COSO ICIF 2013

COSO Internal Control Integrated Framework

Risk Assessment/Control Activities Principles and Points of Focus

Michael L. Piazza
Principal Associate
Professional Development Associates

1

Risk Assessment/Control Activities- Course Agenda

- Definitions of Internal Control and the Organizational Process/Management Function
- Overview and Principles of the Components of the COSO Internal Control Integrated Framework
- RA Principle 6: *The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*
- RA 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.*
- RA Principle 8: *The organization considers the potential for fraud in assessing risks to the achievement of objectives.*
- RA Principle 9: *The organization identifies and assesses changes that could significantly impact the system of internal control.*

2

Risk Assessment/Control Activities - Course Agenda

- CA Principle 10: *The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*
- CA Principle 11: *The organization selects and develops general control activities over technology to support the achievement of objectives.*
- CA Principle 12: *The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.*
- Summary Case Exercise
- Summary, Discussion and Conclusion

3

Participant Introductions

- Name
- Agency/Department/Division
- Position/Title
- Time in Internal Control
- Major Control Responsibilities

4

New Solutions

"Rarely do we find men and women who willingly engage in hard, solid thinking. There is an almost universal quest for easy answers and half-baked solutions. Nothing pains some people more than having to think."

Rev. Martin Luther King, Jr.

5

Persian Proverb

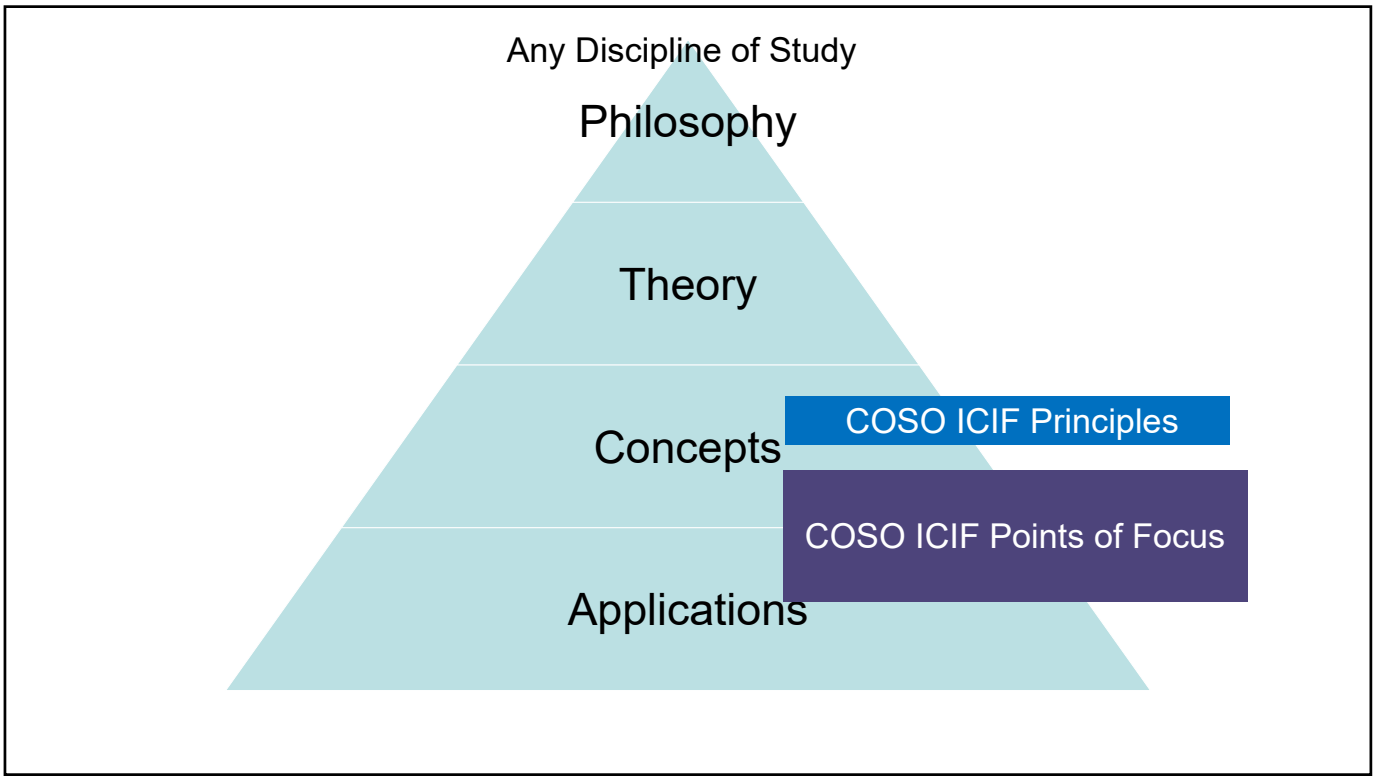
“He who knows not, and knows not that he knows not, is a fool, shun him.

