

Risk Management and Control: Beauty or Beast?

14 March 2014

Geremew Tadele

CONTENT

- ❑ *First impression on risk and control*
- ❑ *What is risk, What is control (current context)?*
- ❑ *Relationship between organizational objectives and risk*
- ❑ *Why risk management?*
- ❑ *Internal control within risk management*
- ❑ *Key stakeholders of risk management*
- ❑ *Tips for effective risk management*

WHAT IS YOUR FIRST IMPRESSION ON: RISK?



Risk is a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities: *Business dictionary.com*

Risk is the possibility of suffering harm or loss; danger:
Free Online Dictionary

WHAT IS YOUR FIRST IMPRESSION ON: INTERNAL CONTROL?



Internal Control is an accounting procedure or system designed to promote efficiency or assure the implementation of a policy or safeguard assets or avoid fraud and error etc. **Free online**

Dictionary

Is this your impression on Risk?



- “Risk is what an entrepreneur eats for breakfast. It's what she sleeps into bed with at night. If you have no appetite for this stuff, or no ability to digest it, then get out of the game right now.” *Heather Robertson*
- “My client loved risk. Risk, I had learned, was a commodity in itself. Risk could be canned and sold like tomatoes.” *Michael Lewis*
- “If you only take small risks, you are only entitled to a small life.” *Robin S. Sharma*

WHAT IS RISK (CURRENT CONTEXT)?



Risk is the '*effect of uncertainty on objectives*'. ISO:31000

Three key aspects of risk:

Organizational Objective: Preserving or creating value.

Effect: A deviation from the expected (positive /negative).

Uncertainty: The state of deficiency of information related to understanding or knowledge of an event.

RISK.....

‘Event can have negative impact, positive impact, or both. Events with a negative impact represent risk, which can prevent value creation or erode existing value. Events with positive impact may offset negative impact or represent opportunities’. COSO ERM

The two faces of risk: There is a potential for events to constitute opportunities for benefit (*upside of risks*) and threats to success (*downside of risks*).

WHAT IS CONTROL (CURRENT CONTEXT)?



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. COSO

Key Words:

- Effected by people
- Achievement of objectives
- Reasonable assurance

INTERNAL CONTROL....

Why **reasonable assurance** and not **absolute assurance**:

- Human judgment in decision making could be faulty
- Control breakdown may occur due to human failures/ mistakes
- Controls can be circumvented by collusion of two or more people
- Management override
- Decisions in establishing controls need to consider the relative costs and benefits

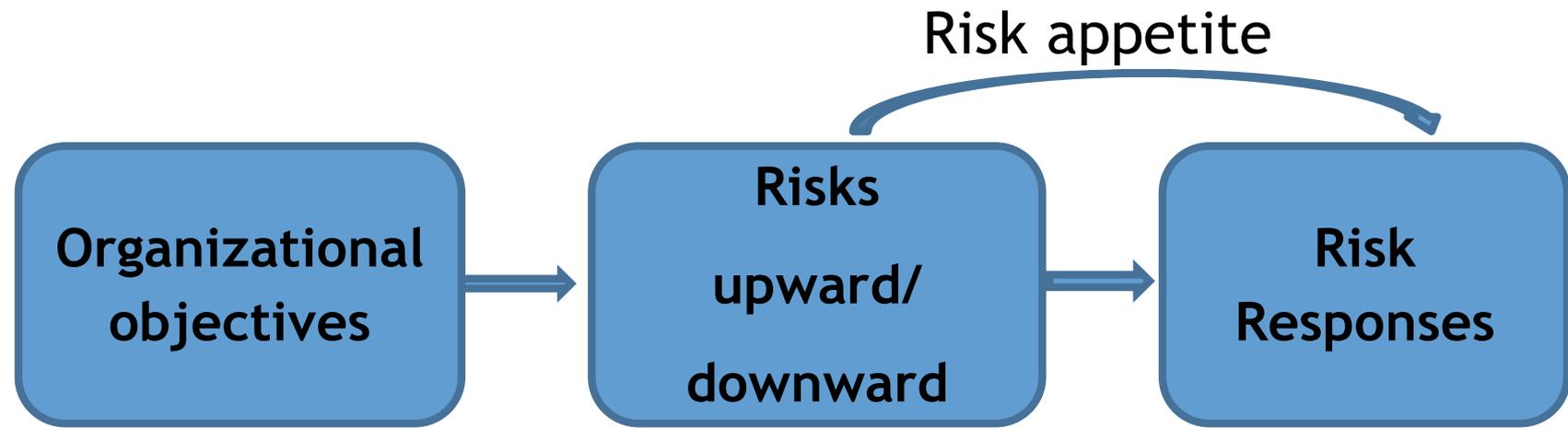
RELATIONSHIP BETWEEN ORGANIZATIONAL OBJECTIVES & RISK

