8th Annual Public Sector Accountants Conference

Risk Management Strategies & Guidelines for the Public Sector & Strengthening the Internal Control Framework within organizations in the Public Sector

CPA Erick Audi

Tuesday, 19th October 2021
Whitesands Hotel, Mombasa County

Uphold public interest

Credibility **Professionalism** **Accountability**

Profile

- CPA Erick Oluoch Audi
- Graduate of UON (Accounting)
- MBA-UON (Finance)
- CPA, CIA, CISA
- Certified ISO Lead Auditor; ISO 9001:2015
- Member of ICPAK, ISACA & IIA
- Over 16 Years working experience from Private Audit Firms, KRA, KeRRA, Ketraco & KenGen
- Passion for Governance, Risk Management & Control Advisory Services.
- Seasoned Facilitator/Trainer/Consultant on Internal Audit, Board & Audit Committee functions
- Married with Children

Presentation Agenda

- Introduction
- The IIA Three Line Model
- Legal Framework for Risk Management & Internal Controls
- Definitions of Risk & Risk Management
- Overview of Risk Management process
- Challenges and Critical Success Factors in Risk Management
- Internal Controls Definition
- Internal Control Components
- Conclusion

Polling Question

Does your organisation have a Risk Management Framework

A. Yes
B. No
C. Not aware

Does your organisation have an Internal Control Framework?

A. Yes
B. No
C. Not Aware

Introduction

- There is a very clear relationship between internal control and risk management.

- Basically, internal controls provide reasonable assurance that risks to the achievement of organizational objectives are at acceptable levels.

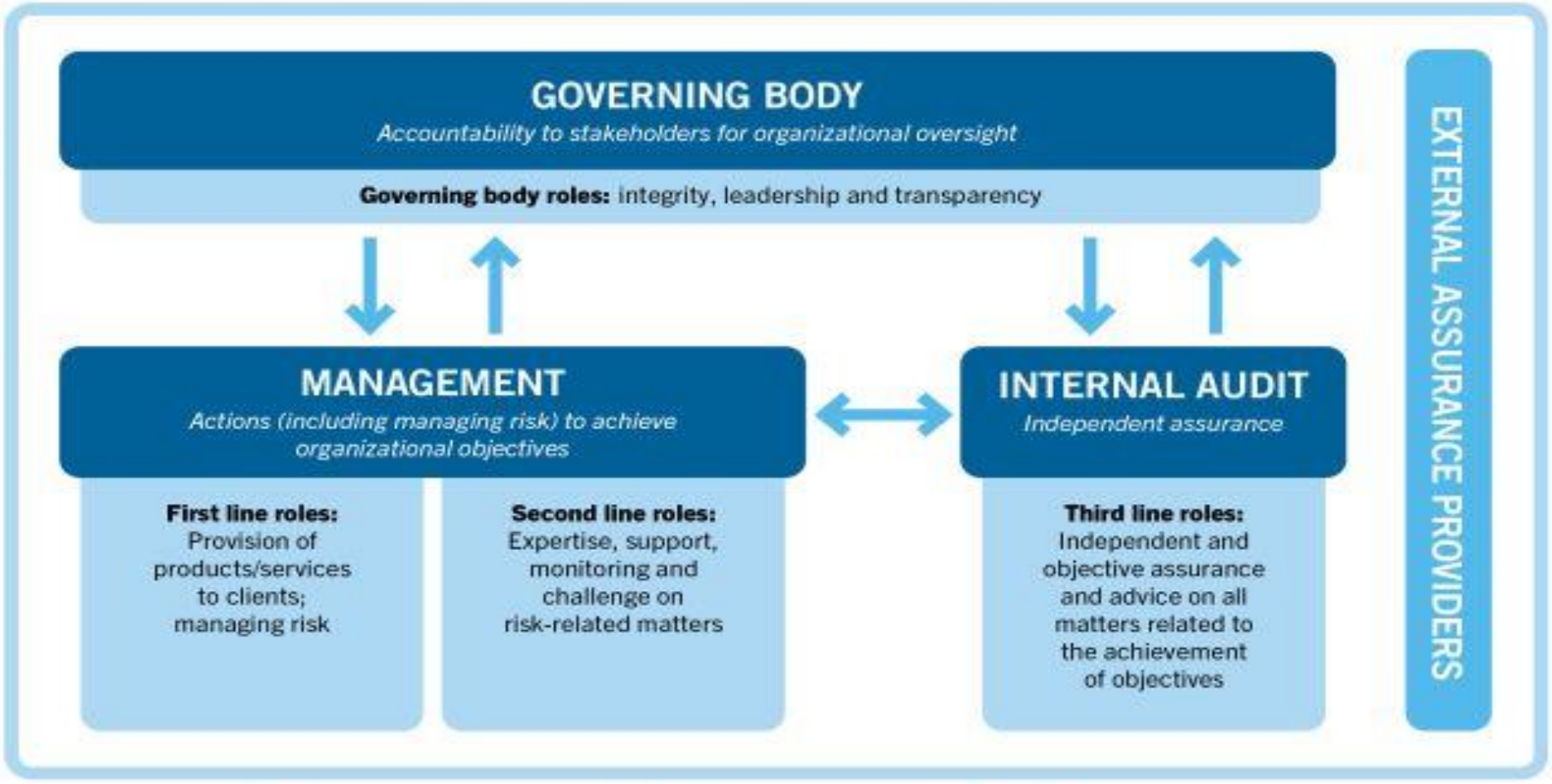
- Thus, we need risks to be identified, understood, and assessed (against levels defined as acceptable) before you know what controls are required.

