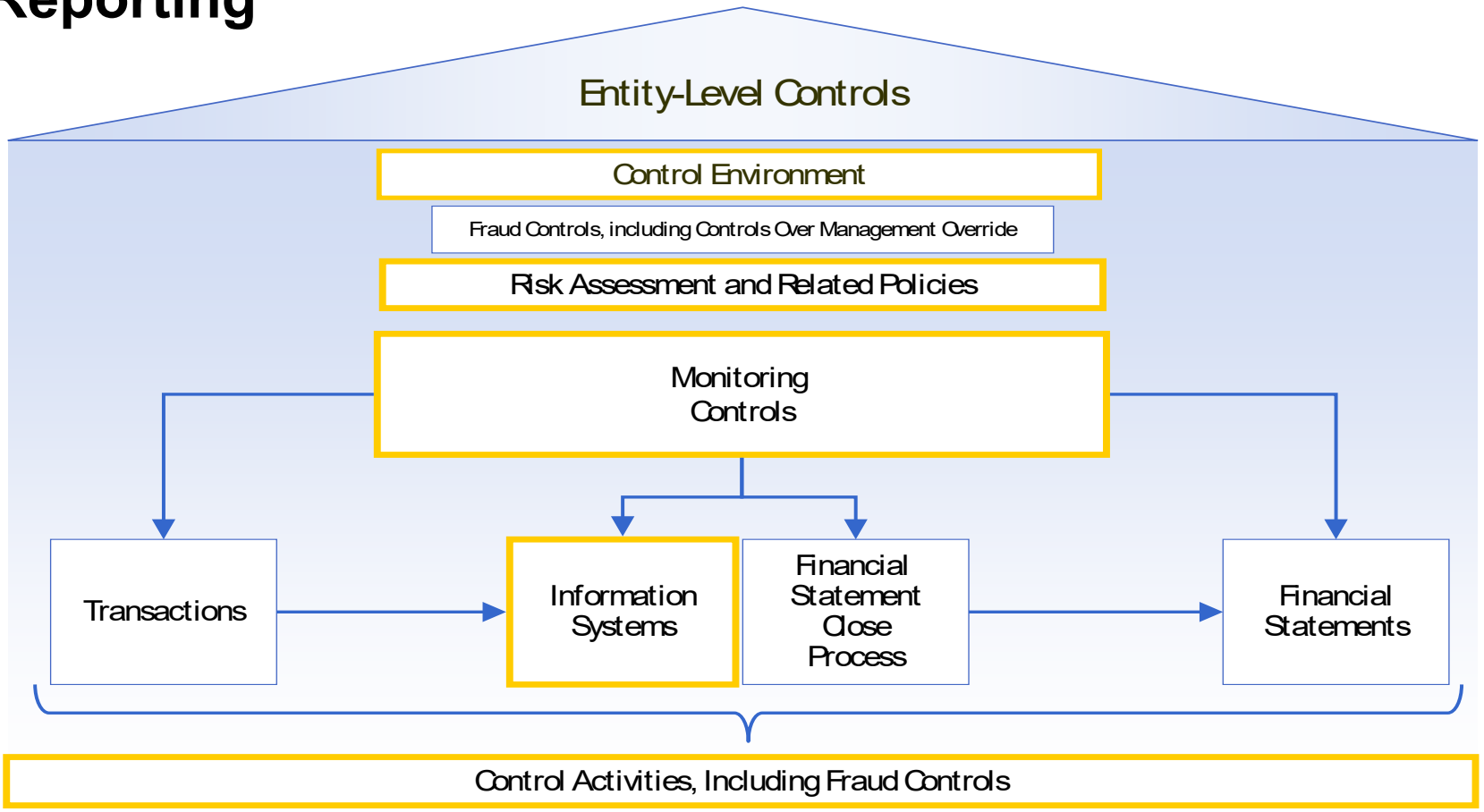
- The set of standards, processes, and structures that provide the basis for carrying out internal control
- Comprises integrity and ethical values of the organization

- The Board and Senior Management - **and you**!
  - Establish **tone at the top**
  - Establish expected standards of conduct and reinforce expectations
- Parameters enable the Board to carry out its governance oversight responsibilities