He who knows not and knows that he knows not, is like a child, teach him.

He who knows and knows not that he knows, is asleep, awake him.

He who knows and knows that he knows, is wise, follow him.”

6



7

COSO (Committee of Sponsoring Organizations)

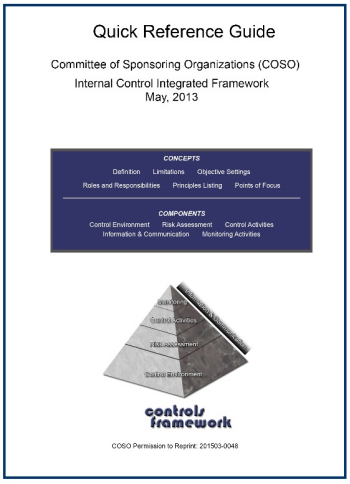
Internal Control Integrated Framework

Publication and Tools - 1992

Update – March , 2013

8

Institute of Internal Auditors - $174



Amazon.com - COSO Quick Reference Guide
$27 paperback
$9.99 Kindle edition

9

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Convened in 1984

American Institute of Certified Public Accountants

American Accounting Association

The Institute of Internal Auditors

Institute of Management Accountants

Financial Executives Institute

10

Treadway Commission met with President Ronald Reagan

"Yes, as auditors we trust that management has sufficient controls in place, but we must verify that."

" We trust but verify."