- At the same time, we need controls to manage those risks and ensure they are at and remain at acceptable levels.

Roles of BOD, Management & Internal Audit Functions

Board of Directors	Management	Internal Audit Function
Oversee the development and implementation of an adequate internal control systems	**Establish and maintain** an adequate and effective system of internal controls	**Assist** management in the efficient and effective discharge of their responsibilities
Monitor the independent assurance function	**Develop** a system to monitor and control risks	**Advise** and **make recommendations** on internal control, risk management and corporate governance

The IIA's Three Lines Model (2020)



Legal Framework for Risk Management & IC

- ***Public Finance Management Act, 2012, sections*** 12(2)(i)), 50(1), 59(a)(iii), 62(3)(a), 63, 141, 73(3), and 155(3) and its attendant 2015 Regulations requires the Accounting Officer to ensure that entities *develop risk management strategies, which include fraud prevention mechanism; and develop a system of risk management and internal control that builds robust business operations.*
- ***The Company Act 2015, Revised 2017, and International Financial Reporting Standards & Mwongozo Code*** *require directors to disclose policy on risk management, a description of the key risks and uncertainties facing the company in the Annual Report and Notes to the Accounts.*
- ***Gazette Notice No 2691 of April 2016 on "Audit Committee Guidelines For National/County Governments"*** requires the **Audit Committee** to support the Executive Management, Accounting Officers, Boards, and Board Chairs *by monitoring and reviewing the risk, control and governance processes that have been established in the entity pursuant to the Board policies.*

Legal Framework for Risk Management….

- ***Treasury Circular 3/2009 dated 23rd February, 2009*** *introduced formal risk management* in Government Departments and Offices and to promote good governance.

- ***Mwongozo Code of Governance for State Corporations, 2015*** Chapter three requires Boards to *ensure their entities have adequate systems and processes of accountability, risk management and control.*
- ***CMA Code of Governance Gazette Notice No. 1420 issued in December 2015 Clause 6.2-*** The Board should have *an effective risk management framework for the company in place and* determine the *company's level of risk tolerance and actively identify, assess and monitor key business risks to safeguard shareholders' investments and the company's assets.*

Legal Framework for Risk Management….

- The ***Public Sector Accounting Standards Board (PSASB)*** have developed the ***Draft Public Sector Risk Management Guidelines (psasb.go.ke)*** awaiting Gazettement by CS, National Treasury.

- Although risk management is enacted in law, implementation has not been systematic and structured across entities and while some entities have more mature risk management systems, other entities having no formal processes in place.


