



COMMITTEE OF SPONSORING  
ORGANIZATIONS OF THE TREADWAY COMMISSION



# COSO Internal Control Framework – Introductory training

05 May' 2020



# COVERAGE



Risk & Internal Control Basics



COSO Internal Control Framework – Components and Principles



Internal Control Assessment



Internal Control Documentation



Internal Control – Indian Legal Perspective



Internal Control – Benefits & Limitations





Committee of Sponsoring Organizations of the Treadway Commission

# Risk & Internal Control Basics



# RISK & INTERNAL CONTROL IN A COMPANY

## Risk – What can go wrong?

- In general, risk is defined as the possibility that an **event will occur**, which will impact an organization's **achievement of objectives**.
- **Business Risk:** A threat that an event or action will adversely affect an organization's ability to maximize stakeholder value and to **achieve its business objective**.

## Risk Example

Risk of Plant Breakdown due to lack of timely maintenance.

## Internal control?

- Internal control is a **process**, effected by an entity's board of directors, management and other personnel, designed to provide **reasonable assurance** on **effectiveness and efficiency of operations, reliability of financial reporting** and **compliance with applicable laws and regulations**.

## Control Example

Detailed Preventive Maintenance schedule is prepared and Preventive Maintenance is undertaken to ensure periodic maintenance of all equipments

# INTERNAL CONTROL – PART OF OUR DAY TO DAY LIFE



**Risk:** Unauthorized access  
**Control:** Password or Biometric access



**Risk:** Short circuit leading to fire  
**Control:** Circuit breaker



**Risk:** High speed leading to accident  
**Control:** Brakes



**Risk:** Unauthorized activities or theft  
**Control:** CCTV cameras



**Risk:** Incorrect choices  
**Control:** Online review mechanism



**Risk:** Poor health  
**Control:** Monitoring of daily steps

# RISK – FURTHER CLARIFIED



## **Absence of control is not a risk**

*E.g. Physical verification of stock is a control to detect misappropriation or incorrect recording – absence of it is not a risk*



## **Risk is relative to objectives**

*E.g. Rejection rate of 1% is not a risk if business objective already considers a 2% rejection*



## **Risks magnitude is highly subjective**

*. E.g. Stock differences of INR 50,000 may not be a risk at a company which has average stock levels of INR 50 Crores. It becomes a risk for auditing of a warehouse which has average stock levels of INR 500,000*

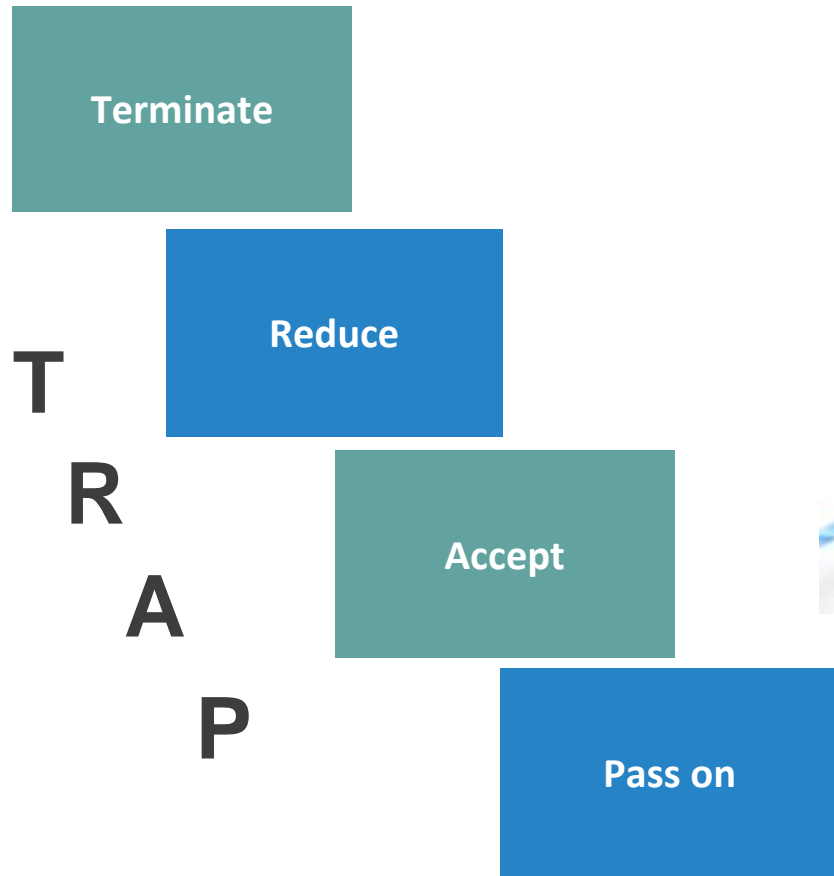


## **Risks are relative to industry**

*.E.g. Human resource related risk would be high and top priority for a IT company but may not be for a manufacturing company*



# DEAL WITH RISKS – CLASSIC FOUR WAYS



Impact / Likelihood

Certain	Reduce			Terminate	Terminate
Likely					
Moderate					
Unlikely					
Rare	Accept			Pass on	
	Insignificant	Minor	Moderate	Major	Catastrophic

*This helps the management and auditors to prioritize their attention and controls assessment as per risk ratings assigned to a risk*

Simply put, control is what's employed to reduce the likelihood of something going wrong.

