

# 1st Capacity Building Seminar on Enterprise Risk Management

Hotel Sea Princess, Mumbai  
10<sup>th</sup> August 2018

## ERM as a Business Enabler

N K V Roop Kumar, EVP, Chief of Risk, Info & Cyber  
Security Management, SBI Life Insurance Co. Ltd.



Institute of Actuaries of India

# Contents

- How does ERM add Value
- Roles & Responsibilities of ERM
- How does 3 Lines of Defense interact
- Risk Assurance to the Stakeholders

# How does ERM add Value

# How ERM adds Value to the Organization



# How ERM adds Value to the Organization



- **Reduce Cost of Hazard Risk**
  - ✓ Risk management aims to reduce the long-term overall cost of risk for the organization
  - ✓ The reduction in the overall cost of risk can increase the organization's profits
  
- **Reduce Deterrence Effects of Hazard Risks**
  - ✓ The fear of possible future losses tends to make senior management reluctant to undertake activities they consider too risky
  - ✓ Risk management reduces the deterrence effects of uncertainty about potential future accidental losses by making these losses less frequent, less severe, or more foreseeable
  
- **Reduce & Manage Downside Risk**
  - ✓ Downside risks, including losses and failures, are an inevitable aspect of any type of business or speculative risk
  - ✓ Reducing downside risk provides similar organizational benefits as reducing the deterrence effects of hazard risks.

# How ERM adds Value to the Organization



- **Intelligent Risk Taking**
  - ✓ Providing the organization with a framework to analyze the risks associated with an opportunity and then to manage those risks
  - ✓ Decisions regarding new opportunities should be based on the organization's risk appetite
  
- **Maximize Profitability**
  - ✓ Risk management provides an organization information to evaluate the potential risk-adjusted return on its activities and to manage the risks associated with those activities
  - ✓ Risk managers can help the organization evaluate the risks and potential return of each option and their effects on the organization meeting its objectives

# How ERM adds Value to the Organization



## ➤ **Holistic Risk Management**

- ✓ Traditional risk management was conducted in silos within an organization, whereas ERM talks of managing Risks enterprise wise.
- ✓ An integrated, holistic approach that manages risk across all levels and function within an organization presents a more complete picture of an organization's risk portfolio and profile

## ➤ **Legal and Regulatory Requirements**

- ✓ Organizations with effective risk-management programs will be able to comply with the various Indian & Global regulatory requirements.

# How ERM adds Value to the Economy



**Reduced Waste of Resources**

**Improved Allocation of Productive Resources**

**Reduced Systemic Risk**



# How ERM adds Value to the Economy



- **Reduced Waste of Resources**
  - ✓ When a fire or an earthquake demolishes a factory or destroys a highway, that economy's overall productive resources are reduced. Risk management prevents or minimizes the waste of these productive resources.
  
- **Improved Allocation of Productive Resources**
  - ✓ Risk management also improves the allocation of productive resources because, when economic uncertainty is reduced for individual organizations, allocating productive resources is improved.
  - ✓ Risk management makes those who own or run an organization more willing to undertake formerly risky activities because they are better protected against the downside of risk.
  
- **Reduced Systemic Risk**
  - ✓ Systemic Risks are those risks who have the potential to do major disruption in the function of an entire market or financial system.
  - ✓ If organization does not have an effective risk-management program, that organization's risks can result in failure not only for the organization but also for the economy

# What is Risk Framework?



- ✓ Risk Management Framework prepares the organization to achieve long term goals, effective use of resources, dependable reporting and compliance with regulations/norms/guidelines.
- ✓ A good risk framework should have a strong governance structure so that the board and the management should know how risks are being managed.
- ✓ To ensure this, there are a few well-known frameworks available such as ISO 31000 : 2018 Risk Management Standard and the COSO ERM 2017