REPUBLIC OF KENYA
OFFICE OF THE DEPUTY PRIME MINISTER &
MINISTRY OF FINANCE

THE TREASURY
P.O. Box 30007
NAIROBI

Date 23rd FEBRUARY, 2009

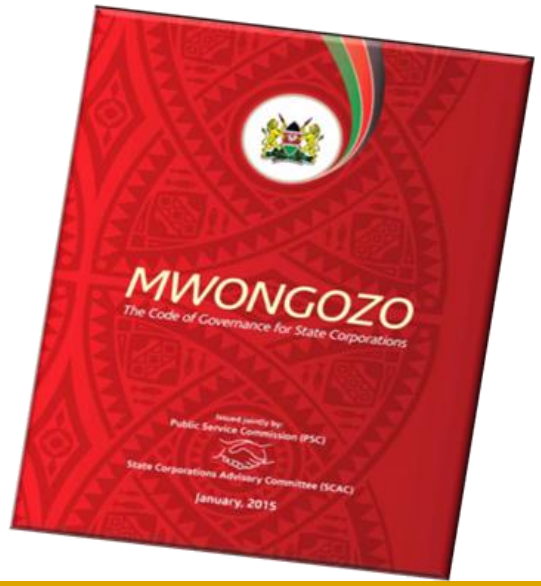
Telegraphic Address: 22921
FINANCE NAIROBI
Fax No. 318073
When replying please quote

Ref. No. MOF/ (AG/063/75)

TREASURY CIRCULAR NO 3/2009

TO: All Accounting Officers,
All Chief Executives of State Corporations,
All Clerks to Local Authorities.

RE: DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL RISK MANAGEMENT POLICY FRAMEWORK (RMFI) IN THE PUBLIC SECTOR



Audit Committee Role & Responsibilities- Internal controls and risk management systems

(Gazette Notice Number 2691 of April 2016)

- The AC should review the entity's *internal financial controls (that is, the systems established to identify, assess, manage and monitor financial risks).*
- The Entity's management is responsible for the *identification, assessment, and management and monitoring of risk, for developing, operating and monitoring the system of internal control* and for providing assurance to the board and executive management that it has done so. Except where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should *receive reports from management on the effectiveness of the systems they have established and the conclusions of any testing carried out by internal and external auditors.*
- Except to the extent that this is expressly dealt with by the board or risk committee, the audit committee should review and approve the *statements included in the annual report in relation to internal control and the management of risk.*

Mwongozo Code of Governance-Internal Controls

Internal Control Systems - The Board should:

- Maintain an effective & efficient system of internal controls.
- *Set out its responsibility for internal controls* in the Board Charter.
- Delegate to management the responsibility of designing, implementing and monitoring effectiveness of internal control systems.
- Receive from the internal audit function *a written assessment of the effectiveness of the system of internal controls on a quarterly basis.*
- Receive from the *external auditor an assessment of the effectiveness of the system of internal control after the audit process.*
- Ensure that the *internal audit function monitors for rectification, weaknesses noted by the external auditor.*

CMA Code of Corporate Governance-Internal Controls

6.3 Internal control systems

- The Board shall put in place an *effective system of internal control.*
- The Board shall establish and review on a regular basis the *adequacy and integrity of the company's internal control systems and the management of information systems, including compliance with applicable laws, regulations, rules and guidelines.*
- The Board shall set out its *responsibility for internal control in the Board Charter.*
- The Board shall *delegate to the management the responsibility of designing, implementing and monitoring effectiveness of internal control systems.*
- The Board shall review the *effectiveness of the company's risk management and internal control practices on an annual basis.*

Risk Management definitions

- ***ISO 31000: 2018, Risk Management Guidelines,***

Defines risk as ***"the effect of uncertainty on objectives".***

- ***COSO Enterprise Risk Management-Integrating with Strategy and Compliance, 2017, defines risk as;***

"the possibility that events will occur and affect the achievement of strategy and business objectives". Risk can have either ***positive, negative effects or both****, and create or result in opportunities and threats.*

Risk Management def….

- ***ISO 31000: 2018, Risk Management Guidelines***, defines ***Risk Management*** as;

  "the coordinated set of activities to direct and control an entity with regard to risk".