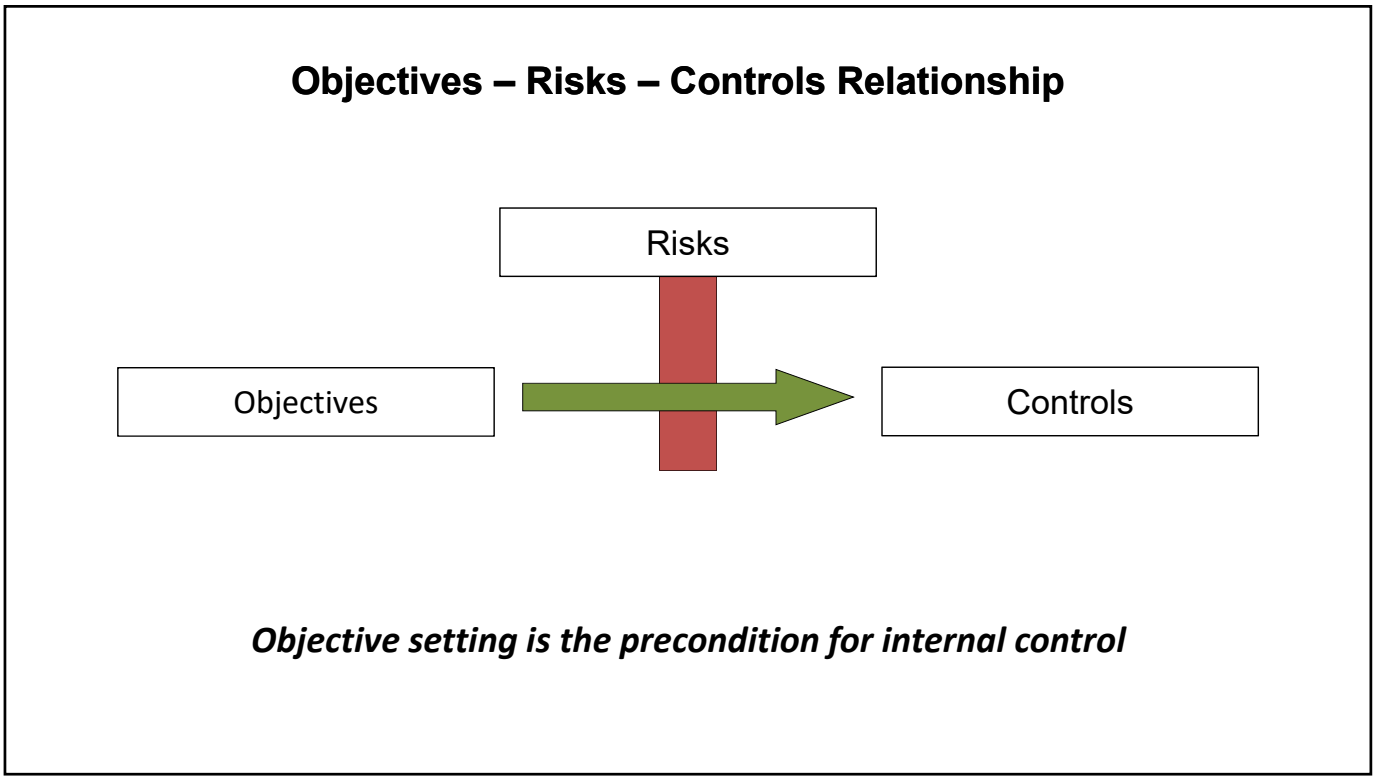
11

Organizational Process and the Management Function

12


Organizational Process
Mission
Vision
Values
Goals
Objectives
RISKS
Planning
Organizing
Directing
Controlling

13


Objectives – Risks – Controls Relationship
Risks
Objectives
Controls
Objective setting is the precondition for internal control

14

Objectives

Objectives are the things an organization wants to accomplish

15

Risks

Risks are things that could prevent an organization from meeting its objectives

16

Controls

Controls are things that help meet an organization's objectives.

17

Objective setting is the precondition for internal control

18

Definition of Internal Control ICIF 1992

Internal control is broadly defined as 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 financial reporting
- Compliance with applicable laws and regulations.

19

Definition of Internal Control From ICIF 1992 to 2013

Internal control is broadly defined as 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 financial reporting
- Compliance with applicable laws and regulations

20

Definition of Internal Control From ICIF 1992 to 2013

Internal control is broadly defined as 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: relating to :

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

21

Definition of Internal Control ICIF 2013

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.

22

This definition emphasizes that internal control is:

Geared to the achievement of objectives in one or more separate but overlapping categories - operations, reporting and compliance

A process consisting of ongoing tasks and activities - it is a means to an end, not an end in itself

Effected by people - not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organization to effect internal control

Able to provide reasonable assurance - but not absolute assurance, to an entity's senior management and board of directors

Adaptable to the entity structure - flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process