- University tone at the top: Policy 804, Standards of Ethical Conduct

COSO cube – 5 Integrated Components

Control Environment for Financial Reporting



UNIVERSITY OF NORTH CAROLINA CHARLOTTE

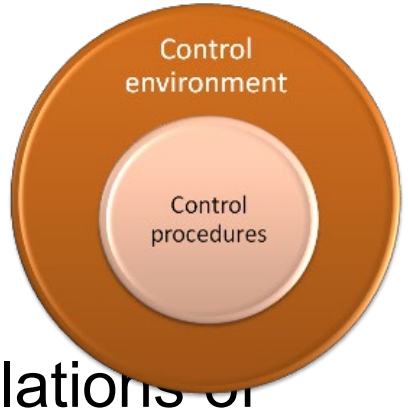
COSO cube – 5 Integrated Components

The **Control Environment** should ensure controls are in place, covering areas such as:

- Hiring practices
- Training programs
- Whistleblower policies
- Code of **Ethics**
- Clear lines of responsibility and authority
- Etc.

As part of our regular business processes, we should continually monitor and update the Control Environment for dynamic changes

COSO cube – 5 Integrated Components



Difference between
Compliance v. Integrity Strategy:

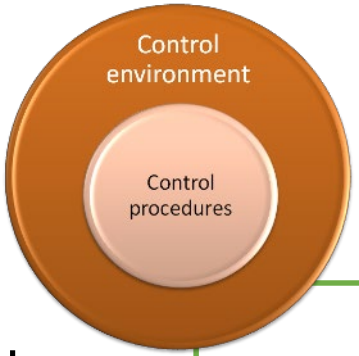
A **'Compliance Strategy'** tries to prevent violations of regulations and self-interested behavior by employees by imposing standards of conduct that are intended to compel acceptable behavior.

An **'Integrity Strategy'** seeks to create conditions that support right action by communicating the values and vision of the organization, aligning the standards of employees with those of the organization, and relying on the whole management team, not just lawyers and compliance officers.

COSO cube – 5 Integrated Components

The **Control Environment** should be documented:

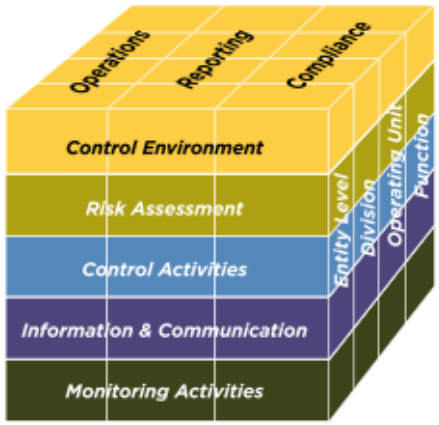
- **Process documentation/ controls**
  - Determine extent of existing documentation; leverage this
  - Create new if no documentation exists
  - Update for changes in operations



Types of documentation that can be used:

- Process Narratives
- Organizational charts
- Flowcharts
- Questionnaires
- Memorandums
- Checklists

COSO cube – 5 Integrated Components



2. Risk Assessment

- Involves a dynamic and iterative process for identifying and assessing risks
- Risk: the possibility that an event will occur and adversely affect the achievement of objectives.

- The Board and Senior Management (and you!)
  - Establish **objectives** linked at different levels of the entity
    - Must take holistic approach – look at the full organization
    - Apply internal control to achieve multiple objectives
      - Prevent domino effects, e.g., weakness in financial reporting that jeopardizes operations
  - Establish risk tolerances

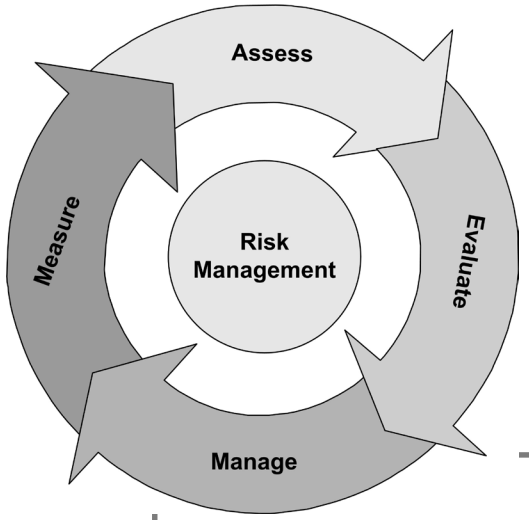
- Increasingly important when resources are constrained

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

COSO cube – 5 Integrated Components

Risk Management

A **process** applied in a strategic setting and across the entity, designed to identify and **manage risks to stay within risk appetite/tolerance level**, to provide reasonable assurance about achieving entity goals and objectives.