To manage the inherent industry challenges and risks, an Organization should have a Robust Integrated Internal Control Environment. And thus need for implementing a widely accepted **control framework**



**FRAMEWORK**





Committee of Sponsoring Organizations of the Treadway Commission



# COSO Internal Control Framework – The Components & The Principles

# COSO – GLOBALLY ACCEPTED IC FRAMEWORK

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a **voluntary private sector organization** dedicated to **improving the quality of financial reporting** through business ethics, effective internal controls, and corporate governance. Based on these principles, the COSO framework was developed as a foundation for establishing internal control systems and determining their effectiveness. Originally formed in 1985, COSO is a joint initiative of five private sector organizations”



## COSO 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 Vision

COSO’s vision is to be a **recognized thought leader** in the global marketplace on the development of **guidance in the areas of risk and control** which enable good organizational governance and reduction of fraud.

# COSO – INTERNAL CONTROL 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 following objectives: Effectiveness and efficiency of operations, Reliability of financial reporting , Compliance with applicable laws and regulations.



**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** – 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.



# COSO OBJECTIVES – FURTHER ELABORATED



## OPERATIONS

- ✓ Effectiveness & efficiency of entity's operations
- ✓ Operational & Financial performance
- ✓ Safeguarding assets against loss
- ✓ Compliance with entity policies

- **GROWTH:** Grow revenue by X%
- **COST:** Reduce COP by X%
- **PROFITABILITY:** EPS of INR XXX
- **GEOGRAPHIC:** Enter new market
- **INFRASTRUCTURE:** Upgrade ERP
- **QUALITY:** Minimal defects



## REPORTING

- ✓ Internal & External
- ✓ Financial & Non-financial
- ✓ Reliability, Timeliness, Transparency
- ✓ Compliance with standards and entity policies

- Existence or occurrence
- Completeness
- Right and obligations
- Valuation or allocation
- Presentation and disclosure
- Internal reporting to management (MIS) and board (Quarterly)



## COMPLIANCE

- ✓ Adherence to laws & regulations
- ✓ To which the entity is subject

- Applicability of laws, rules & regulations
- Country specific laws and regulations
- Compliance monitoring
- Evidence and documentation

# COSO STRUCTURE

## CATEGORY OF BUSINESS OBJECTIVES (TOP)

- ✓ Effectiveness and Efficiency of Operations
- ✓ Reliability of Financial Reporting
- ✓ Compliance with Applicable Laws and Regulations

## FIVE COMPONENTS OF INTERNAL CONTROL

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

## HIERARCHY OF OBJECTIVES (SIDE)

May be set for the entity as a whole or targeted to specific divisions, operating units, or functions (business process)



- *An internal control structure is simply a different way of viewing the business - a perspective that focuses **on doing the right things in the right way.***
- **Principle based, not rule based:** *The Framework does not prescribe controls to be selected, developed, and deployed*
- **Management judgement:** *Selection of controls is a function of management judgment based on factors unique to the entity*

# COSO – CONTROL ENVIRONMENT

- Foundation upon which other components are built
- Tone at the top – Management attitude towards internal control
- Culture, history, management style, preferences
- Shared values of management and employees
- Permeates the company from top to bottom