23

Limitations of Internal Control

Preconditions of Internal Control

Judgment

External Events

Management Override

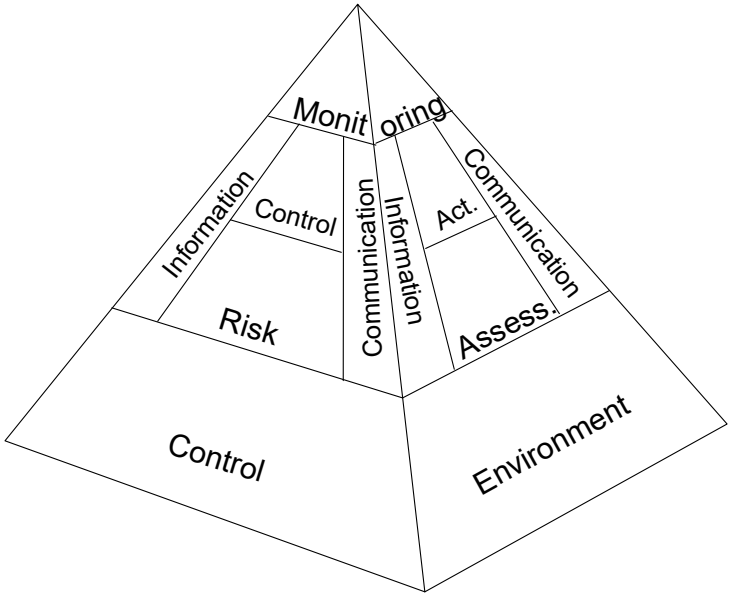
Collusion

24

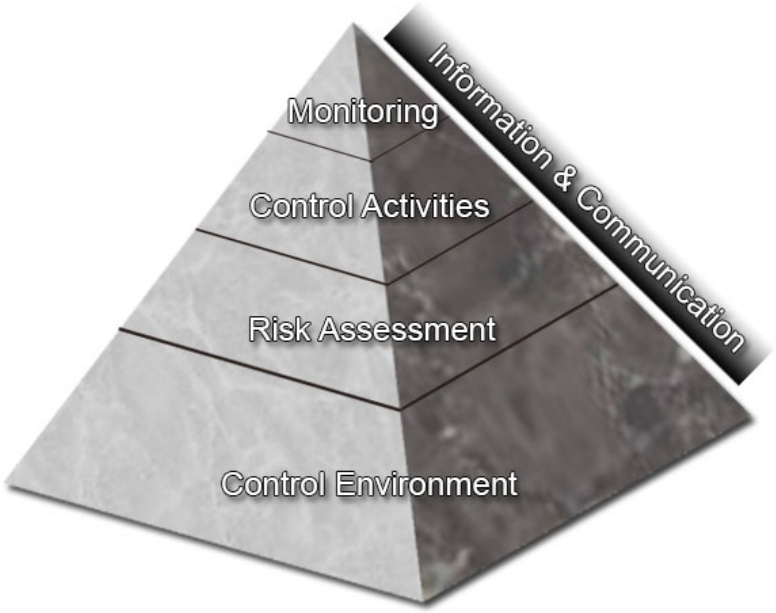
Components of the

Internal Control Integrated Framework

25



26



27

COSO Internal Control Integrated Framework

28

Framework with Objective Categories and Organizational Levels

29

Categories of Objectives

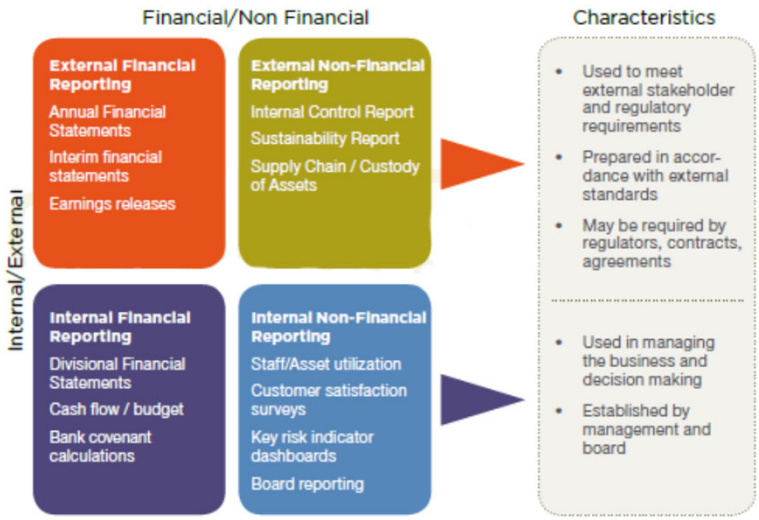
Operations

Internal Reporting
- Internal Non-Financial
- Internal Financial

External Reporting
- External Non-Financial
- External Financial

Compliance

30



31

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

32

Risk Assessment

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

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.