# COSO ERM 2017 Framework

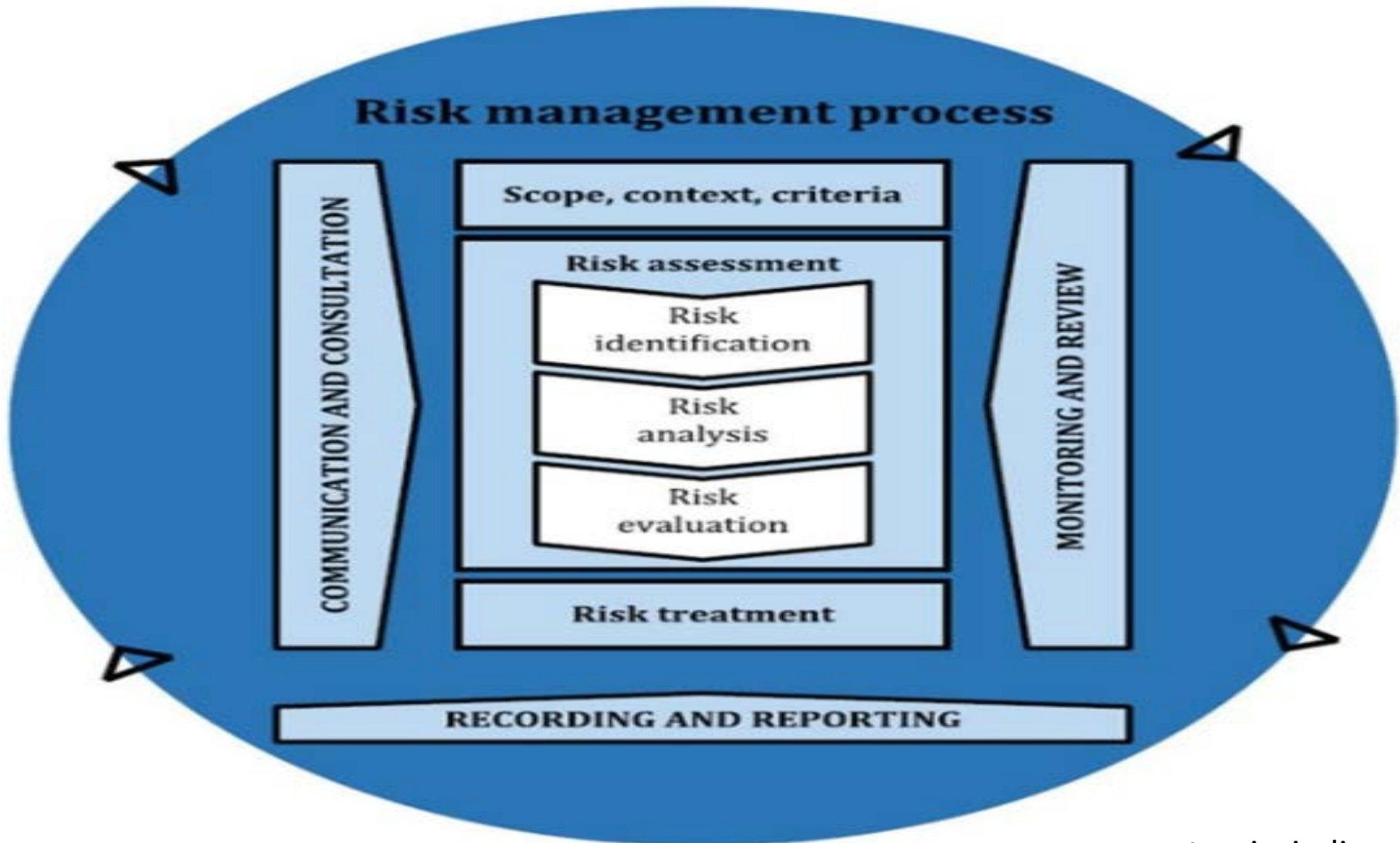


COSO ERM 2017—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions.

