

## **Presentation on Internal Controls**

February 13, 2022

Private and confidential

The views expressed in this session are my personal views and not the views of organization where I work

# Contents

- Understanding internal controls
- Types of controls and Management control Techniques
- Internal controls on the accounting function
- Internal financial controls frameworks
- Role of internal auditors in implementation of internal controls and risk management
- Examination of effectiveness of Internal Controls

# What is risk and risk management

- Risk implies future **uncertainty**, it is measured in terms of **impact and likelihood**
- Whether wickets are taken by bowlers or fielders?
- Can business achieve its objectives without managing risks?
- Whether all risks require same treatment?
- Which hospital you would prefer for minor ailment vs bypass surgery?
- Would you wear your best dress during local shopping or in meeting/wedding?

**Risks are numerous, resources are limited, use it wisely**

# Global risk and controls framework - COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework defines internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives in the following categories:

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



# Global risk and controls framework - COSO

## Control environment – **At entity level**

- **Demonstrates commitment to integrity and ethical value**
- **Exercises oversight responsibility** - Independence from Management and exercises oversight in development and performance of internal control
- **Establishes structure, authority, and responsibility**
- **Demonstrates commitment to competence** - Attract, develop, and retain competent individuals in alignment with objectives
- **Enforces accountability** – Individuals accountable for their internal control responsibilities in the pursuit of objectives

## Risk assessment – **Enterprise risk management**

- **Specifies suitable objectives** – For identification/ assessment of risks
- **Identifies and analyze risk**

# Global risk and controls framework - COSO

- **Assesses fraud risk** – potential for fraud in assessing risks
- **Identifies and analyze significant change** - Affecting internal control

## **Control activities – Internal Controls**

- **Select and develops control activities** – For mitigation of risk
- **Select and develops general controls over technology**
- **Deploy control activities through policies and procedures** – Policies establish expectation and procedures action the policies

## **Information and communication – To strengthen Internal Controls**

- **Uses relevant information** – To support functioning of internal control
- **Communicates internally** – Information, including objectives and responsibilities for internal control
- **Communicates externally** – matters affecting internal control

# Global risk and controls framework - COSO

## **Monitoring – Internal/external audits and control self assessment**

- **Conducts ongoing and/or separate evaluations** - To ascertain whether the components of internal control are present and functioning
- **Evaluates and communicates deficiencies** – For corrective actions

# Internal control on the accounting function

- Well defined policies and procedures
- Roles and responsibilities should be documented and segregated
- System access are on "Need to know" basis
- Systems controls on various masters in ERP system, maker checker controls, journal entries and restrictive access of FICO module
- Book closing guidelines should be documented and reviewed
- Restrictive access to open closed period, activities after reopening period should be monitored for supporting and accuracy
- Consistent accounting policies to avoid individual judgment on inventory valuation, provision, accruals, write-off, impairment etc.

# Internal financial controls

## Companies Act requirements

### Director's responsibility statement

Section 134(5)(e) - The directors, in the case of a listed company, had laid down **internal financial controls** to be followed by the company and that such internal financial controls are **adequate** and were **operating effectively**.

Section 134(5)(f) - The directors had devised proper systems to ensure **compliance with the provisions of all applicable laws** and that such systems were **adequate** and **operating effectively**.