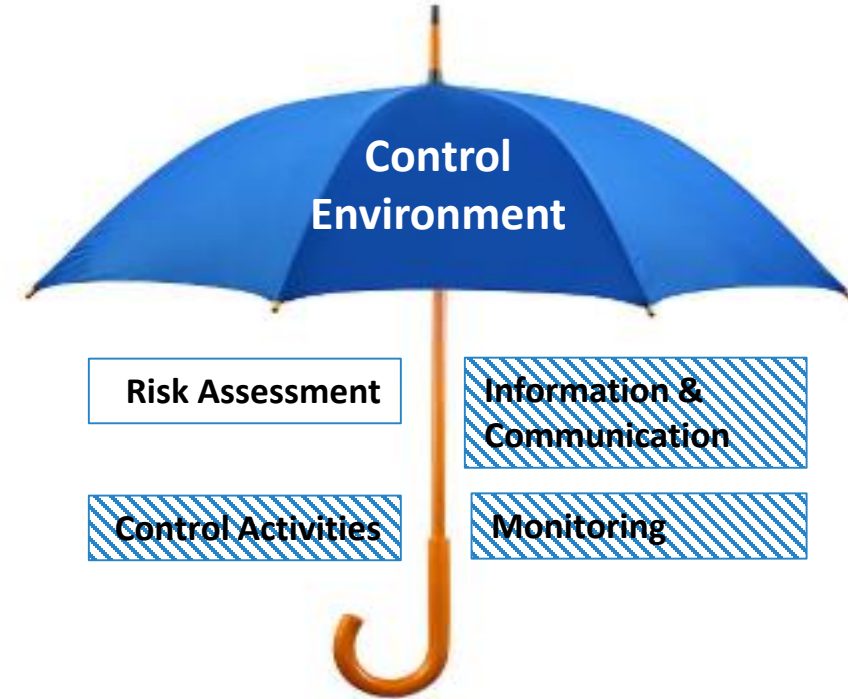


## COSO PRINCIPLES

- 1 Demonstrate commitment to integrity and ethical values**  
*Establishes standard of conduct; Evaluate adherence and addresses deviations*
- 2 BOD exercise oversight responsibility**  
*Applies relevant expertise; Operates independently; Oversee internal control*
- 3 Establishes structure, authority and responsibility**  
*Establishes reporting lines; Defines authorities and responsibilities*
- 4 Demonstrate commitment to competence**  
*Policies & procedures; evaluate competence; attract develop & retain individuals; Succession planning*
- 5 Enforces accountability**  
*Holds individuals responsible for IC responsibilities; Establishes performance measures, incentives and rewards and evaluates the same; Considers excessive pressure*

# COSO – RISK ASSESSMENT

- Established objectives prior to risk identification
- Determine critical success factor (CSF) of each objective
- Identify risks against each objective/ CSF
- Risk identification at entity and process level
  - Entity Level:** Competition, New Regulation, Natural disaster
  - Process Level:** RM inventory, Sub-standard quality, Fund utilization
- Likelihood and impact assessment of risk

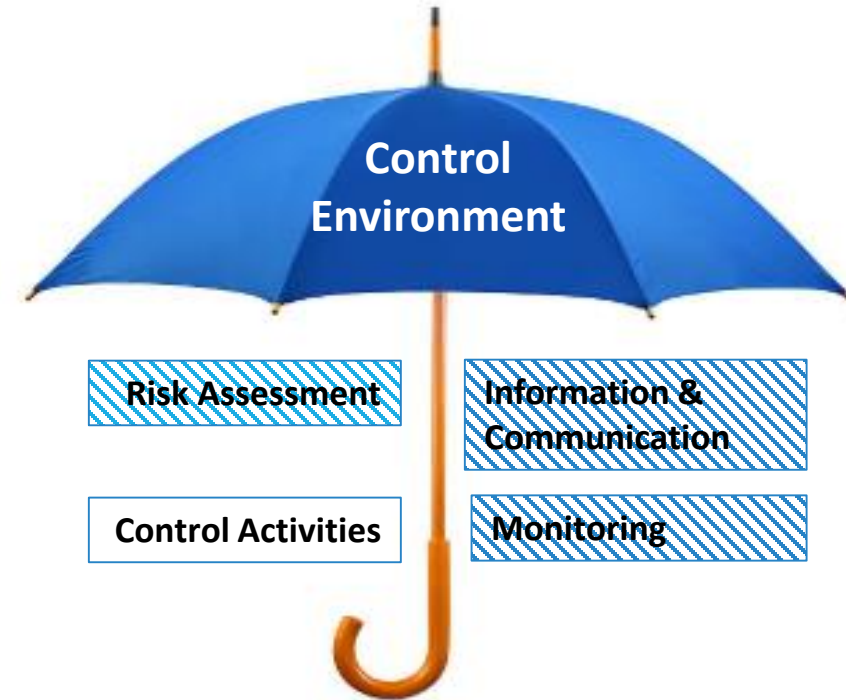


## **COSO PRINCIPLES**

- 6 Specify relevant objectives**  
*Operational; Financial & Non-financial; External & internal; Compliance*
- 7 Identify and analyzes risk**  
*Across entity against objectives; Internal & External; Involves appropriate levels; Determine risk response*
- 8 Assesses fraud risk**  
*Considers various types of frauds; Assesses incentives, pressures, opportunities, attitude and rationalization*
- 9 Identify and analyzes significant change**  
*Assesses changes in the external environment, business model and leadership*

# COSO – CONTROL ACTIVITIES

- Actions established by policies and procedures
- To manage risks – Integrated with risk assessment
- Mechanisms to achieve organization’s objective
- **Entity Level Controls:** Corporate wide, having pervasive effect on organization – e.g. Delegation of Authority, Whistle blower policy
- **Process Level Controls:** Directly involved with the step by step tasks or activities within a process – e.g. Three way match



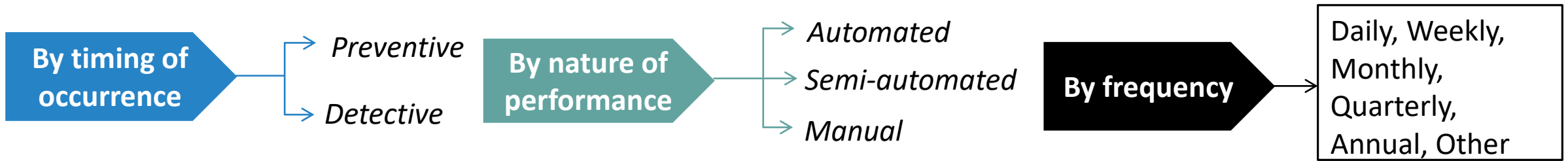
## **COSO PRINCIPLES**

- 10 Select and develop control activities**  
*Integrates with risk management; Entity specific, Across all levels, Addresses Segregation of Duties*
- 11 Select and develop general controls over technology**  
*Technology general, infrastructure, security and maintenance controls*