- An organization is established for a reason...
- The main objective of an organization is to create and/or preserve value to stakeholders.
- Almost every key **decision** in creating and/or preserving organizational value requires balancing **risk and reward**.
- Thus organizational objectives and risks are interlinked. ***One does not exist without the other.***

RELATIONSHIP BETWEEN ORGANIZATIONAL OBJECTIVES & RISK

In order to survive, organizations need to ***take calculated risks*** with informed decisions and ***seize opportunities***.

- "How many millionaires do you know who have become wealthy by investing in savings accounts? I rest my case." *Robert G. Allen*
- "He who doesn't risk never gets to drink champagne."
Russian Proverb
- "It's important to take risks but it's idiotic to take them blindly." *Terry Levine*



What is the mechanism to take the right balance of risk to pursue organizational objectives?

WHY RISK MANAGEMENT?

“If you do not actively attack the risks, they will actively attack you.” *Tom Gib*



“Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.”

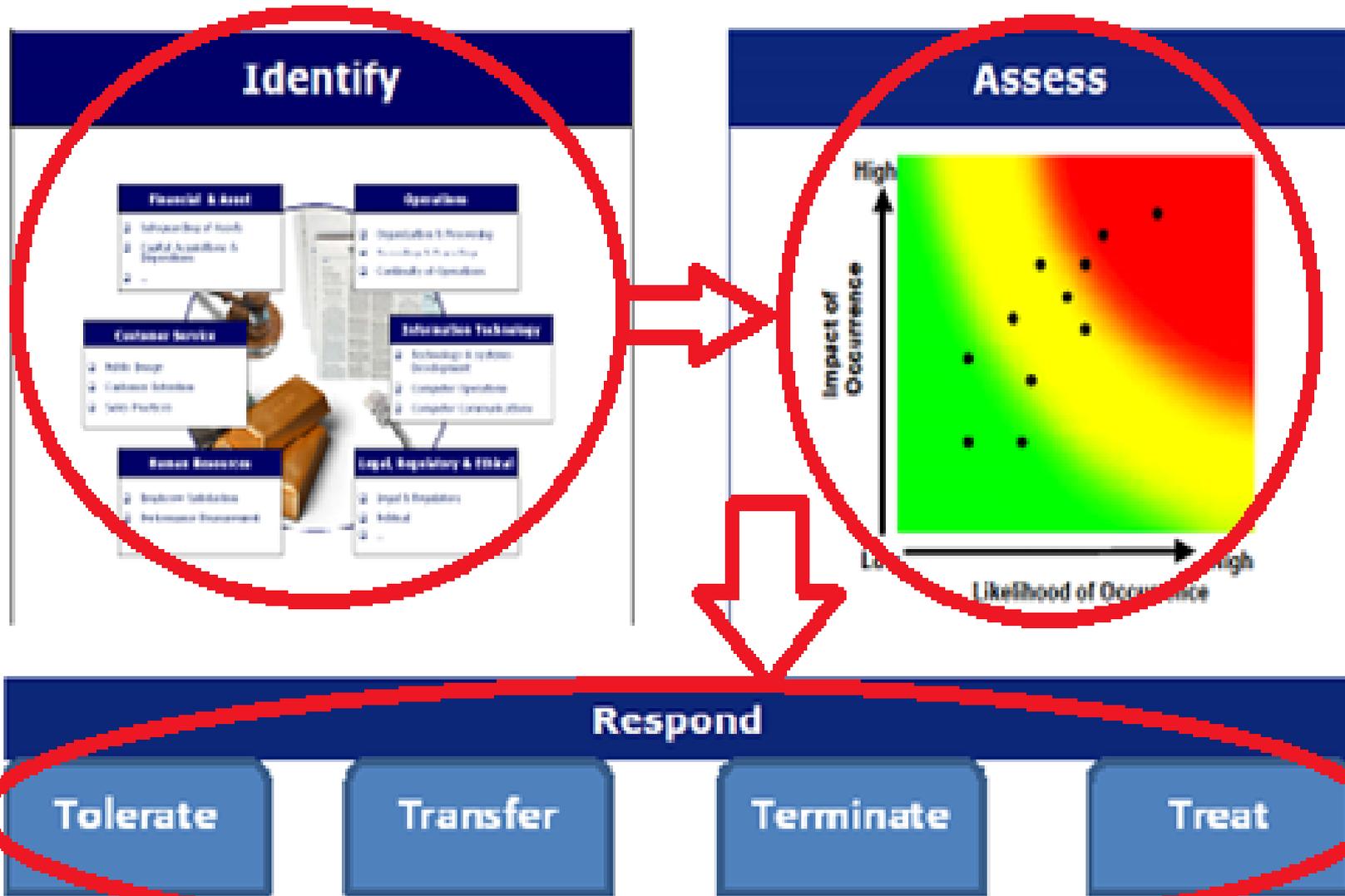
Theodore Roosevelt

RISK MANAGEMENT

Risk management is coordinated activities to direct and control an organization with regard to risk. *ISO 31000*