Risk Assessment

An **element of internal control** within the risk management process that enables management to identify and assess key risks to achieving its objectives; this **forms the basis on which control activities are determined**.

COSO cube – 5 Integrated Components

Risk assessment

should occur at the business process level as well as the entity level

Risk Assessment

Four Primary Factors

1. **Materiality of the amounts**
   - Large dollars/transaction
   - High volume of transactions
   - Significant impact on key ratios or disclosures
2. **Complexity of the process**
   - Limited internal skills
   - Multiple data handoffs
   - Highly technical in nature
3. **History of accounting adjustments**
   - Accounting errors
   - Valuation adjustments, etc.
4. **Propensity for change in**
   - Business processes or controls
   - Related accounting

Grading Filter

Process-level Risk Assessment

High

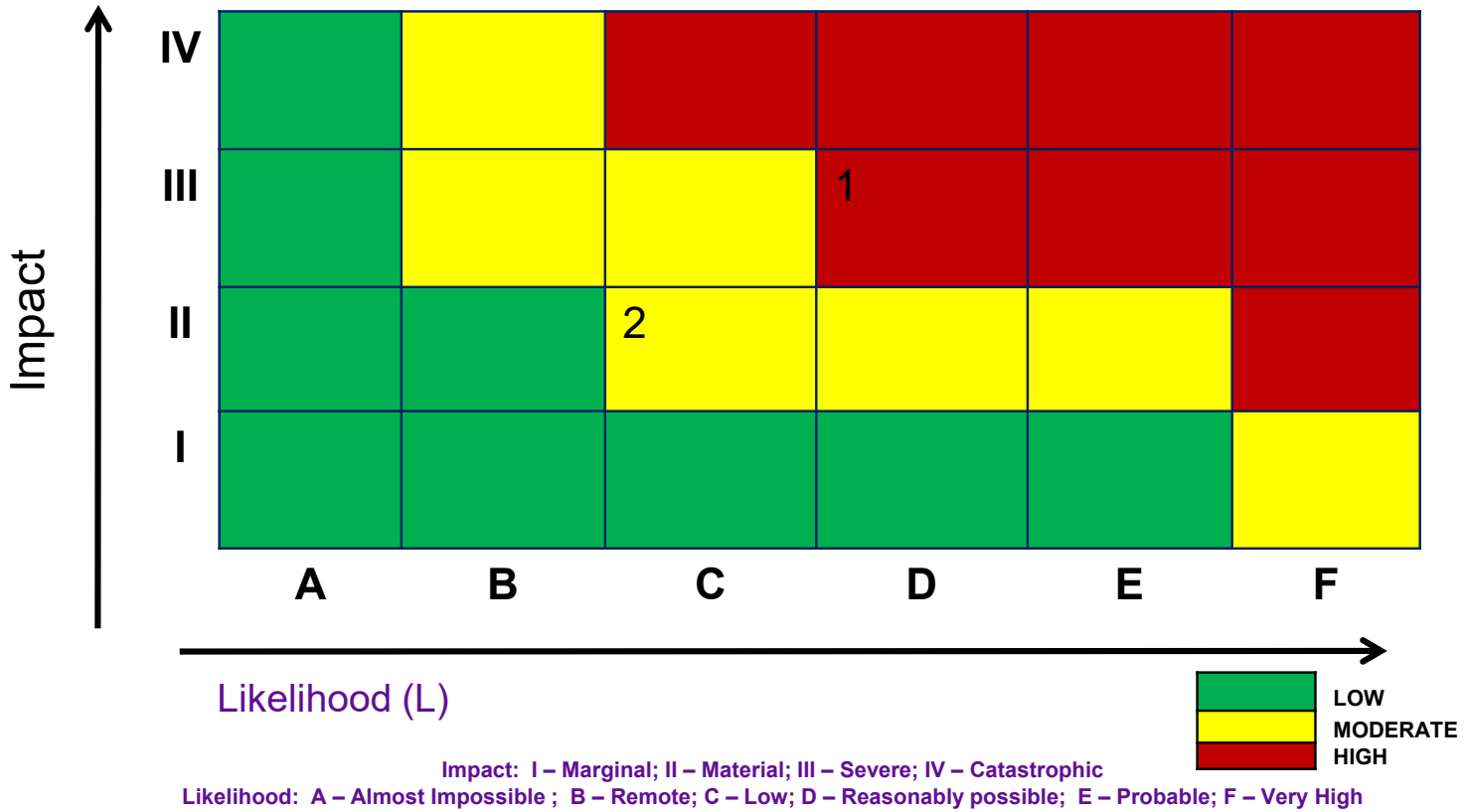
Medium

Low

COSO cube – 5 Integrated Components

Risk Mapping

Consider the organization's risk tolerance and risk appetite related to the risk response



Risk Strategies

Avoidance
Do not proceed!