- 12 Deploy through policies and procedures**  
*Policies establishes what is expected and procedures put policies into action; Periodic review of policies & procedures*



# COSO – CONTROL ACTIVITY TYPES (1-2)

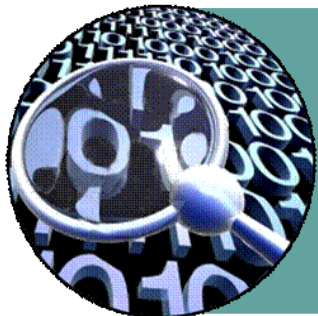


## PREVENTIVE

- Proactive in nature
- Prevents a problem within a process
- Normally applied at single transaction level
- Can be automated or manual

### EXAMPLES

- Purchase order approval
- Three way match
- Restricted access to ERP



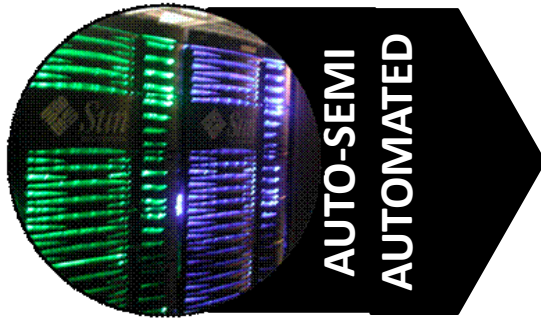
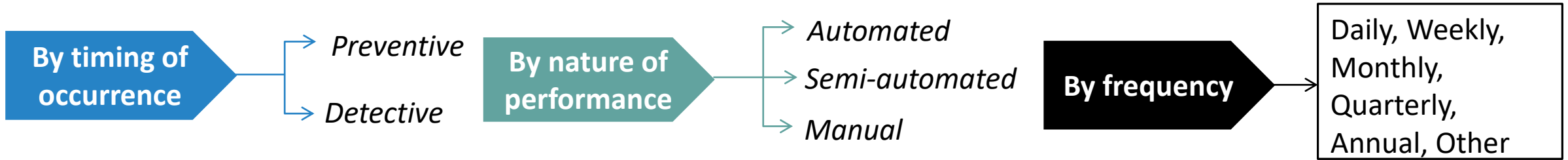
## DETECTIVE

- Catch errors that were not originally prevented
- Monitor reliability of preventive controls
- Applied to group of transactions
- Can be automated or manual

### EXAMPLES

- Variance analysis
- Reconciliations – Bank etc.
- Review of system change logs

# COSO – CONTROL ACTIVITY TYPES (2-2)



- Programmed to proactively mitigate risks
- Applied at root cause level
- Eliminate human intervention, non-judgmental
- Relies on system generated information






- EXAMPLES**
- Three way match
  - Doubtful debt provisioning
  - Prevent duplicate invoice processing



- Tasks manually performed
- To mitigate risks
- Through checks and approvals
- Susceptible to human error and judgement

- EXAMPLES**
- Inventory physical verification
  - MIS maker-checker
  - Lock & key control

# CONTROL ACTIVITIES – COMMONLY USED (1-2)

	<b>System Access</b>	Automated, Preventive, Continuous	Restricted access to vendor master, only limited people can pass JV etc.
	<b>System Configuration</b>	Automated, Preventive, Continuous	Alarms control at DCS, three way match of PO, GRN and Invoice
	<b>Authorization</b>	Manual or Automated, Preventive, Periodic or as needed	Invoice approval before payment, BOM change approval
	<b>Maker Checker</b>	Manual or Automated, Preventive, Periodic or as needed	Masters updated by IT department reviewed by end user, Performance MIS prepared by the team and reviewed by the Manager.
	<b>Segregation of Duties</b>	Manual or Automated, Preventive, Continuous	Company policy prohibits a single individual from being able to create a PO and approve payment for a related vendor invoice.

# CONTROL ACTIVITIES – COMMONLY USED (2-2)



## Policy & Procedures

Manual, Preventive, Continuous

Company has established policies and procedures, approved annually by the Executive Committee covering, instructions, limits, and controls are associated with the purchasing process.



## Physical Access

Manual or Automated, Preventive or Detective, Continuous

Physical access to the data center is protected by locked door requiring magnetic id badge and handprint biometric recognition to gain access