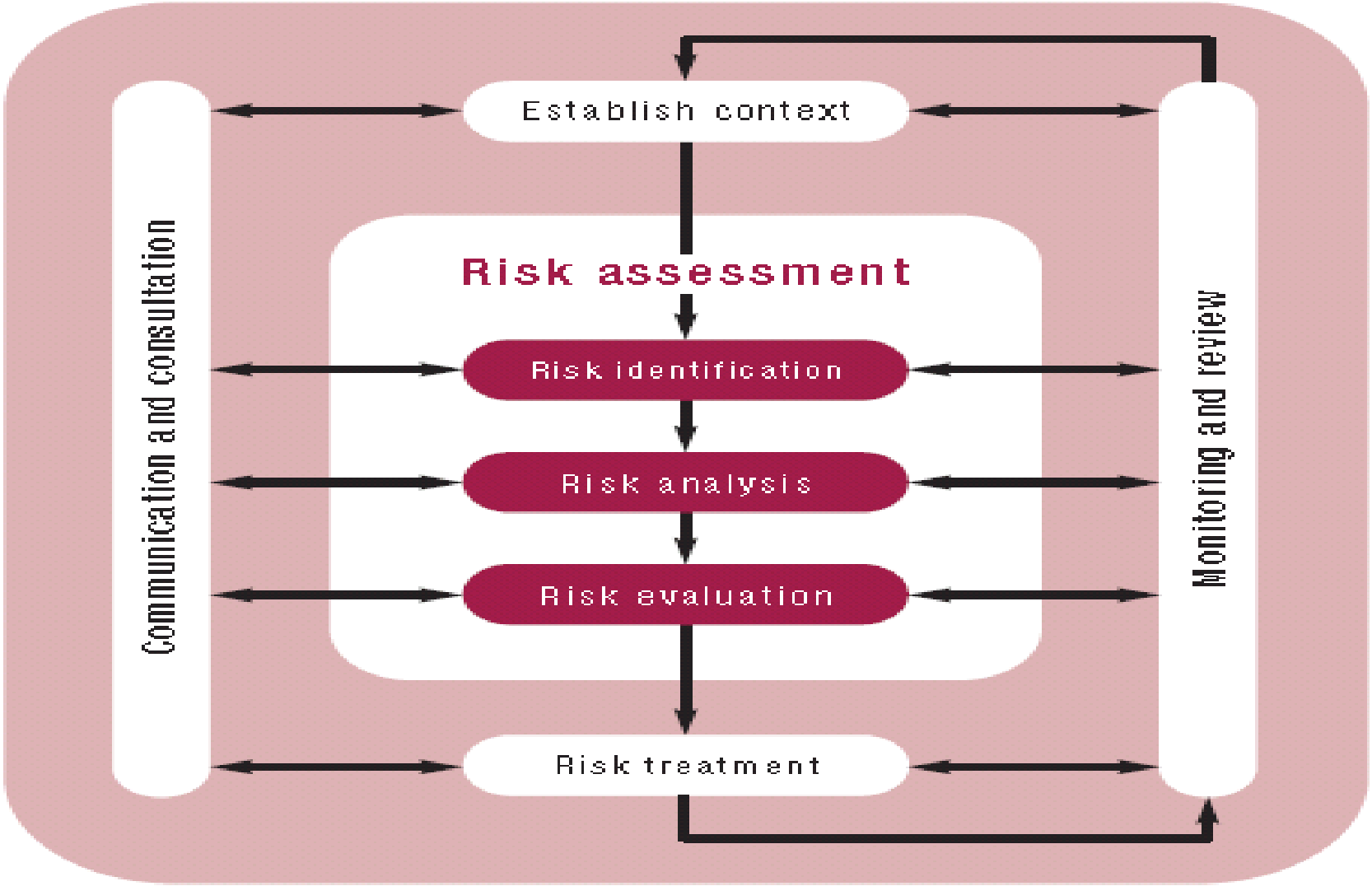
- ***COSO Enterprise Risk Management-Integrating with Strategy and Compliance, 2017,***

  Enterprise Risk Management *as "the culture, capabilities, and practices, integrated with strategy-setting and its performance that entities rely on to manage risk in creating, preserving, and realising value".*

Risk Terminologies….