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

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

33

Control Activities

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

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

12. The organization deploys control activities as manifested in policies that establish what is expected and in relevant procedures to effect the policies.

34

Information & Communication

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

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

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

35

Monitoring Activities

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

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.

36

Governance Definitions

Governance is that separate process or certain part of management or leadership processes that makes decisions that define expectations, grant power, or verify performance. Frequently a government is established to administer these processes and systems.

Governance (in business) is the action of developing and managing consistent, cohesive policies, processes and decision rights for a given area of responsibility. For example, managing at a corporate level: privacy, internal investment, the use of data.

37

Origin

The word derives from Latin origins that suggest the notion of 'steering'. This sense of 'steering' a group or society can be contrasted with the traditional 'top-down' approach of governments 'driving' society or the distinction between 'power to' in contrast to governments 'power over'.

38

General Description

As a process, governance may be carried out for any size organization from a single human being to all of humanity, and it may be carried out for any purpose, good or evil, for profit or not. A reasonable or rational purpose of governance is to see to it (assure), sometimes on behalf of others, that the organization produces a worthwhile pattern of good results while avoiding an undesirable pattern of bad circumstances.

Perhaps the most moral or natural purpose of governance is to assure, on behalf of those governed, a worthy pattern of good while avoiding a truly undesirable pattern of bad. The ideal purpose, obviously, would assure a perfect pattern of good with no bad. A government, then, is a set of inter-related positions that govern and use or exercise power, particularly coercive power.

39

IIA Glossary

Governance

The combination of processes and structures implemented by the board in order to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

40

Uncertainty - Value

UNCERTAINTY: Enterprises operate in environments where factors such as globalization, technology, regulation, restructurings, changing markets, and competition create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that potential events will occur and the associated outcomes.

VALUE: Value is created, preserved or eroded by management decisions ranging from strategy setting to operating the enterprise day-to-day. Inherent in decisions is recognition of risk and opportunity, requiring that management1 considers information about internal and external environments, deploys precious resources and recalibrates enterprise activities to changing circumstances.

41

Realize Value

Entities realize value when stakeholders derive recognizable benefits that they in turn value.

For companies, shareholders realize value when they recognize value creation from share-value growth.

For governmental entities, value is realized when constituents recognize receipt of valued services at an acceptable cost.

Stakeholders of not-for-profit entities realize value when they recognize receipt of valued social benefits.

Enterprise risk management facilitates management's ability to both create sustainable value and communicate the value created to stakeholders.