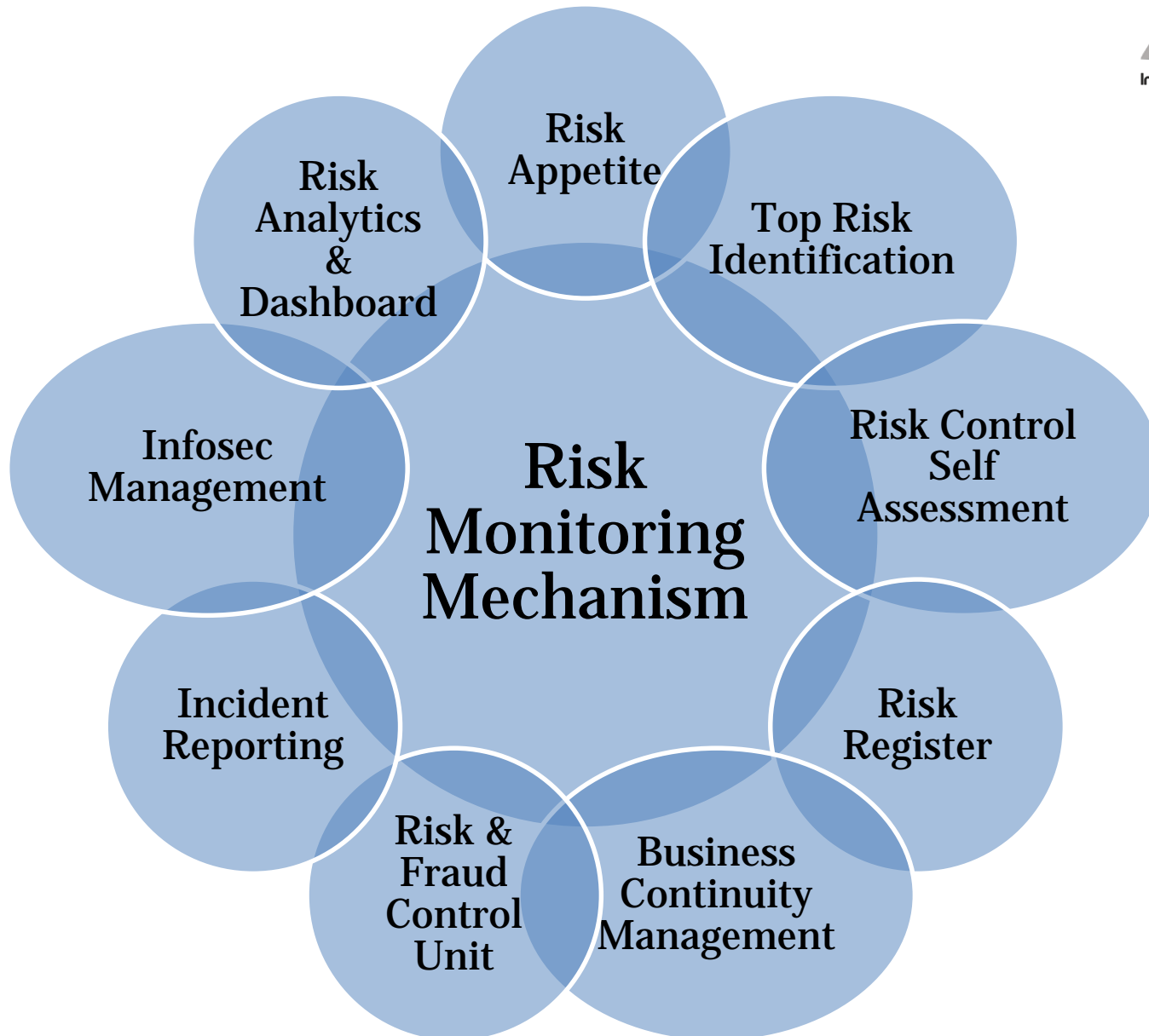


# ISO 31000:2018 Process

- ISO 31000 ERM- coordinated activities to direct and control an organization with regard to risk