- **Inherent Risk** - The level of risk associated with the entity as a whole, or the individual system being examined before considering the effectiveness of controls.
- **Risk Appetite** - Amount and type of risk an organization is willing to accept in pursuit of its business objectives/value.
- **Risk Capacity** - The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives.
- **Residual Risk -**The level of risk associated with the entity as a whole, or the individual system being examined after considering the effectiveness of controls.
- **Opportunity** - An action or potential action that creates or alters goals or approaches for creating, preserving, and realizing value.
- **Risk tolerance:** Means the boundaries of acceptable variation in performance related to objectives.

Risk Management Process



Source: ISO 31000:2018 Framework Overview

Benefits of Risk Management

- Improved accountability and better governance;
- Improved entity performance and resilience;
- Improved the ability to identify, evaluate, and manage major threats;
- Improved recognition and seize of opportunities;
- Enabling risk-based decision making and strategy-setting;
- Optimised resource allocation to match risk exposure;
- Decreased potential for unacceptable or undesired behaviours such as fraud and other unethical practices;
- Improved communication and consultation within the entity and parties sharing risks;
- Improved compliance with laws and regulations

Challenges in Implementing Risk Management

- Lack of sustained commitment from the Governing Body and top management in implementing risk management.
- Risk management not being aligned to strategic objectives
- Failure to embed risk management in governance and entity processes
- Risk management being treated as an extension of compliance or internal audit function resulting into lack of ownership by risk owners;
- Lack of a clear roadmap and plan for risk management implementation and improvement.

Challenges in Implementing Risk Management….

- Lack of integrated risk management framework resulting in silo approach to risk management;
- Limitations in the quality and reliability of information used;
- Past mistakes being overlooked and with no consideration to learn and improve controls;
- Focus on compliance limiting innovation and change management;
- Unsupportive risk behaviour and culture such as secrecy and fear of retribution;
- Entities not keeping abreast with changing business and regulatory environment;
- Inadequate risk capacity including skills, experience and resources, among others.

Risk Management Strategy- Definition

- A risk management strategy is a key part of the risk management lifecycle. After identifying risks and assessing the likelihood of risk events happening, as well as the impact they could have, you will need to decide how to treat them.

- The approach you decide to take is your risk management strategy. **This is also sometimes referred to as risk treatment.**

Risk management strategies, or risk treatment options

There are four main risk management strategies, or risk treatment options:

- ✓ **Risk acceptance**
- ✓ **Risk transference**
- ✓ **Risk avoidance**
- ✓ **Risk reduction**

- **Choosing the right one will mean the difference between managing each potential risk effectively or facing serious consequences that could damage our institutions**

Selecting a Risk Management Response….

- What the residual risk would be after responding to the risk, and whether this residual risk is acceptable.
- The cost-to-benefit ratio analysis
- Legal and/or regulatory requirements.
- Risk response that may not be economically viable, but still warranted (*e.g.: high-impact, small likelihood risks e.g. natural disasters pandemics*).
- Solitary response options or combinations of responses (e.g.: *a mixture of preventative and corrective measures; organisations generally benefit from using a combination and variety of risk response options*).
- Inter-dependencies – where risk response options can affect risk elsewhere in the organisation, in which case the stakeholders involved in those areas also need to be consulted.

Negative Risk Response Strategies

Avoid (Terminate/Eliminate)

- Avoidance eliminates the risk by removing the cause. It *may lead to not doing the activity or doing the activity in a different way.*

- Some risks can be avoided by an early collection of information, by improving communication between stakeholders or by use of expertise.

- Examples of options here is *ceasing a product line, declining to expand to a new geographical market, abandoning a project/programme, or selling a division.*
- *Recent example would be allowing employees to work from home to prevent covid-19 infections.*

Negative Risk Response Strategies….

Transfer (Sharing)

- In this approach, the risk is shifted to a third party. The third-party, like insurance company or vendor, is paid to accept or handle the risk on your behalf and hence the ownership, as well as impact of the risk, is borne by that third party.

- Risk transfer does not eliminate the risk, but ***it reduces the direct impact of the risk on the business.***
- Few transference tools are an insurance policy, performance bonds, warranties, guarantees, etc. Other examples include outsourcing to specialist service provider, purchasing insurance products and engaging in hedging transactions.

Negative Risk Response Strategies….

