Internal Financial Controls (IFC)

ICAI Seminar – October 8, 2016

Financial Reporting Assertions

Effective Internal Controls over Financial Reporting

All Significant Accounts considered

Financial Assertions addressed for each significant Account

Minor or few internal control deficiencies noted

Risk • Pro

Financial Assertions

1. Existence/Occurrence

- **Existence** – Balance Sheet focused – Assets, Liabilities and Ownership Interests (Equity) **exist** as of the statement date and balances have a **real world counterpart** (i.e. customers, suppliers, employees, banks, etc).

- **Safeguard Assets** – Access to assets and critical documents that control their movement are suitably restricted to authorized personnel. Often covered as part of Segregation of Duties review.

- **Occurrence** – Income Statement focused – Transactions and events that have been recorded **actually occurred** and pertain to the entity.

Risk • Pro

Financial Assertions

2. Completeness

- **Completeness** – **All** transactions and events that should have been recorded have been recorded.

- **Cut-Off –** Transactions and events have been recorded in the **proper period**.

3. Valuation/Allocation

- **Valuation** – Amounts based on **estimates and judgments** are in accordance with US GAAP

- **Allocation** – Costs are allocated from the Balance Sheet to the Income Statement in the proper period (e.g. depreciation and amortization).

- **Accuracy** – Amounts recorded are **mathematically** accurate.

Financial Assertions

4. Rights/ Obligations

- **Rights** – The entity holds the rights to the **assets**.
- **Authorization** – Transactions are executed in accordance with management's general and specific authority.
- **Obligations** – **Liabilities** recorded are the obligation of the entity.

5. Presentation / Disclosures

- **Classification** – financial statement focused – transactions and events have been recorded in the proper **accounts**.
- **Understanding** – **disclosure** driven (generally footnotes) – financial information is appropriately described and understandable to users.

Risk • Pro

Identify Assertions addressed by following Controls

Inventory is physically verified at Year End Date	• Existence, Completeness
Inventory in the Balance sheet is reported using FIFO method of valuation	• Valuation
Premium accounting by Insurance Cos deploys a maker checker control when entering data in system	• Valuation (Accuracy)
All sales invoices are manually generated and have a single series of numbers	• Completeness
Changes in Depreciation policy are reported in the Notes to Accounts	• Presentation and Disclosures
Provisions for liabilities are created at 31 March	• Obligations

Risk • Pro

Identify Assertions addressed by following Controls

Interest Expense on Fixed Deposits is automated and calculated using rates from master tables.	• Completeness and Accuracy
Provision for Write off are properly classified and reported	• Presentation and Disclosures
Sales returns are recorded when occurred	• Completeness
Variance Analysis is done for F/S before release to Stock Exchange	• Completeness, Accuracy, Existence
Clearing of inter company and suspense items	• Completeness, Presentation and Disclosure
All Legal lawsuits are identified and their impact assessed / reported	• Presentation and Disclosure, Completeness

Risk • Pro

Case Study – Revenue Internal Controls

1. A small yarn Manufacturer sells **yarn and fabric** through its agents and to the end wholesaler as its customers.
2. Orders are received via email from the Agents, entered in the system, and based on which goods dispatched to wholesaler.
3. Prices are input at the time of recording the order. Tax rates are part of the masters.
4. Data from the order is used to create automated invoice (No new data entered to create invoice). Invoice copy is checked by security as goods are loaded / shipped.
5. Data input in the order system can be modified. Invoice cannot be modified.
6. Data from Sales Dept system is imported by Accounts Dept before finalising Balance sheet. Disclosure for segmental reporting is taken from accounting system.

Identify key internal controls necessary for Revenue

COSO and IFC

Internal Control Defined – COSO Definition

- 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*"

  - Geared to the achievement of objectives in one or more separate but overlapping categories
  - A process consisting of ongoing tasks
  - Effected by people—it is not merely about policy and procedure manuals, but about people and the actions they take at every level to effect internal control
  - Able to provide reasonable assurance, not absolute assurance

Risk • Pro

Why do Controls Fail

Therefore, internal controls provide reasonable assurance, not absolute assurance

Scenario → What do you think changes the most in the situation. What needs to be done.