## Environmental Safeguards

Manual or Automated, Preventive or Detective, Continuous

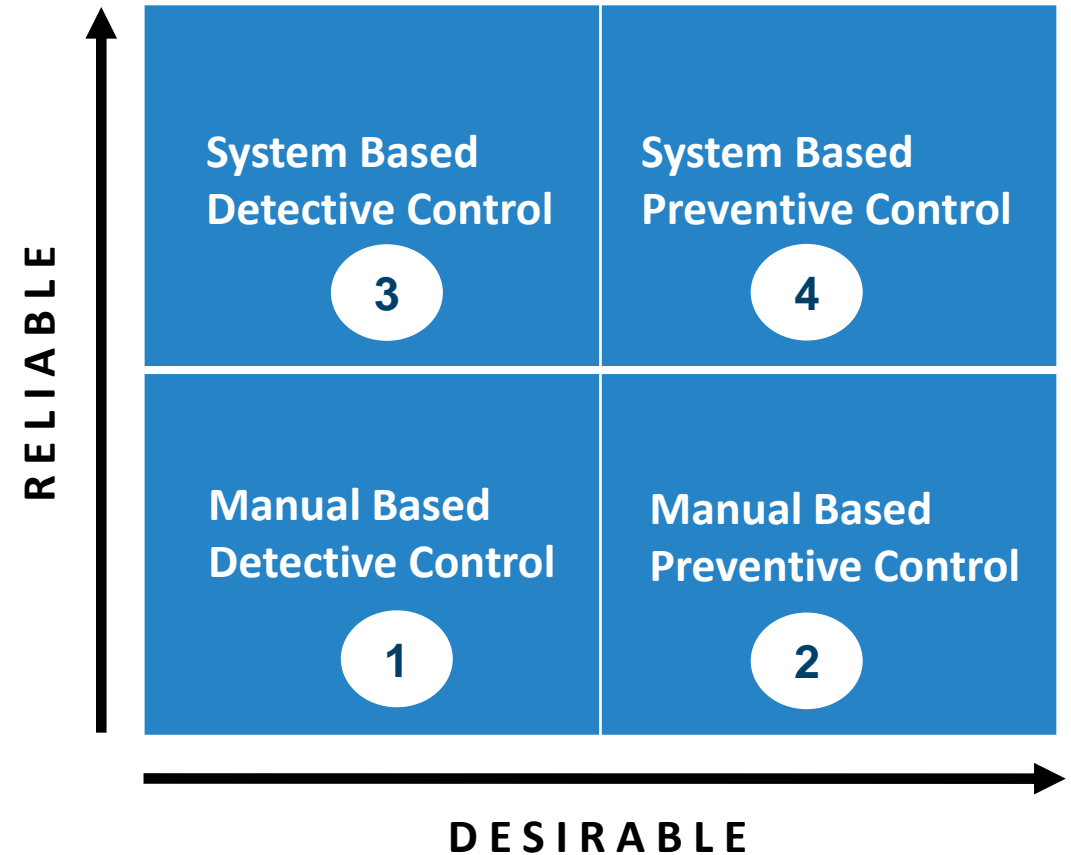
The data center is equipped with a fire suppression system to help ensure that the company's IT assets in the data center are protected from threats of fire.



# CONTROL RELIABILITY

As we consider different types of controls, it is important to note that some controls are more reliable than others.

To establish sound internal control compliance, an entity's aim is to have an adequate level of reliability to effectively mitigate risk to a sufficient level.



# A QUICK EXERCISE

Identify the type of control i.e. Preventive or Detective and Automatic, Semi Automatic or Manual

Payment to vendor is processed by the Accounts Officer and approved by the CFO in ERP system

Preventive	Detective	
Auto	Semi-Auto	Manual

Bank reconciliation performed on a monthly basis in excel sheet

Preventive	Detective	
Auto	Semi-Auto	Manual

Manual entry in security gate register before entering plant premises

Preventive	Detective	
Auto	Semi-Auto	Manual

System does not allow creation of GRN in excess of PO quantity

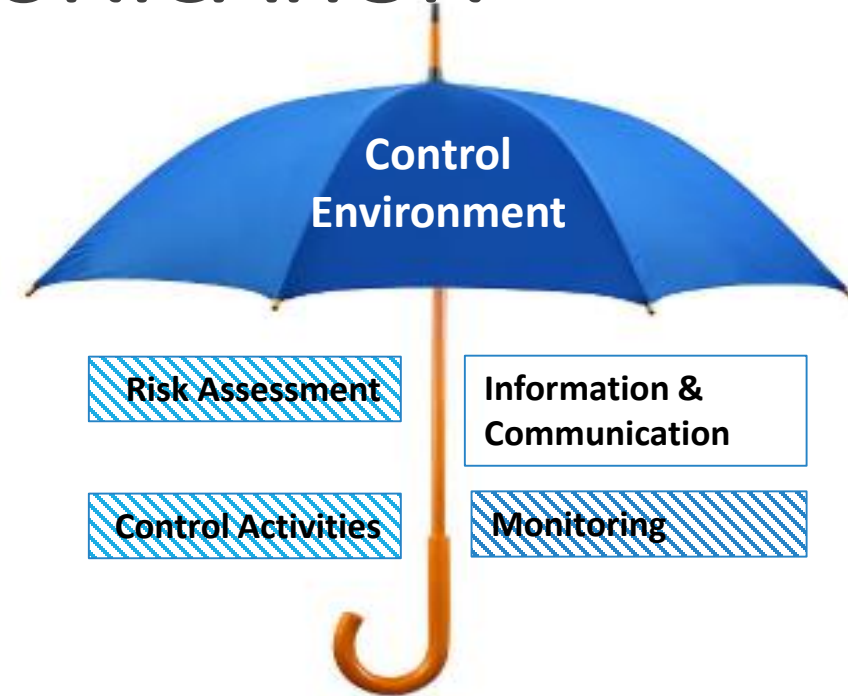
Preventive	Detective	
Auto	Semi-Auto	Manual