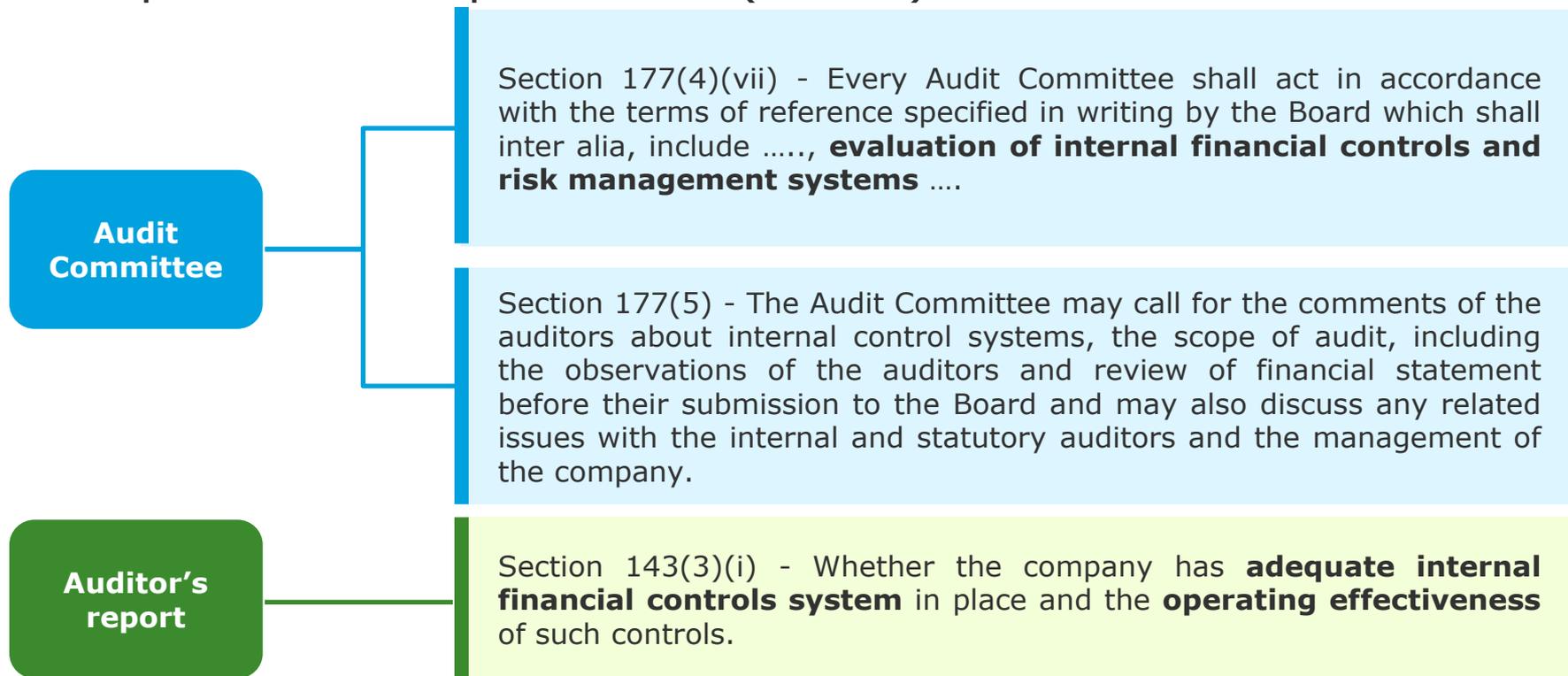
Section 134(3)(q), sub-rule 8(5) - "In addition to the information and details specified in sub-rule (4), the report of the Board shall also contain: ..."the details in respect of adequacy of **internal financial controls** with reference to the **financial statements**."

Explanation - For the purpose of this clause "Internal Financial Controls" means 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 financial controls reporting covers not just financial reporting aspects, but also the strategic and operational aspects of business and the efficiency with which those operations are carried out**

# Internal financial controls

## Companies Act requirements (contd.)



Whilst section 134(5) requires directors to state their responsibility on internal financial controls in case of listed companies, auditors are required to report on the adequacy and operating effectiveness of such controls in case of all companies.

Further, Rule 8(5)(viii) of the Companies (Accounts) Rules, 2014 requires the board report of all companies to state the details in respect of adequacy of internal financial controls with reference to the financial statements.