A medium sized company is well managed and has good internal controls with respect to process activities and oversight of the operations.

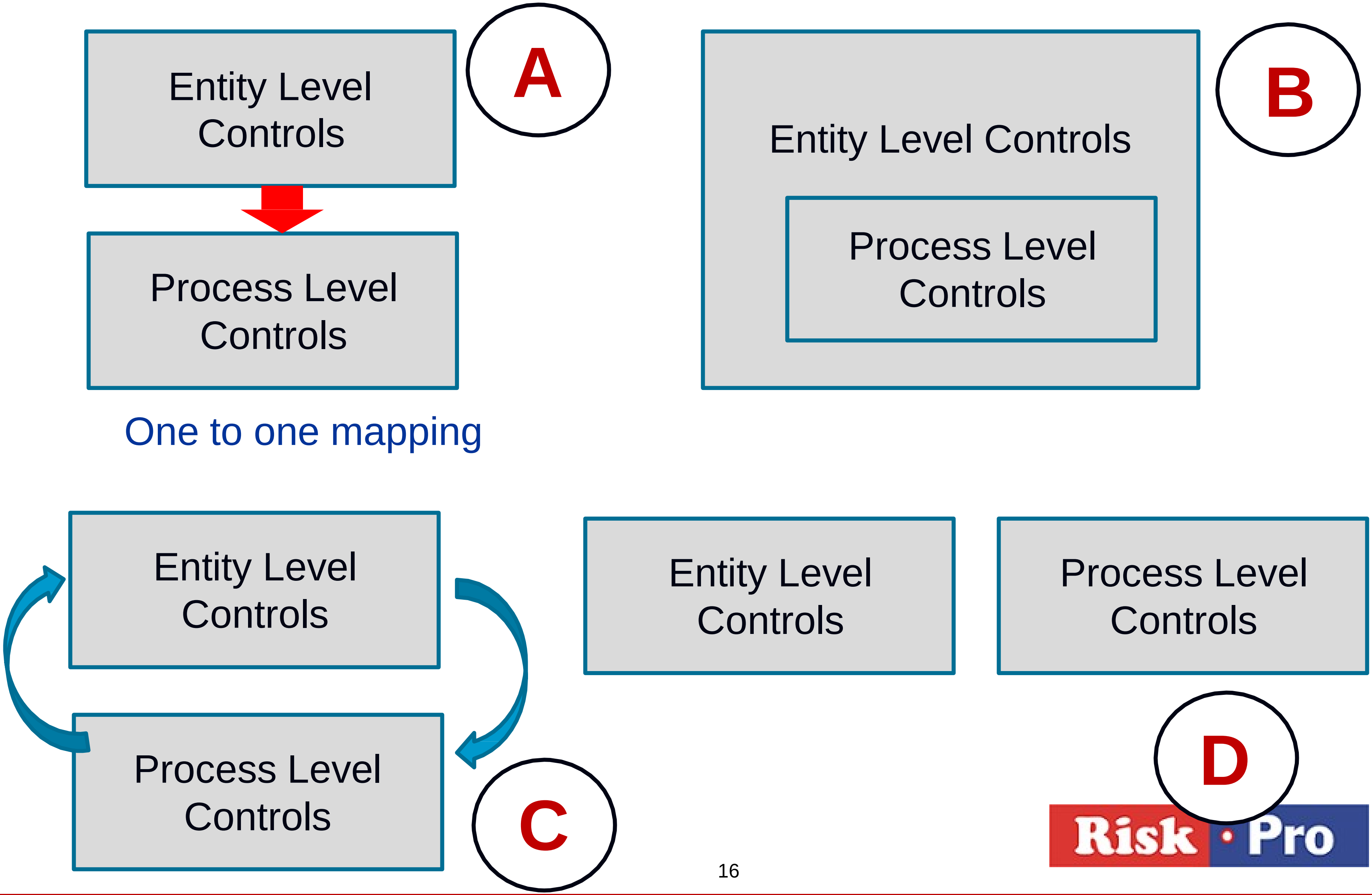
As it grows, it decides to pivot its business model and outsources most of its activities. Logistics, supply chain, HR, accounting etc.