Risk management is the *identification, assessment,* and *prioritization* of risks followed by coordinated and economical application of resources to minimize, **monitor**, and control the *probability* and/or impact of unfortunate events or to maximize the realization of opportunities. *<http://en.wikipedia.org>*

RISK MANAGEMENT PROCESS



RISK MANAGEMENT.....

Effective risk management:

- ✓ Allows for responsible risk taking in pursuit of return
- ✓ Encourages innovation
- ✓ Builds a risk-smart workforce
- ✓ Assist in making informed business decisions

One of the risk management principles is to help decision makers make informed choices, prioritize action and distinguish among alternative courses of action. (ISO:31000)

INTERNAL CONTROL WITHIN IN RISK MANAGEMENT



Internal control is an integral part of risk management.

If no risk no need for internal control!

4T Risk Response: Tolerate (retaining risk by informed decision),

Transfer (sharing risk with another party or parties) and

Terminate (avoiding the risk by deciding to drop the activity)

Treat (modifying risk through control measures),

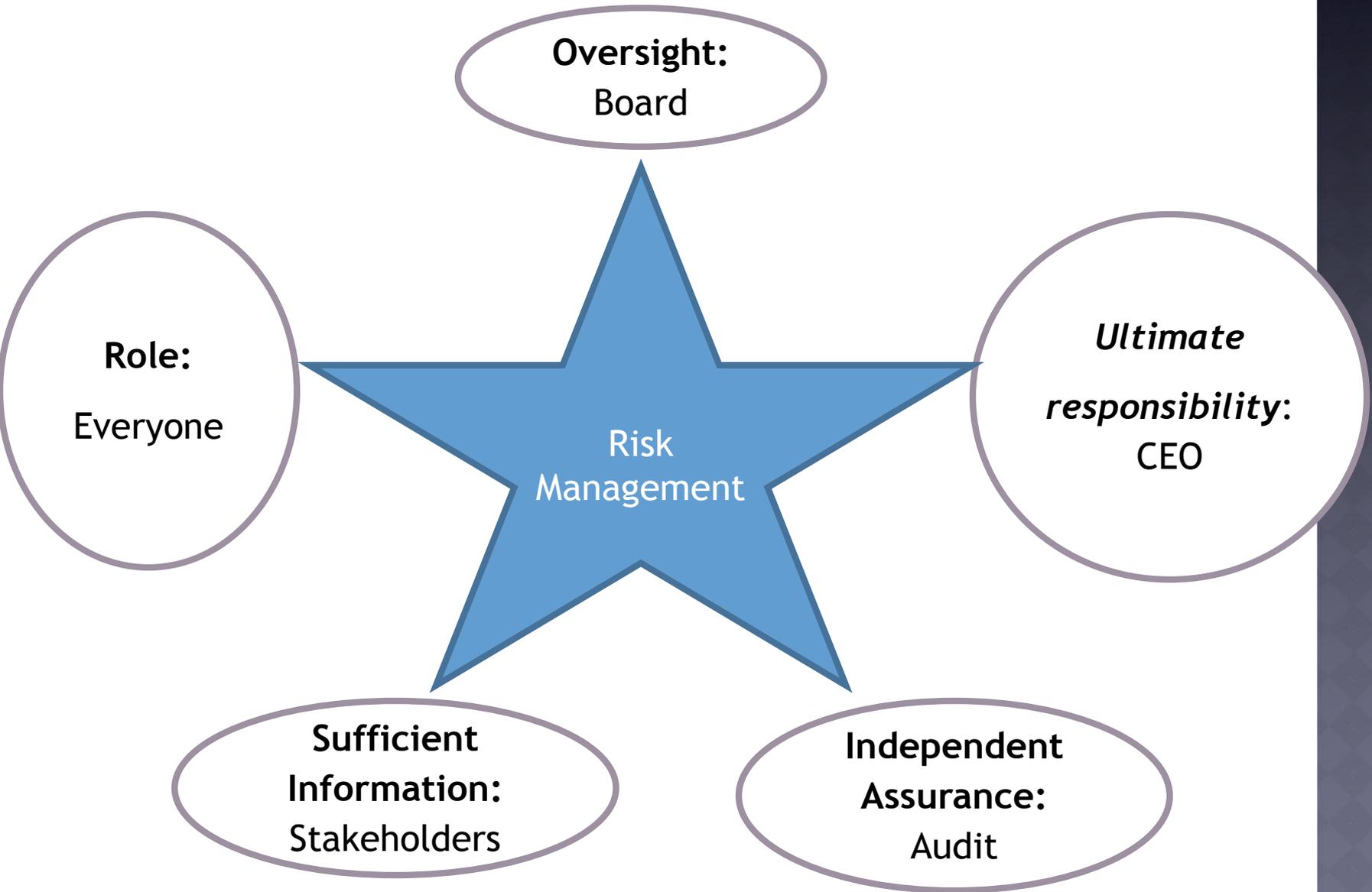
Effectiveness of Internal Control is assessed:

- i. by the extent to which risks are reduced by the control measures.
- ii. with cost effectiveness (cost of implementing the control compared to the risk reduction benefits achieved).

Internal controls without purpose, ineffective and costly internal controls are one of the major risks to an organization.

Ineffective /inefficient control lacks the agility and innovation to exploit new opportunities.

KEY STAKEHOLDERS OF RISK MANAGEMENT



Board/Governing body:

- Establish the structure for risk management
- Determine strategic approach to risk and set risk appetite
- Oversight on risk management
- Comprehension of key organizational risks
- Manage organization in a crisis

CEO/Management:

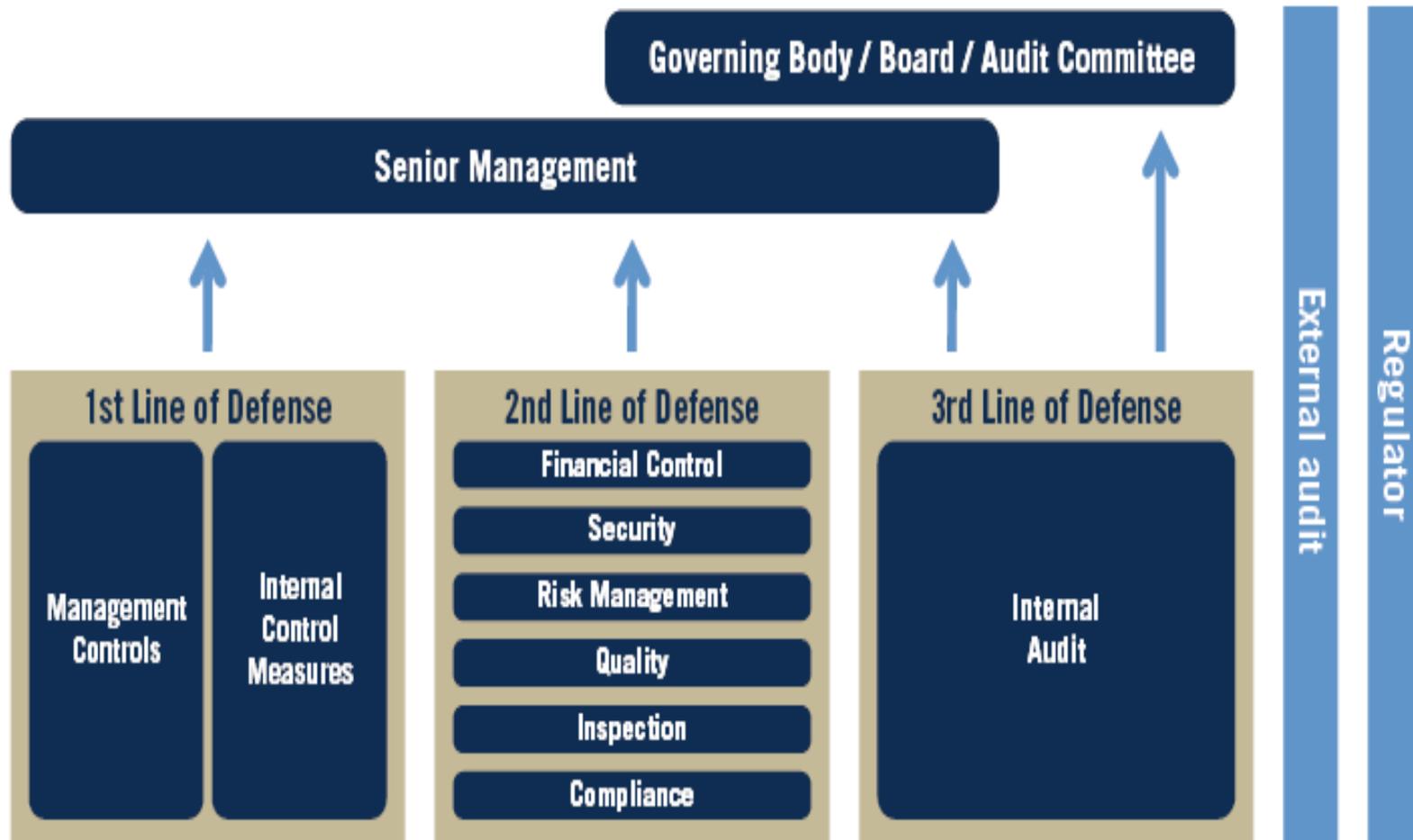
- ❑ Primary responsibility for identifying and managing risks
- ❑ Responsible for setting the organizational attitude regarding risk
- ❑ Build risk aware culture
- ❑ Set up risk management systems and Key Risk Indicators (KRI)
- ❑ Ensure implementation of risk improvement measures
- ❑ Coordinate risk management and internal control activities

Internal Audit:

Provides independent and objective assurance on:

- the risk management process itself
- significant risk and management assertions
- the follow up of risk treatment plans
- adequacy and effectiveness of controls **(Risk are not over controlled or inefficiently controlled)**

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

TIPS FOR EFFECTIVE RISK MANAGEMENT

i. Risk Culture (Fundamental):

- a) Creating a positive attitude towards risk and risk management
- b) Embedding risk management in to all the organization's practices and process. ***Risk management should not be seen in isolation.***
- c) Developing a culture of learning from experience. Avoiding blame without treating root cause.