# Internal financial controls – What is expected?

	IFC Objective	IFC Requirements	What to do ?
Operations Objectives	Efficiency and effectiveness in Operations	<ul style="list-style-type: none"> <li>Defined <b>Policies and procedures</b> to ensure effective and efficient operations.</li> <li>Effective <b>Delegation of Authority</b> and <b>Entity level controls</b></li> </ul>	<ul style="list-style-type: none"> <li>Define and ensure compliance to appropriate policies and procedures and Delegation of Authority</li> <li>Define appropriate Entity level controls</li> <li>Define and monitor operating effectiveness of appropriate controls over various activities.</li> <li>Fraud Risk Management</li> </ul>
	Prevention and detection of fraud and error	<ul style="list-style-type: none"> <li>Preventive controls to address <b>Fraud risk</b></li> <li>Mechanism for <b>timely detection</b> of fraud and errors</li> </ul>	
	Safeguarding of assets	<ul style="list-style-type: none"> <li>Adequate control over <b>asset movement</b>, storage, loss or theft.</li> <li>Risk identification and mitigation plan to reduce loss of asset</li> </ul>	
Reporting Objectives	Accuracy and completeness of Accounting records	<ul style="list-style-type: none"> <li>Controls over <b>accurate and timely</b> update of accounting records</li> <li>Control over <b>completeness</b> of accounting records</li> </ul>	Defined effective controls and ensure operating effectiveness (ELC, PLC, ITGC and Fraud Risk)
	Reliability of Financial reporting	<ul style="list-style-type: none"> <li><b>Timely</b> preparation of financial reports</li> <li>Adequate <b>controls over preparation</b> of financial reports</li> </ul>	<ul style="list-style-type: none"> <li>Defined appropriate controls over preparation of financial reports</li> <li>Adequate review mechanism</li> </ul>
Compliance Objectives	Compliance with applicable laws and regulations	<ul style="list-style-type: none"> <li>Adequate <b>framework</b> to ensure compliance to applicable laws and regulations</li> <li>Adequate framework to <b>monitor</b> the compliance</li> </ul>	Legal Compliance Framework

# Internal financial controls

## Entity level controls

ELC Component	Requirement
Business Risk Management	Whether <b>risk management policy and procedures are in place</b> ? Whether formal risk assessment has been carried out or not?
Business Ethics Framework	Whether <b>whistle-blower policy and Code of conduct</b> exists and implemented ?
Internal Audit and Financial Integrity	Whether <b>internal audit function is independently reporting to Audit Committee</b> ? Whether <b>roles and responsibilities</b> of senior management is defined and documented? And Whether adequate <b>segregation of duties</b> exists?
Legal Compliance Framework	Whether <b>legal compliance framework</b> is documented and compliance health to checked on periodic basis?
Fraud Risk Management	Whether Fraud Risk Management policy exists, detailing structure of fraud deterrence, prevention and investigation, fraud incidence response guidelines. Whether <b>Key controls to mitigate fraud risks</b> are identified and monitored for compliance on regular basis.
Business and Operations Continuity	Whether <b>Disaster Recovery Plan, Business continuity plan</b> and crisis management policy defined and implemented?
Succession Planning	Whether formal process of <b>succession planning</b> defined and implemented?
Management Review	Whether formal process <b>management oversight and review mechanism</b> exist and followed?