42

Categories of Objectives

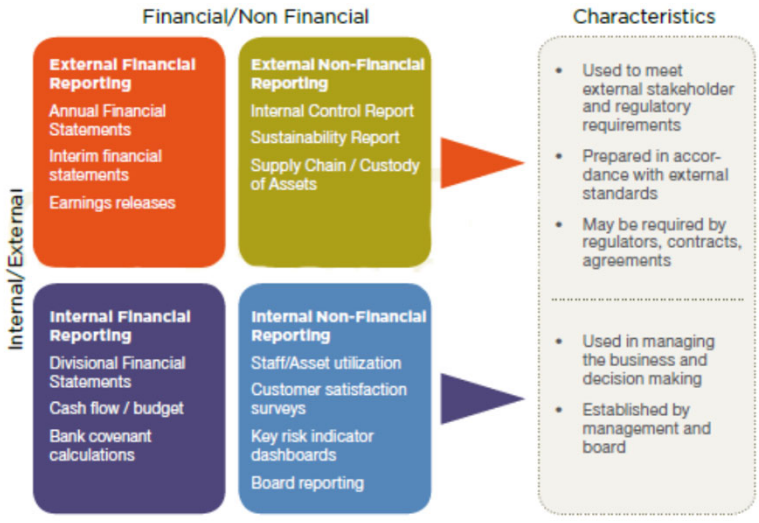
Operations

Internal Reporting
- Internal Non-Financial
- Internal Financial

External Reporting
- External Non-Financial
- External Financial

Compliance

43

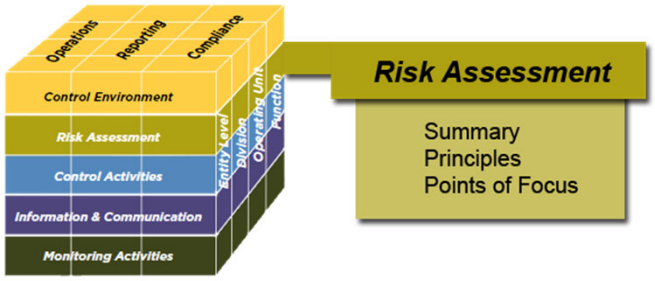


44

Risk Assessment and Control Activities

Principles and Points of Focus

45



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.

46

Risk Assessment

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

- Alignment between established objectives and strategic priorities
- Articulation of risk tolerances for objectives
- Alignment between established objectives and established laws, rules, regulations, and standards applicable to the entity
- Articulation of objectives using terms that are specific, measurable or observable, attainable, relevant, and time-bound
- Cascading of objectives across the entity and it subunits
- Alignment of objectives to other circumstances that require specific focus by the entity
- Approval objectives within the objective-setting process

47

Risk Assessment

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

Operations Objectives:

- **Reflects Management's Choices**—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
- **Includes Operations and Financial Performance Goals**—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
- **Forms a Basis for Committing of Resources**—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

48

Risk Assessment

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

Reporting Objectives – External Financial Reporting:

- **Complies with Applicable Accounting Standards**—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
- **Considers Materiality**—Management considers materiality in financial statement presentation.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

49

Risk Assessment

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

Reporting Objectives – External Non-Financial Reporting:

- **Complies with Externally Established Standards and Frameworks**—Management establishes objectives consistent with laws and regulations, or standards and frameworks of recognized external organizations.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs and as based on criteria established by third parties in non-financial reporting.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

50

Risk Assessment

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

Reporting Objectives – Internal Reporting:

- **Reflects Management's Choices**—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
- **Considers the Required Level of Precision**—Management reflects the required level of precision and accuracy suitable for user needs in non-financial reporting objectives and materiality within financial reporting objectives.
- **Reflects Entity Activities**—External reporting reflects the underlying transactions and events within a range of acceptable limits.

51

Risk Assessment

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

Compliance Objectives:

- **Reflects External Laws and Regulations**—Laws and regulations establish minimum standards of conduct which the entity integrates into compliance objectives.
- **Considers Tolerances for Risk**—Management considers the acceptable levels of variation relative to the achievement of compliance objectives.

52

Risk Assessment

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.*

- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels**—The organization identifies and assesses risks at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
- **Analyzes Internal and External Factors**—Risk identification considers both internal and external factors and their impact on the achievement of objectives.
- **Involves Appropriate Levels of Management**—The organization puts into place effective risk assessment mechanisms that involve appropriate levels of management.
- **Estimates Significance of Risks Identified**—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
- **Determines How to Respond to Risks**—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

53

Risk Assessment

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

- **Considers Various Types of Fraud**—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
- **Assesses Incentive and Pressures**—The assessment of fraud risk considers incentives and pressures.
- **Assesses Opportunities**—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering of the entity's reporting records, or committing other inappropriate acts.
- **Assesses Attitudes and Rationalizations**—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.