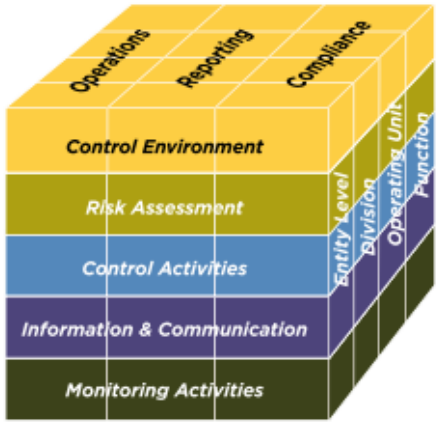
Mitigation
Improve controls to reduce likelihood/impact

Transfer
Shift responsibility to an external party

Acceptance
Accept the risk!

Creation
Seek risk activities strategically to maximize opportunities

COSO cube – 5 Integrated Components



3. Control Activities

- The actions established through policies and procedures that help ensure management's directives to mitigate risks are carried out.
- Performed at all levels within the entity

Types:

- Preventive and detective and corrective
- Compensating
- Manual and automated

Examples:

- Approvals & Authorizations
- Embedded verifications
- Reconciliations
- Independent Reviews
- Asset security
- Segregation of duties

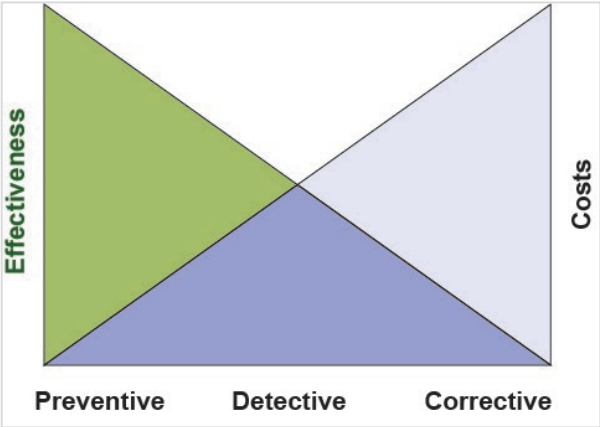
COSO cube – 5 Integrated Components

Preventive Control

Prevents the occurrence of a negative event in a proactive manner

Examples:

- Approval for purchase > $5,000
- Passwords for access to Banner
- Petty cash held in lockbox
- Security and surveillance systems
- Pre-numbered checks



Detective Control

Detect the occurrence of a negative event after the fact in a reactive manner

Examples:

- Supervisor review & approval
- Report run showing user activity
- Reconcile petty cash
- Physical inventory count
- Review missing/voided checks