# Internal financial controls

## Process level controls

### PLC Component

### Requirement

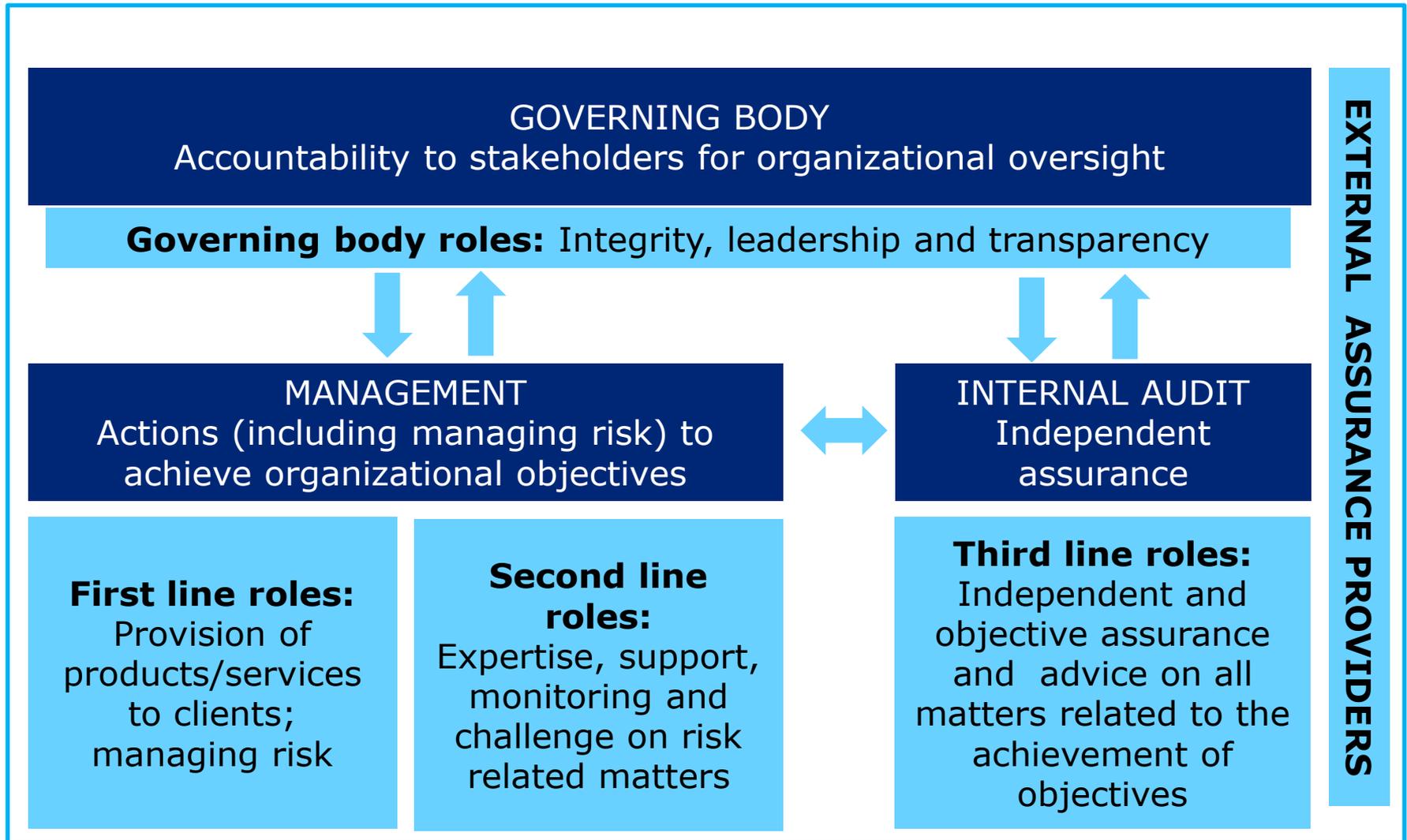
#### Design Effectiveness

**Significant policy and procedures are defined.** Process of assessing adequacy and appropriateness of policies and process to be developed

Completeness of RCM documented for all business cycles to be assessed. Example RCM for Treasury etc. to be prepared. Existing RCM to include following:

- Review and update RCMs for all financial assertions.
- Controls description to be elaborated
- Fraud Risk to be highlighted
- Whether Policy/ Procedure exists or not to be documented
- Control Category specifying COSO control level
- Control Owner and responsibility for testing and reporting

# The IIA's Three Lines Model



**KEY:**  Accountability, reporting  Delegation, direction, resources, oversight

 Alignment, communication, coordination, collaboration

# The IIA's Three Lines Model

## Principle #1: Governance

**Governance of an organization** requires appropriate structures and processes that enable:

- **Accountability** by a governing body to stake-holders for organizational oversight through integrity, leadership, and transparency.
- **Actions** (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.
- **Assurance and advice** by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

# The IIA's Three Lines Model

## **Principle #2: Governing body roles**

### **The governing body ensures:**

- Appropriate structures and processes are in place for effective governance.
- Organizational objectives and activities are aligned with the prioritized interests of stakeholders.

### **The governing body:**

- Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.
- Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

# The IIA's Three Lines Model

## Principle #3: Management and first and second line roles

- **Management's responsibility to achieve organizational objectives** comprises both first- and second-line roles.
- **First line roles are most directly aligned with the delivery of products and/or services** to clients of the organization, and include the roles of support functions
- **Second line roles provide assistance with managing risk.**
- First and second line roles may be blended or separated. Some **second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles.**
- Second line roles can focus on specific objectives of risk management. Alternatively, second line roles may span a broader responsibility for risk management, such as enterprise risk management. However, responsibility for managing risk remains a part of first line roles and **within the scope of management.**

# The IIA's Three Lines Model

## Principle #4: Third line roles

**Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.** It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to management and the governing body to promote and facilitate continuous improvement. **In doing so, it may consider assurance from other internal and external providers.**

# The IIA's Three Lines Model

## **Principle #5: Third line independence**

Internal audit's **independence from the responsibilities of management is critical to its objectivity, authority, and credibility.** It is established through; accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

## **Principle #6: Creating and protecting value**

All roles working together collectively contribute to the creation and protection of value when they are **aligned with each other and with the prioritized interests of stakeholders. Alignment of activities is achieved through communication, cooperation, and collaboration.**

**Questions?**

Thank you