# Risk Monitoring Mechanism

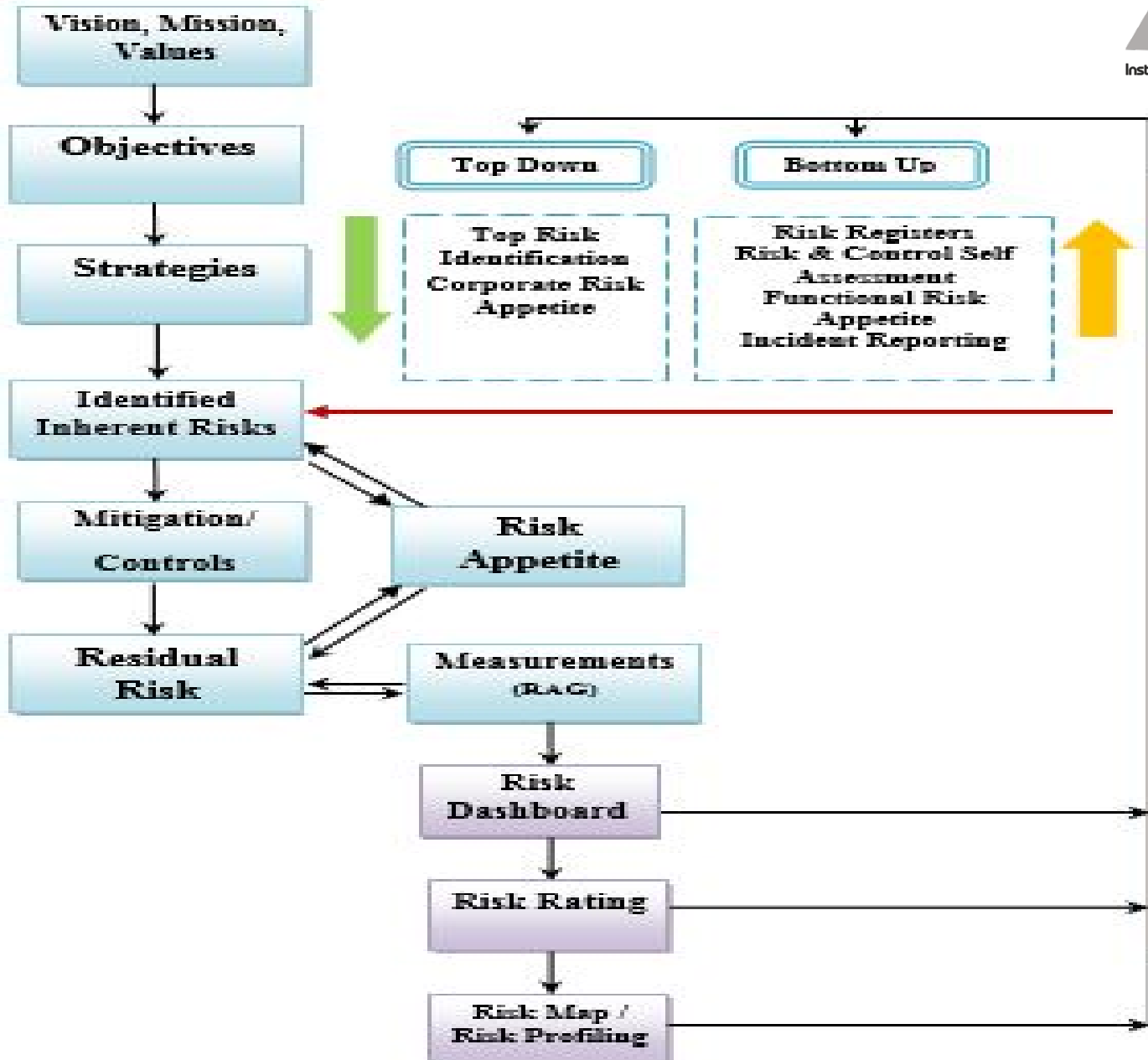


# ERM Workflow

Board/Senior Management

Risk Management/  
Risk Owner

Risk Management



Communication and Reporting

# Roles & Responsibilities of ERM

# Roles & Responsibilities of ERM



Tolerable Uncertainty

Legal and regulatory compliance

Survival

Business continuity

Earnings stability

Profitability and growth

Economy of risk management operations



# Roles & Responsibilities of ERM



- **Tolerable Uncertainty**
  - ✓ Aligning risks with the organization's risk appetite
  - ✓ Managers want to be assured that whatever might happen will be within the bounds of what was anticipated and will be effectively addressed by the risk management program.
  