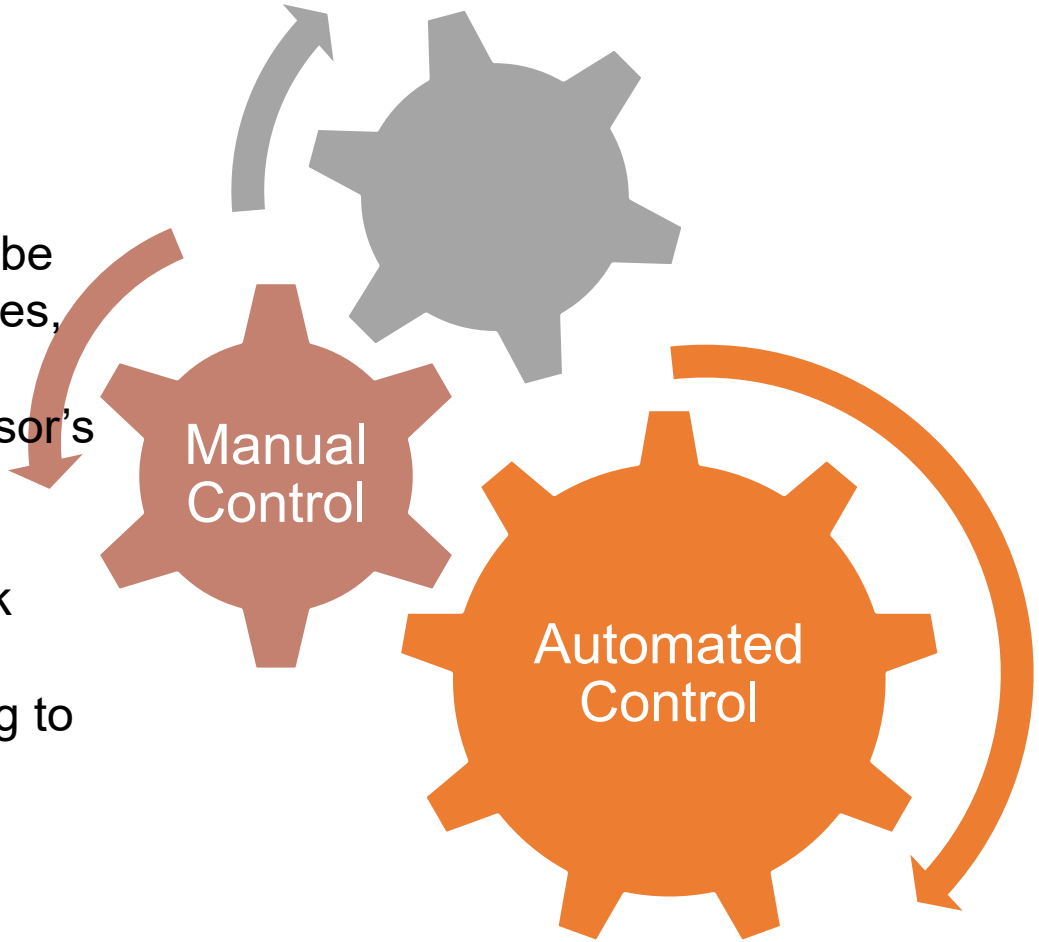
Control Activities

- If a weakness or limitation exists within the control environment, a **compensating control** may be relied upon to mitigate the risk
- Can be preventive *or* detective
- Example: A unit does not have the staff resources to establish an adequate segregation of duties. Potential compensating controls could include:
  - Automation of certain transaction data that cannot be altered by the staff
  - Manager review of detailed summary reports of the transactions initiated by the staff
  - Peer staff and/or manager selects a sample of transactions and vouches back to supporting documentation

Control Activities

Require action to be taken by employees, e.g.,

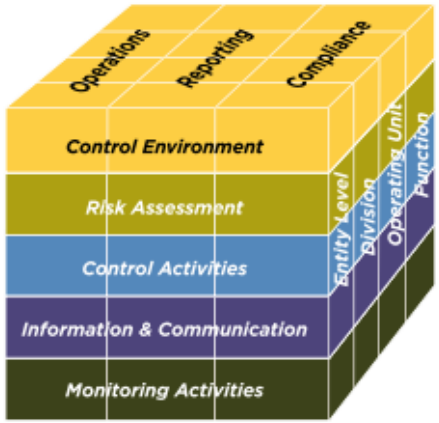
- Obtain supervisor's approval for overtime
- Reconcile bank accounts
- Match receiving to POs



Built into network infrastructure and software applications, e.g.,

- Passwords
- Data entry validation checks
- Batch controls

COSO cube – 5 Integrated Components



4. Information and Communication

- Information is necessary to carry out internal control responsibilities to support achievement of objectives

- Communication: the continual, iterative process of providing, sharing, and obtaining necessary information

- Internal and external
- Information should be timely, accessible, and allow for successful control actions