Mitigate (Reduce)

- Mitigation reduces the probability of occurrence of a risk or minimizes the impact of the risk within acceptable limits.
- This approach is based on the fundamental principle *that earlier the an action is taken to reduce the probability or impact of a risk is more effective than doing fixes to repair the damages after the risk occurs.*

- Example of mitigating a risk includes the *use of advanced technology or best practices to produce more defect-free products.*

Negative Risk Response Strategies….

Accept

- Acceptance means accepting the risk, especially *when no other suitable strategy is available to eliminate the risk*. ***Acceptance can be passive acceptance or active acceptance.***

- Passive acceptance requires no other action except to document the risk and leaving the team to deal with the risks as they occur.

- In an active acceptance approach, a contingency reserve is designed to recover the losses of time, money, or resources.

Negative Risk Response Strategies….

Contingent Risk Response Strategies

- These strategies are implied only when certain events occur. The execution of these strategies happens only under certain predefined conditions.
- The team waits for sufficient warning signals before implementing these strategies. These signals could be missing the milestones work items or deadlines etc.
- These strategies include using financial reserves, staffing re-allocations, and implementing workarounds to minimize the loss, repair the damage to the extent possible and prevent a recurrence.
- *The risk treatment plans should identify those responsible for action, time frames for implementation, budget requirements or resource implications, performance measures and review process where appropriate.*
- *Progress of treatments against critical implementation milestones should be monitored.*

Positive Risk (Opportunities) Management Strategies

Exploit

- Exploitation increases the chances of making a positive risk happen, leading to an opportunity.
- This approach reduces the uncertainty associated with a positive risk by ensuring that it happens.

Share

- When the business is not fully capable of taking advantage of the opportunity they might call in another company to partner with. The expertise of another company is to leverage to maximize the return out of the opportunity.
- Examples of sharing opportunity include forming risk-sharing partnerships, teams, special purpose companies, or joint ventures.
- In this, all parties gains as per their investment and action.

Positive Risk Management Strategies……

Enhance

- Enhancing involves increasing the probability of occurrence of the risk and expanding its impact. This is done by identifying and influencing the various risk triggers.
- An example of enhancing an opportunity includes *adding more resources to a project to finish it earlier.*

Accept

- This involves taking advantage of the positive risk as it happens but not actively pursuing it.
- It is just like an opportunity coming and being accepted without much pre-planning.