- **Legal and Regulatory Compliance**
  - ✓ An important goal for risk management programs is to ensure that the organization's legal obligations are satisfied
  - ✓ A risk management professional has an essential role in helping the organization manage regulatory risk and the potential for liability
  
- **Survival**
  - ✓ Many risks can threaten the survival of an organization.
  - ✓ Survival of an organization depends on identifying as many risks as possible that could threaten the organization's ability to survive
  - ✓ It also depends on anticipating and recognizing emerging risks, such as those related to Bitcoins

# Roles & Responsibilities of ERM



## ➤ **Business Continuity**

- ✓ Survival requires that no risk occurrence (no matter how severe) permanently shut down an organization, the goal of continuity of operations is to become resilient.
- These are the steps an organization should take to provide business continuity and, therefore, resiliency:
  - ✓ Identify activities whose interruptions cannot be tolerated
  - ✓ Identify the types of accidents that could interrupt such activities
  - ✓ Determine the standby resources that must be immediately available to counter the effects of those accidents
  - ✓ Ensure the availability of the standby resources at even the most unlikely and difficult times

## ➤ **Earnings Stability**

- ✓ Rather than strive for the highest possible level of current profits in a given period, some organizations emphasize earnings stability over time.
- ✓ Striving for earnings stability requires precision in forecasting fluctuations in asset values; liability values; and risk management costs, such as costs for insurance.

# Roles & Responsibilities of ERM



- **Profitability and Growth**
  - ✓ An organization's senior management might have established a minimum amount of profit that no event should reduce.
  - ✓ To achieve that minimum amount, risk management professionals must identify the risks that could prevent this goal from being reached, as well as the risks that could help achieve this goal within the context of the organization's overall objectives.
  
- **Economy of Risk Management Operations**
  - ✓ Risk management should operate economically and efficiently; that is, an organization generally should not incur substantial costs for slight benefits gained.
  - ✓ Risk management programs should be operated economically and efficiently.
  
- **Trade offs among Goals**

# How 3 Lines of Defense interact with each other

# Three Lines of defence Model



## First Line

The first level of control environment is the business operations which perform day to day risk management activity.

## Second Line

**Oversight functions** in the Company such as Risk Management, Compliance, Legal & Finance set directions, define policy, and provide assurance.

## Third Line

Internal and external audit are the third line of defense, offering **independent** challenge to the levels of assurance provided by business operations & oversight functions.

# First Line of Defense & Second Line of Defense

1

**Business Units**

- Business Units are responsible for managing their own units.
- Responsible for identifying & controlling risks by using control frameworks, implement internal control processes and adequate controls.

2

**Risk Management**

- Responsible for ERM
- Independent reporting to the Management, Board, Audit Committees.
- Advisor consultant to 1<sup>st</sup> Line of Defense

# Second Line of Defense & Third Line of Defense

2

## Risk Management

- Design and implementation of the risk management plan, including the choice of appropriate tools and responses to risk, in accordance with board guidance.
- Defining Risk Appetite & Tolerance levels & establishing Internal Risk Management Controls
- Risk Assessment and monitoring the Risk levels

3

## Internal Audit

- Reviews and critiques the implementation of the Risk Management Plan
- Auditing the internal controls implemented by the risk management team.
- Evaluating the effectiveness of the controls to determine whether the intended RM goal is being Achieved
- Providing alternatives & recommending solutions

# Assurance to various Stakeholders



# Assurance to the Stakeholders



## What?

Risk assurance refers to the level of confidence in the effectiveness of the organization's risk management culture, practices, and procedures

## How?

Both within the organization and with outside stakeholders

## Why?

High levels of risk assurance result in lower costs to the organization, enhancing its long-term value.