- The internal controls continue as before and are tested regularly.
- Company continues to do well and make profits.

Risk • Pro

Entity Level Controls

Which scenario best describes the relationship between Entity Level Controls and Process Level Controls



Entity Level Controls

- The PCAOB gives some examples, although it did not come up with a definition. *Entity Level Controls are controls that have the following* characteristics:
  - they exist on a higher level than transactional controls; and,
  - set positive conditions and boundaries for the transactional controls; and,
  - are the internal control infrastructure.
- Entity Level controls strengthen the business process controls.
- In the absence of entity level controls, a process cannot be made strong enough, however many controls we have.

Risk • Pro

Components and Entity Level Controls

- All processes and control activities and frameworks that address each of the principle and focus point are largely Entity Level Controls (Softer or indirect controls”).

- Absolutely essential for an ICS to be effective. Without Entity level controls, most of the objectives could not be met.

- Internal Audit usually don’t test these entity level controls in a specific clear cut manner.

CE	RA	CA	IC	MA

Risk • Pro

Entity versus Process Level Controls

All 17 Principles relate to People

Entity.olevel – People

Generic – for any level or type of entity

IC Documentation

COSO Template

Activity-Level = The activities done by People

Specific .... to the act lty be ng performed

Control Activities Principles 10 and 11are closest to The Work

RCM

RCM

RCM

Risk Pro

Examples of Entity Level Controls

- Controls related to the control environment
- Controls over management override
- Risk Assessment Process
- Centralized processing and controls, including shared service environments
- Controls to monitor results of operations
- Controls over the period-end financial reporting process
- Internal audit
- Whistle-blower hotline / Code of conduct
- IT environment and organizations

Risk • Pro

Examples of Entity Level Controls

- Oversight by the Board of Senior Management
- Variance analysis reporting
- Remediation mechanism
- Management triggers embedded within IT systems
- Internal communication and performance reporting
- Change management
- Governance
- Hiring and retention practices
- Fraud prevention/detection controls and analytical procedures

Risk • Pro

Summary of Five Principles in Control Environment.

Demonstrate Integrity and Ethics			
Board and Mgmt Oversight	Structures and Responsibilities	Competence	Enforce Accountability

IFC / Entity Level Controls for SME

SME

SMALL & MEDIUM ENTERPRISES

Smaller

Less Complex

- **Aug 22, 2016 Guidance Note on IFC for smaller companies**

Risk • Pro

What are the difficulties in IFC Testing in SME

Lack of ELC

Processes not documented

Segregation of duties / Few staff

Lack of IT Controls

Risk • Pro

COSO and Internal Controls

1992-7 2013

COSO Internal Control -Integrate Framework (1992- 2013)

Control ErwlrontnMt

Why COSO was updated – Some reasons

Transition to a principles-based approach; codify prior implicit concepts

- COSO 1992 was difficult to implement and to evaluate control deficiencies

Fraud

- **Putting fraud right out in the forefront.**
- A business's control structure must now address issues of fraud directly

Outsourcing

- More companies are outsourcing key portions of their business processes or controls to third parties.
- It includes expanded guidance and considerations relating to outside resources, such as third-party processors.

Overview of the COSO Content

Components	Principles
Control Environ1nent	1, Demonstrates commitment to int-egrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitn1ent to competence 5. Enforces accountability
Risk Assessn1ent	6. Specifies relevant objectives 7. ldentifies and ana1yzes risk 8. Assesses fraud risk 9. ldentifies and anaJyzes significant change
Control Activities	1.0. Selects and develops control activities 1.1 Selects and develops general controls over technology !1.2. Deploys through policies and procedures
InforJ.nation and Con1Juunication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Principles Based

- The Framework does not prescribe controls to be selected, developed, and deployed for effective internal control.
- An organization’s selection of controls to effect relevant principles and associated components is a function of management judgment based on factors unique to the entity.