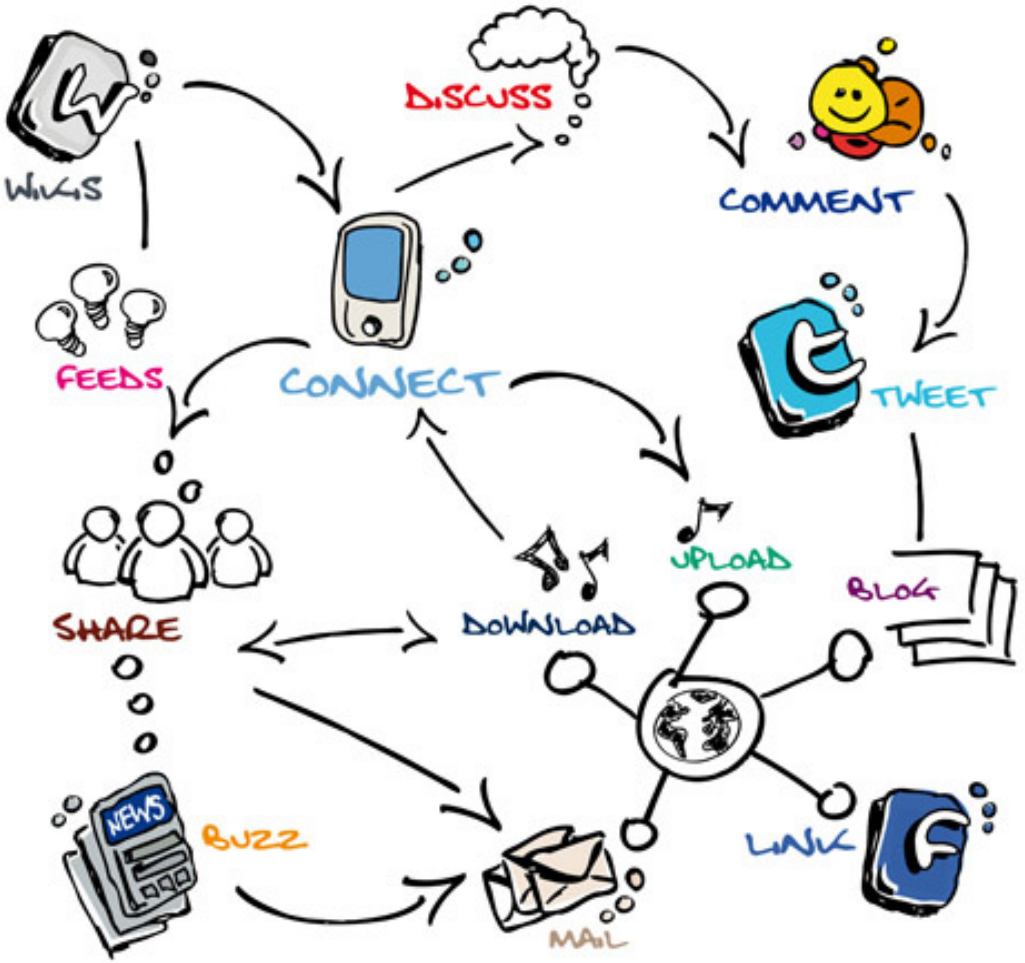
Key: To **communicate** the **right information** to the **right people** at the **right time**

COSO cube – 5 Integrated Components

Information & Communication

Things to communicate:

- Initiatives
- Goals
- Changes
- Opportunities
- Feedback
- Questions
- Answers
- Policies
- Procedures
- Standards
- Expectations



UNIVERSITY OF NORTH CAROLINA CHARLOTTE

COSO cube – 5 Integrated Components

5. Monitoring Activities

- Evaluations used to ascertain whether components of internal control are **present** and **functioning**

- *Ongoing* evaluations:
  - Built into business processes
  - Provide timely information

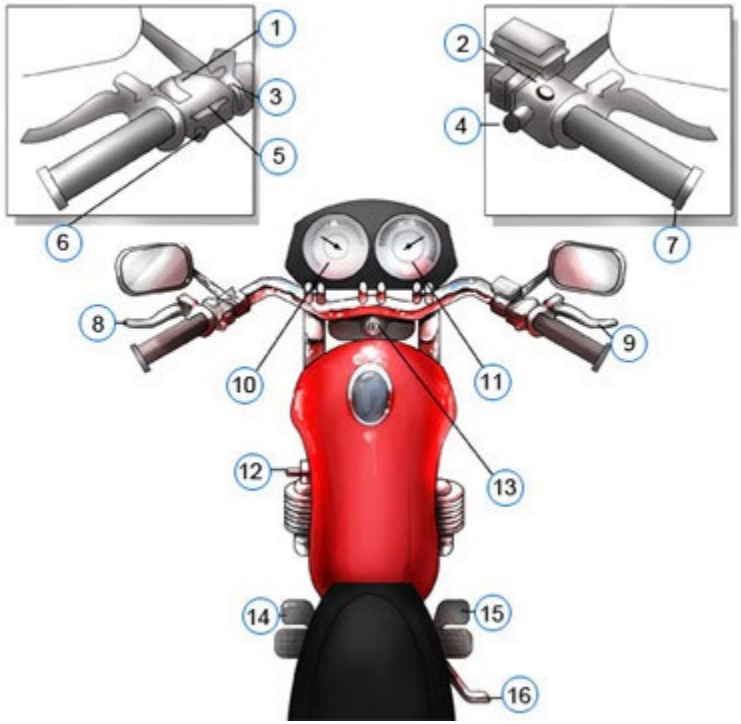
- *Separate* evaluations:
  - Conducted periodically
  - Vary in scope and frequency
    - Dependent on assessment of risks, effectiveness of ongoing evaluations, other management considerations