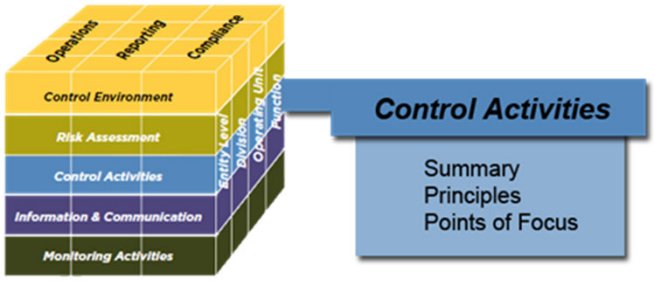
54

Risk Assessment

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

- **Assesses Changes in the External Environment**—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
- **Assesses Changes in the Business Model**—The organization considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
- **Assesses Changes in Leadership**—The organization considers changes in management and respective attitudes and philosophies on the system of internal control.

55

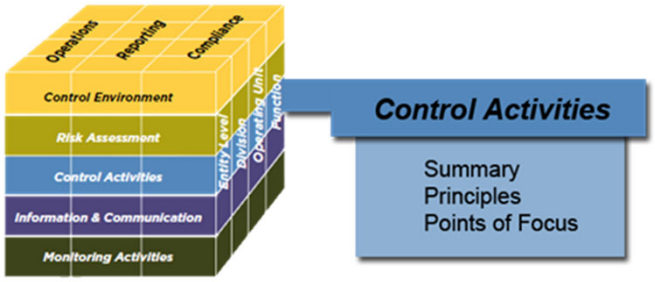


Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment.

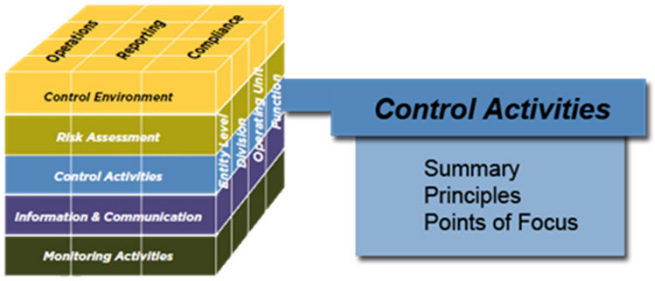
They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

56



Control activities serve as mechanisms for managing the achievement of an entity's objectives and are very much a part of the processes by which an entity strives to achieve those objectives.
They do not exist simply for their own sake or because having them is the right or proper thing to do.

57



Control activities can support one or more of the entity's operations, reporting, and compliance objectives.
For example, an online retailer's controls over the security of its information technology affect the processing of accurate and valid transactions with consumers, the protection of consumers' confidential credit card information, and the availability and security of its website.
In this case, control activities are necessary to support the reporting, compliance, and operations objectives.

58

Control Activities

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

- **Integrates with Risk Assessment**—Control activities help ensure that risk responses that address and mitigate risks are carried out.
- **Considers Entity-Specific Factors**—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
- **Determines Relevant Business Processes**—Management determines which relevant business processes require control activities.
- **Evaluates a Mix of Control Activity Types**—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.

59

Control Activities

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

- **Determines Dependency between the Use of Technology in Business Processes and Technology General Controls**—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
- **Establishes Relevant Technology Infrastructure Control Activities**—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.

60

Control Activities

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

- **Establishes Relevant Security Management Process Control Activities**—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
- **Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities**—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.

61

Control Activities

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

- **Establishes Policies and Procedures to Support Deployment of Management's Directives**—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions
- **Establishes Responsibility and Accountability for Executing Policies and Procedures**—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.

62

Control Activities

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

- **Performs in a Timely Manner**—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
- **Performs Using Competent Personnel**—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
- **Reassesses Policies and Procedures**—Management periodically reviews control activities to determine their continued relevance, and refreshes them when necessary.