- d) Behavior towards acceptable risk taking. ***Avoid reckless risk taking.***
- e) Behavior towards following/complying with policy.
- f) Appropriate performance measures, accountability for action.

'Tone at the top' is key ingredient in developing conducive risk culture

ii. People- centered risk management approach:



- “Better to have a simple model backed by **excellent people** than the other way around.” *Paul Carrett*
- “The kinds of errors that cause plane crashes are invariably errors of **teamwork** and communication.” *Malcolm Gladwell*

Engaging, participatory, interactive risk management process!

iii. Monitoring and Communication



An organization needs to have a mechanism for ongoing monitoring or periodic evaluation on risk management.

It will assist management to determine whether the risk management process continues to be **relevant** and able to address new risks.

Ongoing monitoring need to be inbuilt into the normal, recurring operating activities of the organization.

Continuous, truthful, accurate and understandable exchanges of information within an organization are key aspects of effective risk management.

Note: Ongoing monitoring is more effective than separate evaluation.

iv. Attention to strategic and reputation risks

- “Fail to identify the strategic risks and you fail as a business, no matter how well you manage your operational and project risks.” *Keith Baxter*
- “It takes 20 years to build a reputation and 5 minutes to ruin it and if you understand this you will do things differently” *Warren Buffett*

FINAL THOUGHT.....



- Should Risk Management and Control be Imposed or Owned?
- Should Risk Management and Control be Preventive or Curative?
- Is Risk Management and Control Beauty or Beast?



The END!!!