Findings are evaluated against relevant criteria

Deficiencies are communicated to the Board and Sr. Management

Testing Control Processes

- **Identify**
  - transactions to be tested
  - key controls
  - applicable standards to test the transactions (i.e., criteria to judge compliance effectiveness)
- **Determine**
  - appropriate type of testing
  - extent of testing
- **Create** test plan
- **Conduct** tests for effectiveness
- **Document** testing and results
- **Assess** test results
- **Communicate** findings, recommendations



Monitoring/Validating Controls

Deficiency in Design – A critical control is not properly designed, i.e., even if the control operates as designed, the control objective is not always met.

When validating control design (determining effectiveness):

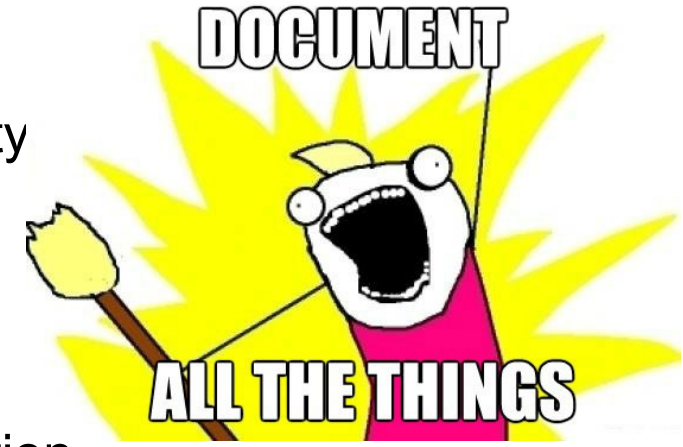
- Consider various factors (**how** control is performed, **who** performs the control, **what** data/reports used in performing control, what physical evidence is produced from the control)
- Work off of process narratives, flowcharts, and any other relevant material obtained and/or completed in the **documentation** stage
- Be aware that application controls are either programmed control procedures (e.g., edits, matching, reconciliation routines) or computer processes (e.g., calculations, on-line entries, automatic system interfaces).

Monitoring/Validating Controls

Deficiency in Operation – A properly designed control does not operate as intended, or the person performing the control does not possess the necessary authority or qualification to perform the control effectively.

- Testing operating effectiveness includes, in part:
  - Reviewing supporting documentation for proper authorization,
  - Reviewing the results of periodic reconciliations, and
  - Reviewing policies and procedures to determine if they are being followed.
- Use appropriate sampling techniques as necessary.

Monitoring/Validating Controls



Documentation should be maintained for:

- The evaluation of internal control at the entity and process levels
- What testing has been performed
- Identified deficiencies

Documentation must contain sufficient information to:

- Identify who performed the work and when
- Enable understanding of the nature, timing, extent, and results of the procedures performed
- Enable understanding of the evidence obtained
- Support the conclusions reached

Limitations of Internal Control

Even an effective system of internal control can experience a failure. **Limitations** may result from:

- Suitability of established objectives
- Reality that human judgment in decision making can be faulty and subject to bias
- Breakdowns that can occur because of human failures such as simple errors
- Ability of management to override internal control
- Ability of management, other personnel, and/or third parties to circumvent controls through collusion
- External events beyond the University's control

Again, internal control provides ***reasonable***, not absolute, assurance of achieving objectives.

Practical Implications

How can you incorporate internal controls within your current processes?

Connect


Objectives
What are you trying to achieve?
What might thwart our efforts?
Risks
Controls
How can we manage risk?

Determining Where Controls are Needed

First, must …

Document the process!