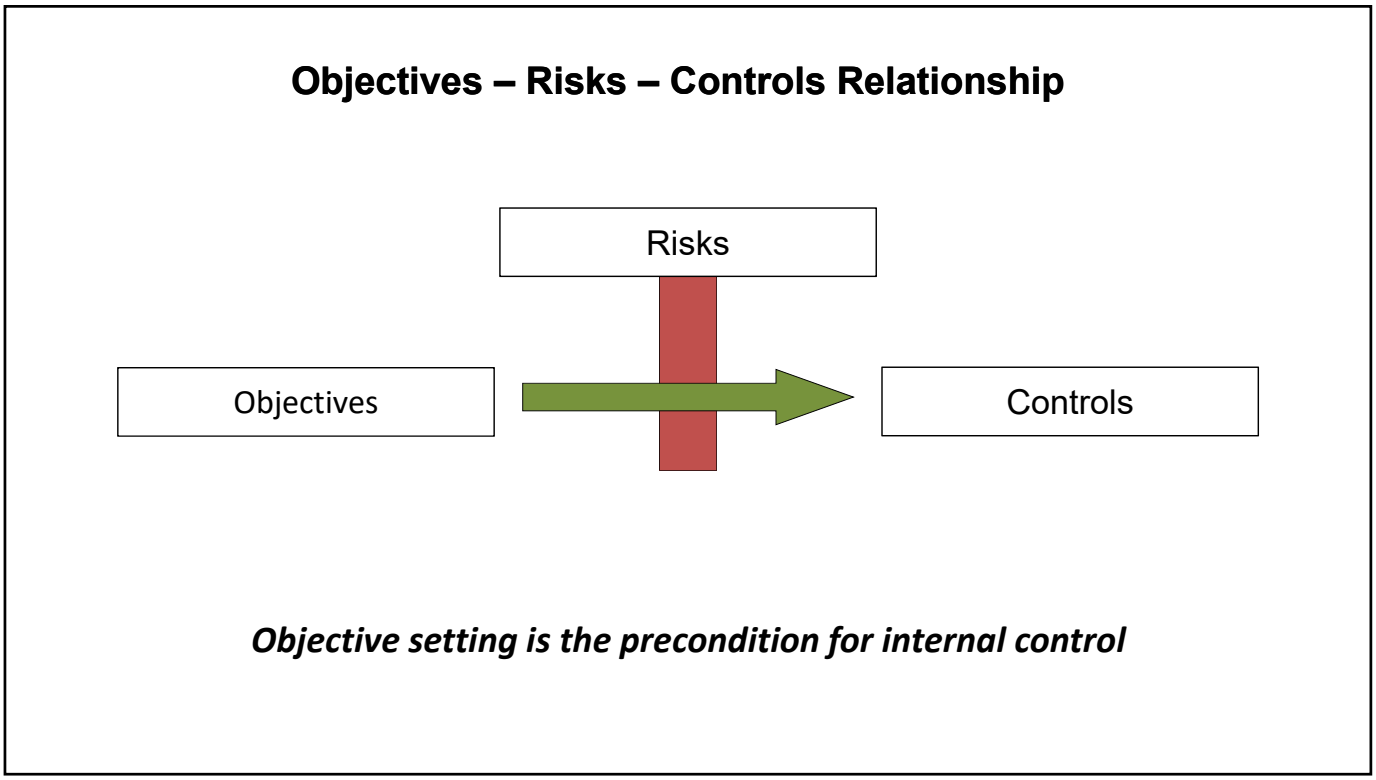
63

Overview of topics

64


Organizational Process
Mission
Vision
Values
Goals
Objectives
RISKS
Planning
Organizing
Directing
Controlling

65


Objectives – Risks – Controls Relationship
Risks
Objectives
Controls
Objective setting is the precondition for internal control

66

Definition of Internal Control
ICIF 2013

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.

67

Michael L. Piazza

Professional Development Associates

michael@pda-usa.com

www.pda-usa.com

www.controlsframework.com

68