A pop-up warning to Manager in case his subordinates violates their access rights

Preventive	Detective	
Auto	Semi-Auto	Manual

# COSO – INFORMATION AND COMMUNICATION

- Support functioning of all other components
- Internal communication
- External communication – Inbound & Outbound
- Relevant and quality information only
- Establish communication lines and protocols
- For design, implement and conduct of internal controls and assess its effectiveness



## **COSO PRINCIPLES**

13

### **Generates and uses relevant and quality information**

*Identifies information requirements; Captures internal and external source of data; Processes data into information; Quality processing; Considers costs and benefits*

14

### **Communicates internally**

*Communicates objectives and IC responsibilities; Communication with BOD; Separate communication lines (Whistle-blower Hotline); Relevant method of communication*

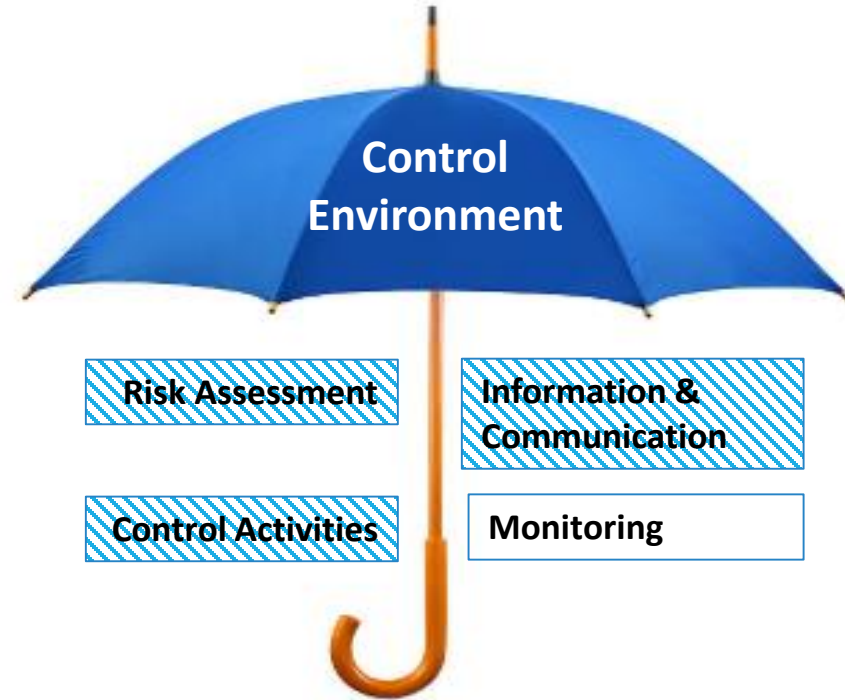
15

### **Communicates externally**

*Shareholders, partners, owners, regulators, customers etc.; Enable outbound and inbound communication; Separate communication lines (Whistle-blower Hotline)*

# COSO – MONITORING

- Evaluate whether each internal control component is **present, functioning and operating together**
- Whether control continues to be relevant or need a change
- **Ongoing or separate evaluation** or combination of both
- Process for capturing, reporting and timely communication of finding
- Organization's assessment of the effectiveness of internal control
- Follow-up on deficiencies



## **COSO PRINCIPLES**

- 16 Conduct ongoing and/or separate evaluations**  
*Consider rate of change; Establishes baseline understanding; Uses knowledgeable personnel; Integrates with business processes; Adjusts scope and frequency; Objectively conducts separate evaluations*
- 17 Evaluate and communicate deficiencies**  
*Assesses results of ongoing and separate evaluations; Communicates deficiencies to the management and BOD; Monitor corrective actions*



# COSO – MONITORING

## Monitoring Controls – Commonly used



### Monitoring or periodic review

Manual or Semi-Automated, Detective, As needed

Weekly operational and financial performance reports, budget vs. actual etc.



### Reconciliation

Semi- Automated or Automated, Detective, Periodic

Bank reconciliation, Physical and book inventory reconciliation

### Control activities

- Integral part of making business process work
- Embedded within the processes
- Prevent and detect errors and irregularities at source
- Provide assurance that relevant assertions are met

### Monitoring

- Evaluate performance of control activities
- To ensure that control activities are in accordance with objectives and performance criteria
- Ongoing and separate evaluation





Committee of Sponsoring Organizations of the Treadway Commission

# Internal Control Assessment



# INTERNAL CONTROL ASSESSMENT

**The assessment of design effectiveness addresses** whether the control activities, as designed, provide reasonable assurance that identified risks are mitigated and the stated financial reporting assertions are achieved.

---

**The validation of operational effectiveness** addresses whether the control activities are functioning as intended (i.e. are they performing as designed?).