1. Pick a method that suits the process: Flowchart or Narrative
2. Identify process owner and activity owners
3. Identify the key inputs, activities, outputs, and risk points
4. Identify policies that impact the process
5. Identify standards that may specify mandatory controls

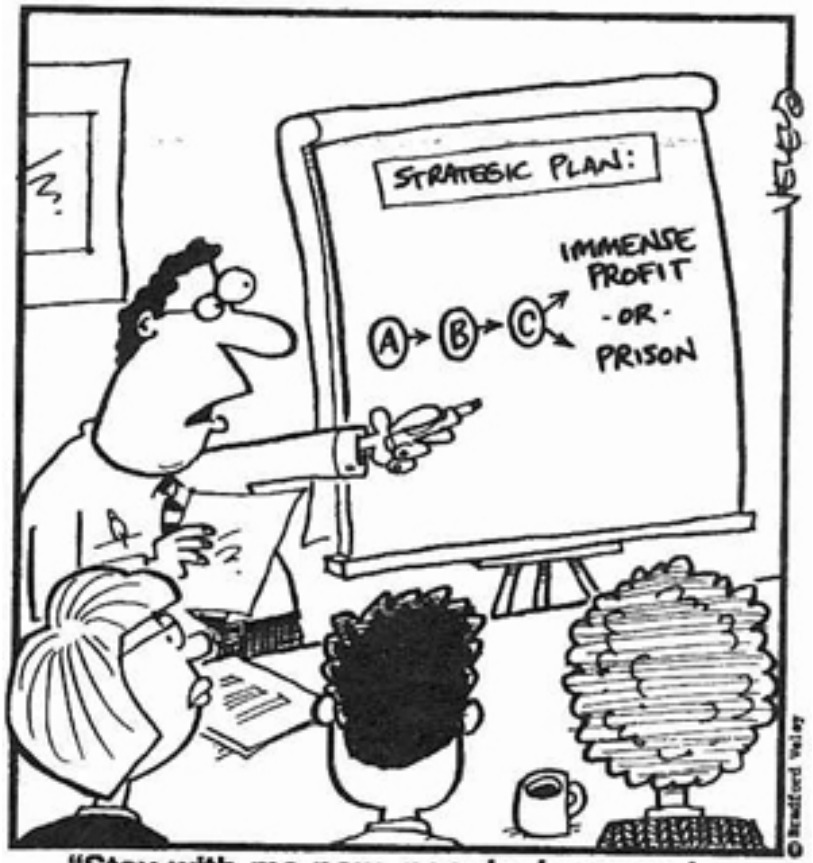
Identifying Key Control Activities

- Identify and document all controls associated with key processes
- Identify the characteristics of controls that, when functioning as intended, would provide the evaluator with a ‘level of comfort’ to conclude that the control is effective with respect to a given risk
- Consider control effectiveness by focusing on:
  - Directness and clarity of the control technique
  - Frequency with which the control technique is applied
  - Experience of personnel performing the control
  - Procedures followed when a control identifies an exception condition

Understanding Control Design

For internal controls over **financial reporting**, consider the following questions:

1. Will the control techniques help achieve the control objectives?
2. Will the controls mitigate risk to an acceptable level?
3. How do the related control objectives prevent or detect a potential misstatement?
4. How do potential misstatements affect the related financial report line item?



"Stay with me now, people, because in step C, things get a bit delicate."

Common Basic Internal Control Principles

Establish Responsibility

- Assign each task to only one person

Segregate Duties

- Don’t make one employee responsible for all parts of a process

Restrict Access

- Don’t provide access to systems, information, assets, etc. unless needed to complete assigned responsibilities

Document Procedures and Transactions

- Prepare documents to show that activities have occurred

Independently verify

- Check others’ work

Understanding Control Design

Good Controls are:

- Focused
- Integrated
- Accurate
- Simple
- Accepted
- Cost Effective

Key Points

- Need to connect **Objectives, Risks, and Controls**

- **Five interrelated components** of Internal Control
  1. Control Environment
  2. Risk Assessment
  3. Control Activities
  4. Information and Communication
  5. Monitoring
- Along **3 main objectives**
  - Operations
  - Reporting
  - Compliance

- Across the **organization, down to the process** functions

- No silver bullet

- Should accompany process **documentation** efforts

Resources

Controller's Office:

- https://finance.charlotte.edu/about-us/offices/controllers-office

Internal Audit:

- https://internalaudit.charlotte.edu/

COSO website:

- https://www.coso.org/