# Assurance to the Stakeholders- High Level Assurance Characteristics

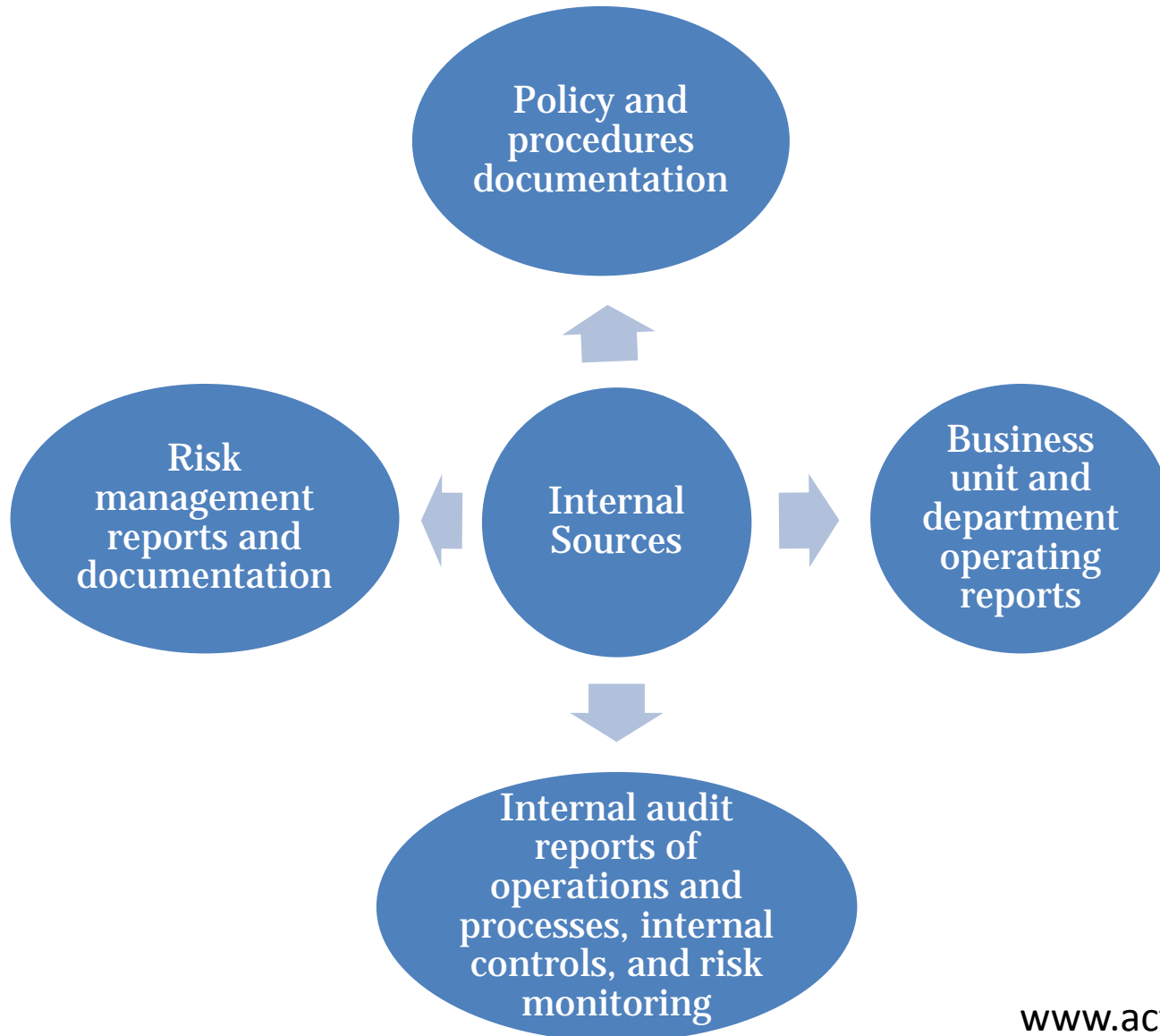


Risk reporting systems are providing information up the management chain to the board of directors, as well as down the management chain to the operating units.