---

**Internal Control Deficiency** refers to a shortcoming in a component or components and relevant principles that reduces the likelihood of an entity achieving its objectives. – **Deficiency, Significant Deficiency, Material Weakness**

- **External reporting:** Criteria set by regulators, standard setting bodies and other relevant bodies acceptable
  - **Internal Reporting:** Criteria set by board, senior management acceptable
- 





Committee of Sponsoring Organizations of the Treadway Commission

# Risk & Control Documentation



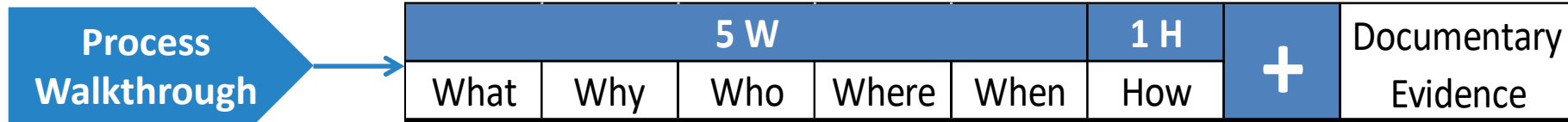
# RISK & CONTROL DOCUMENTATION

## Entity Level Control Documentation – Suggestive only

STEP 1	STEP 2	STEP 3	STEP 4
Principle	Points of Focus	ELCs to support the Principle	Documentary Evidence
<b>CONTROL ENVIRONMENT</b>			
<p><b>Principle 1: Demonstrates Commitment to Integrity and Ethical Values</b> – The organization demonstrates a commitment to integrity and ethical values.</p>	<ul style="list-style-type: none"> <li>• <b><i>Sets the Tone at the Top</i></b> – The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.</li> <li>• <b><i>Establishes Standards of Conduct</i></b> – The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity’s standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.</li> <li>• <b><i>Evaluates Adherence to Standards of Conduct</i></b> – Processes are in place to evaluate the performance of individuals and teams against the entity’s expected standards of conduct.</li> <li>• <b><i>Addresses Deviations in a Timely Manner</i></b> – Deviations of the entity’s expected standards of conduct are identified and remedied in a timely and consistent manner.</li> </ul>	<ol style="list-style-type: none"> <li>1. XXXXXXXXX</li> <li>2. XXXXXXXXX</li> <li>3. XXXXXXXXX</li> <li>4. XXXXXXXXX</li> </ol>	<ol style="list-style-type: none"> <li>1. XXXXXXXXX</li> <li>2. XXXXXXXXX</li> <li>3. XXXXXXXXX</li> <li>4. XXXXXXXXX</li> </ol>
<b>STEP 5</b>	Principle 1 - Are the ELCs deployed across the entity to demonstrate the Principle is present?	Yes or No	If No, describe the gap and action plan
		Yes	Not applicable.

# RISK & CONTROL DOCUMENTATION

## Process Level Control Documentation – Suggestive only



- Major process & sub-process
- Activity
- Risk description and risk heat
- Control description
- Control owner
- Control evidence
- Financial statement assertions
- Control frequency, type, method, nature  
*Preventive, Detective, Automated, Manual, Application etc.*
- Key / Non-key control
- Gap, implementation plan & timelines



**Risk & Control Matrix (RCM)**



Committee of Sponsoring Organizations of the Treadway Commission

# Internal Control – Indian Legal Perspective



# INTERNAL CONTROL – INDIAN LEGAL PERSPECTIVE

## Standard on Auditing (SA) 315

Standard on Auditing (SA) 315, “Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment”

*“The process designed, implemented and maintained **by those charged with governance, management and other personnel** to provide **reasonable assurance** about the achievement of an entity’s **objectives** with regard to reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets and compliance with applicable laws and regulations. The term **“controls”** refers to **any aspects of one or more of the components of internal control**”.*