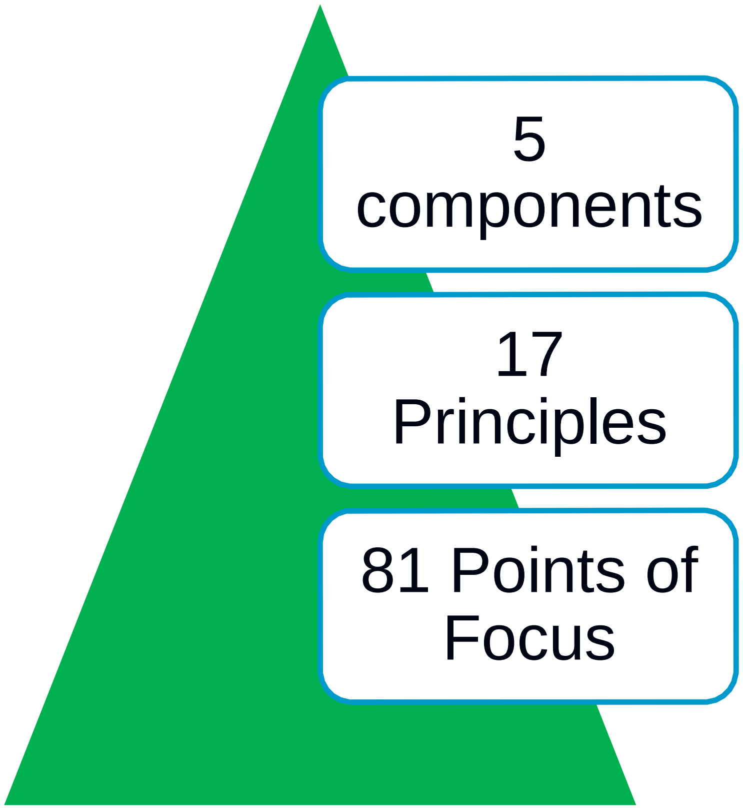
- Principles-based approach that provides flexibility and allows for judgment in designing, implementing, conducting internal control—principles that can be applied at the entity, operating, and functional levels
- Each principle is suitable to all entities

- All principles are presumed relevant except in rare situations where management determines that a principle is not relevant to a component (e.g., governance, technology)

Risk • Pro

Points of Focus

- Represent important characteristics that support each principle
- Provide a much more granular approach, including more detail and clarity on implementation
- Points of focus may facilitate designing, implementing, and conducting internal control



Note

- Points of focus may not be suitable or relevant, and others may be identified
- There is no requirement to separately assess whether points of focus are in place

Risk • Pro

Visual Example of the Structural Hierarchy

3 Objectives

5 Components

17 Principles

81 Points of Focus

Risk • Pro

Visual Example of the Structural Hierarchy

One of three Control Objectives

At a particular

Location or Division

Is affected by

Various Risks

Such risk are controlled by

Control Activities

Why should we use COSO

Applies to any type of entity

Covers all types of Objectives beyond financial reporting

A principles-based approach

Globally recognised and used

ICAI Guidance Note aligns to COSO

Linkages within Components

Relationship between Objectives, Risk and Controls

An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective.

Objectives

- Manufacture Quality Spare Parts

Risk Assessment

- Key risks that impact quality manufacturing

Control Activities

- Controls needed to mitigate the risks

At the heart of COSO Framework is the identification of those risks that can impact the objectives.

Objectives

Risks

Controls

Objectives

- **Operations Objectives**
  - effectiveness and efficiency of the entity's operations,
  - operational and financial performance goals, and
  - safeguarding assets against loss

- **Reporting Objectives**
  - internal and external financial and non-financial reporting
  - May encompass reliability, timeliness, transparency, or other terms set forth by regulators, recognized standard setters, or the entity's policies

- **Compliance Objectives**
  - adherence to laws and regulations to which the entity is

Risk • Pro

subject

Reporting Objectives

- Reporting objectives may relate to financial or non-financial reporting and to internal and external reporting

	Financial Reporting	Non Financial Reporting
External	•**Annual Financial Statements** •Interim Financial Statements •Earnings Releases	•Internal Control Report •Sustainability Report •Supply Chain / Custody of Assets
Internal	•Divisional Financial Statements •Cash Flow / Budgets •Bank Covenant Calculations	•Staff / Asset Utilization •Customer Satisfaction Surveys •Key Risk Indicator Dashboards •Board Reporting