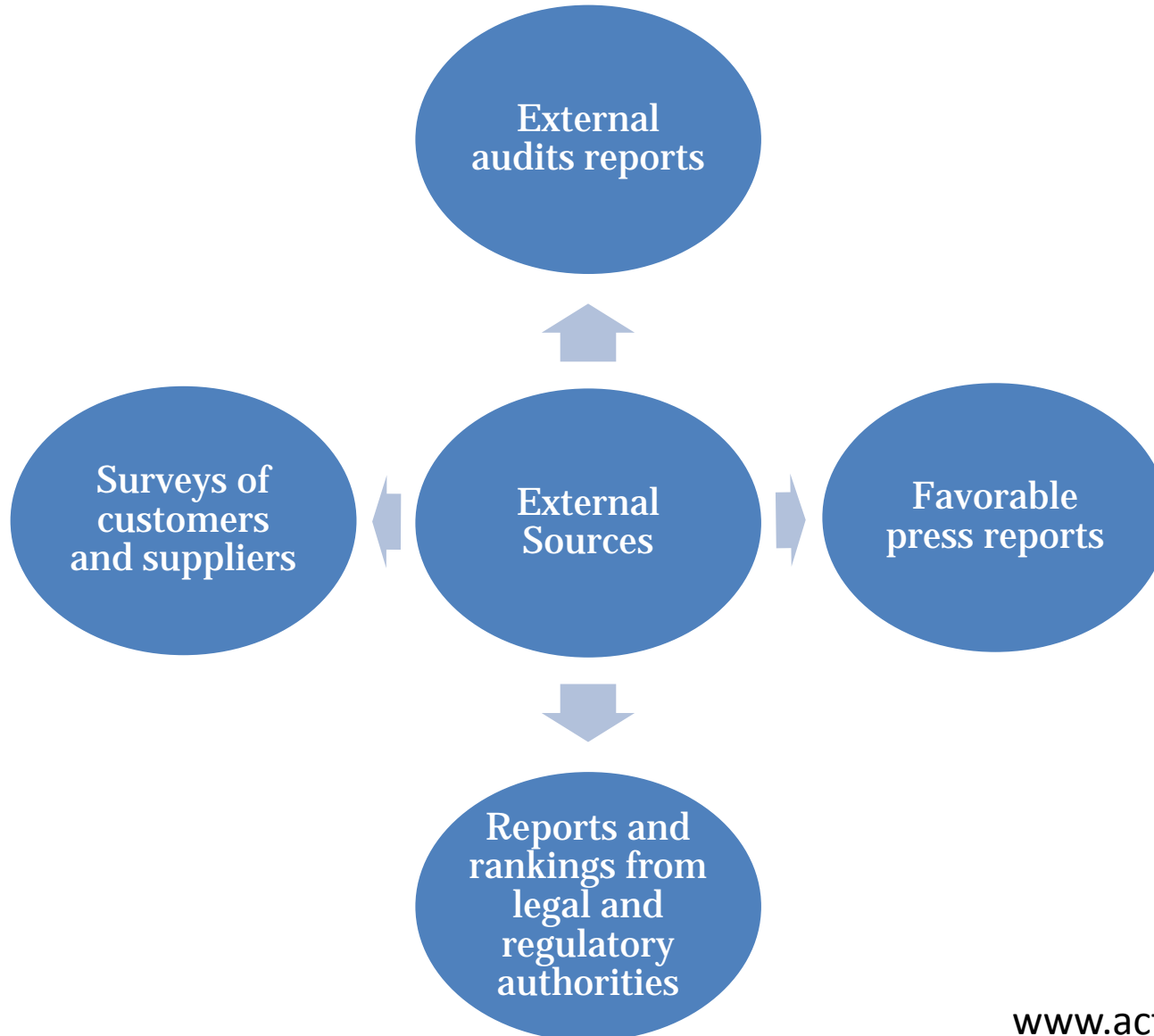
Risk Aware  
Culture

The board of directors is certain that key risks have been properly identified, quantified, prioritized, and managed in an effective and cost-efficient manner.

# Assurance to the Stakeholders- Risk Assurance Sources



# Assurance to the Stakeholders- Risk Assurance Sources



# Assurance to the Stakeholders- Benefits

## **Confidence**

The board of directors & Regulatory Authorities will have greater confidence in management effectiveness

## **Culture of Risk Management**

Employees have greater job security, which itself reinforces a culture of risk management

## **Customers and Suppliers**

Customers and suppliers are more confident in the financial health and well-being of the organization



Institute of Actuaries of India

THANK  
YOU