## Section 134 of the Companies Act 2013

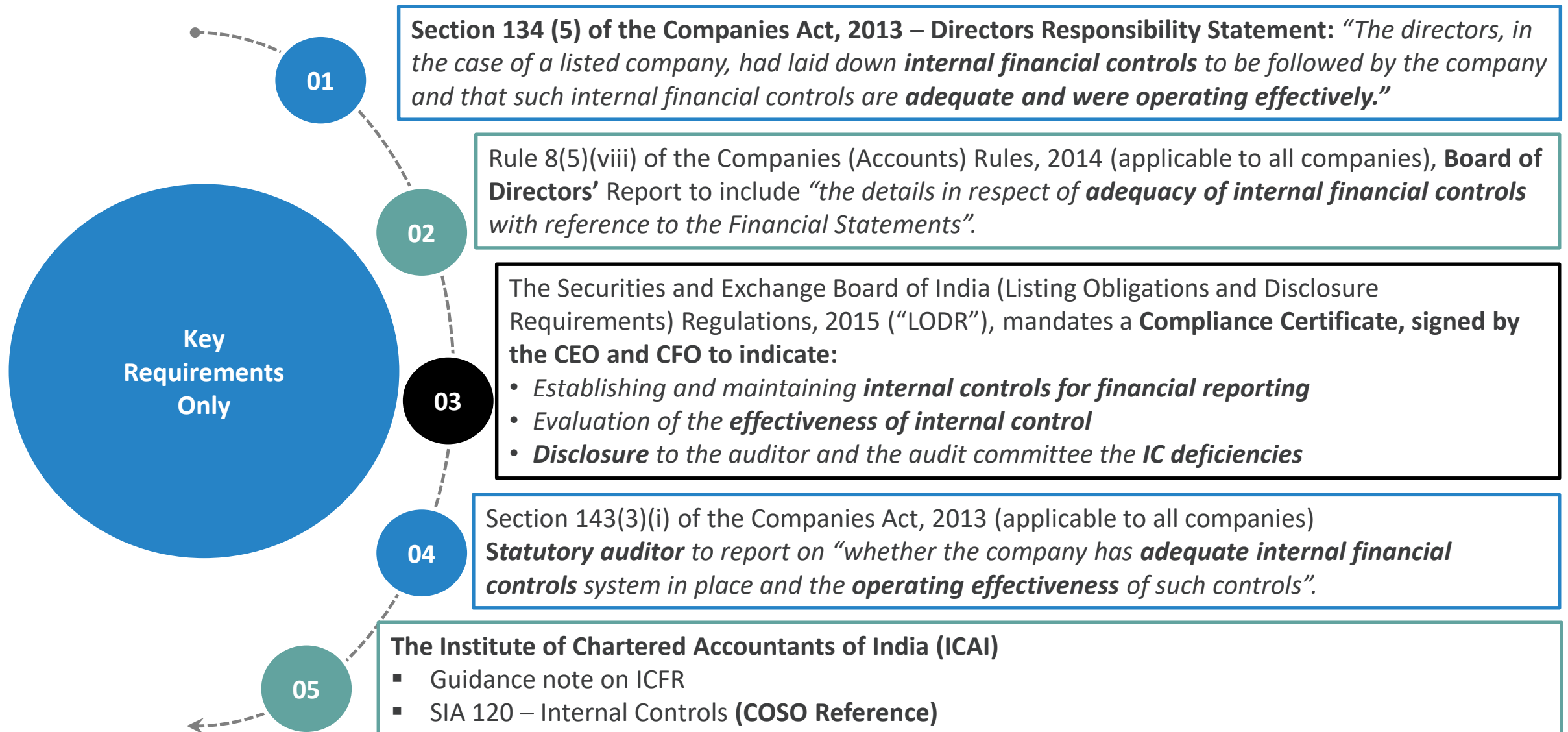
Section 134 (5) of Companies Act, 2013, (applicable to listed companies) concerning Directors’ Responsibility Statement vide clause (e) thereof, defines the term **“Internal Financial Controls”** as follows:

*“**The policies and procedures** adopted by the company for ensuring the **orderly and efficient conduct** of its business, including adherence to company’s policies, the **safeguarding of its assets, the prevention and detection of frauds and errors**, the accuracy and completeness of the **accounting records**, and the **timely preparation** of reliable financial information”.*





# INTERNAL CONTROL – INDIAN LEGAL PERSPECTIVE





Committee of Sponsoring Organizations of the Treadway Commission



# Internal Control – Benefits and Limitations

# INTERNAL CONTROL – BENEFITS & LIMITATIONS



More value to:

- Business partners
- Investors
- Government
- Regulators



Strong governance and compliance culture

Complete and accurate financial reporting

Effective and timely communication

Legally compliant

Prevent and detect errors and frauds

Assets safeguarded

Improved efficiency and resource utilization

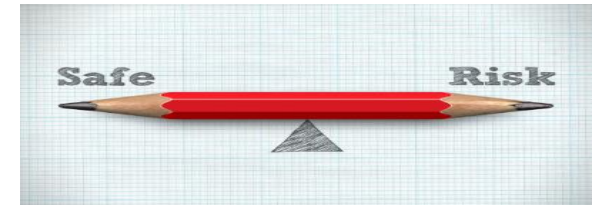
Authorized transactions and transparency

**STRONG INTERNAL CONTROLS**



**LIMITATIONS**

- Suitability of objectives as a pre-condition to IC
- Human judgement can be faulty and biased
- Breakdown due to human error
- Cost of control more than the benefit
- Over or under controlled environment
- Management override of internal controls
- Collusion/ Fraud
- External events beyond control



# INTERNAL CONTROL CAN BE GAME CHANGER

One of India's largest supermarket success story – Its not only right strategy, its right implementation of the strategy through effective internal controls

- Shares got listed at more than 100% premium
- Valued at around INR 40,000 Crores, much more than the competitors
- Strategies like, pay suppliers and vendors within days instead of weeks which was the industry norm
- Passed on the cost benefits to his customers, which ensured consistent footfall.
- **Devised pin point plan for effective execution of strategies**
- Not shut a single store since it started

*Source: Moneycontrol and Public Domain*





## Q & A

**Under Control**

**CA MANINDRA PRAKASH**

**[manindrakra@gmail.com](mailto:manindrakra@gmail.com)**

**+91 99670 46497**

**<https://www.linkedin.com/in/manindrakra/>**

**THANK**

**YOU**