Objectives

Risks

Controls

Risk • Pro

COSO ERM 2016

Principle 7

CE	RA	CA	IC	MA

Identifies and Analyzes Risk

- **Points of Focus:**
- Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels
- Analyzes Internal and External Factors
- Involves Appropriate Levels of Management
- Estimates Significance of Risks Identified
- Determines How to Respond to Risks

COSO's principles 6 through 9 represent significant updates from the 1992 guidance which only articulated 14 objectives; expanding a single "risk" objective into four principles with 27 of COSO's 87 focus points devoted to risk

Objectives

Risks

Controls

Control Activities

- 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.

Principle 10

CE | RA | CA | IC | MA

Selects and Develops Control Activities

- **Points of Focus:**
- Integrates with Risk Assessment
- Considers Entity-Specific Factors
- Determines Relevant Business Processes
- Evaluates a Mix of Control Activity Types
- Considers at What Level Activities are Applied
- Addresses Segregation of Duties

Business Process Control Activities

- Transaction controls are the most fundamental control activities in an entity since they directly address risk responses in the business processes in place to meet management's objectives
- Example controls in sales process, controls in purchase process etc

Risk • Pro

MRC are very commonly used

- monthly comparisons of actual results to forecasted revenues or budgeted expenses
- comparisons of other metrics, such as gross profit margins and expenses as a percentage of sales;
- quarterly balance sheet reviews.
- Review of overall investment portfolio depreciation.

Risk • Pro

Why are Internal Controls Expensive

Need to create audit trail, documentation

Controls are dynamic. They change and break often

Internal Control Testing is Time consuming

Enough controls is still not enough

Management Override of Controls

WHY

- Dependence on financial results for receiving bonuses or other benefits
- Need to meet debt covenants or other benchmarks imposed by lenders or investors
- Manipulation of stock price
- Pending sale of the company or refinancing of debt
- Desire to take shortcuts through the company's system

MINIMIZE

- Code of Conduct
- Job Rotation
- Mandatory Leave
- Strong Internal Controls
- Strong policies with no deviation paths

How

- Adjust accounts recv.
- record non-existent sales,
- manipulate inventory reconciliations,
- record false credits from vendors
- hide documentation relating to unrecorded liabilities
- Capitalise expenses

COSO and Control Effectiveness

What is "effective internal control"?- COSO

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  - Each component and each relevant principle is **present and functioning**
  - The five components are **operating together in an integrated manner**

- An effective system of internal control provides reasonable assurance of achievement of an entity's objectives
- **An effective system of internal control reduces, to an acceptable level, the risk of not achieving an objective relating to one two or three categories**
- Management exercises judgment in assessing whether each of the components and relevant principles are present and function and components are operating together

Present & Functioning

Present – refers to the determinations that components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives

Functioning – refers to the determination that components and relevant principles continue to exist in the conduct of the system of internal control to achieve the specified objectives

Risk • Pro

Examples of Present and Functioning – Control Environment

1. Demonstrates Commitment to Integrity and Ethical Values —The organization demonstrates a commitment to integrity and ethical values.

Establishes standard of Conduct

- The board of directors and senior management have formulated a set of policies on integrity and ethics, and these policies are regularly flashed on the firm's internal portal, and in newsletters as well as being incorporated into the contracts with outsourced service providers.
- There is no formal training program to help make employees aware of the importance of adherence to the standards of conduct

Evaluates adherence to standards of conduct

- It is up to the management of each operating unit to evaluate adherence to the organization's integrity and ethics policies. In most cases, this is not conducted
- There are no formal processes in place to evaluate individuals against the published integrity and ethics policies

Examples of Present and Functioning – Control Environment Contd

The combination of the internal control deficiency noted in the Principle 1 are a major deficiency. While there are formally published and communicated ethics and compliance policies, without training to make people aware of the polices, and processes to evaluate individuals against deviations and identify and address deviations, the organization is not setting a tone that violating the policies is unacceptable.

Principle Not Present and Not Functioning

Risk · Pro

Thanks