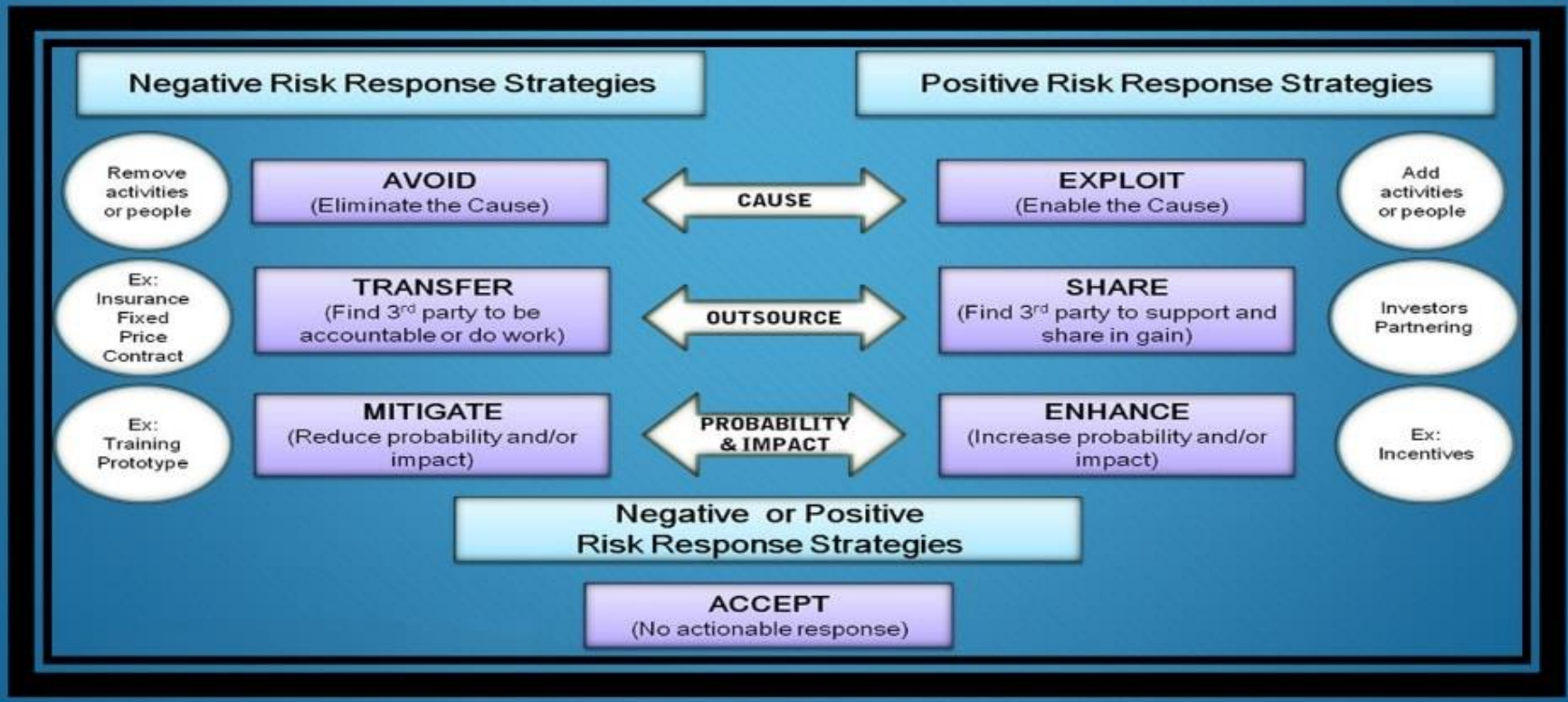
Risk Register……

A risk register should be developed for each process/area assessed and the following information included in the risk register as a minimum.

- Objective of the process
- The risk ref/category/description of the risk.
- The causes and consequence of the risk.
- The inherent risk rating determined from the assessment of the potential
- consequences and likelihood for the risk before controls.
- Details of the existing controls in place to manage the risk.
- The residual risk rating after consideration of the controls in place.
- Details of any proposed controls/improvement actions, including a due date for implementation, risk owner and any resources required.

- Management, staff and stakeholders (assisted by the risk champions) should immediately report emerging risks to the Risk Management Officer and supervisors immediately.

Summary of Positive and Negative Risk Response Strategies



Critical Success Factors for Risk Management

- Sound Objective Setting: Align risk to the strategic objectives.
- Commitment & Support of the Board and Senior Management
- ERM Ownership.
- Regular training & awareness programs to reduce misunderstanding and help staff clearly understand the ERM philosophy and policy.
- Formalized Key Risk Indicators (KRIs):
- Integration of ERM into business processes
- Monitoring, review & improvement of ERM framework
- Iterative & dynamic ERM steps
- Build a positive organization Risk culture and high ethical behaviour.

Critical Success Factors for Risk Management…….

- Report and record incidents and take remedial actions (lessons learnt)
- Involve stakeholders from the initial risk assessment
- Sufficient Resources: such as funds, qualified staff, time, knowledge and expertise
- Risk identification, Analysis and Response
- Leveraging risks as opportunities.
- Risk communication between the management staff and the risk management function
- A common risk language-codified in Risk Management policy and ERM Framework

Risk management Strategies….

- Strong budgetary and internal control systems
- Effective Internal audit functions that reports to the Audit Committee
- Social accountability strategies e.g., Complaint's handling
- Management oversight on the Risk Management Framework
- Effective & sound Procurement Policies and Processes that promote fairness, transparency and value for money.
- Sound Fraud and Corruption prevention mechanisms as part of broad strategy to manage Corporate risks


INTERNAL CONTROLS

Internal Control as defined by COSO Is … (Committee of Sponsoring Organizations)

"A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- ✓ *Effectiveness and efficiencies of operations*
- ✓ *Reliability of reporting*
- ✓ *Compliance with applicable laws and regulations*

Internal Controls defined….

- ✓ Internal Control **is a process**, It is a means to an end and not an end in itself……
- ✓ Internal controls is **effected by People** at every level of an organization. It is not merely policy manuals
- ✓ Effective internal control is **geared towards the achievement of operational, financial reporting, and compliance objectives**
- ✓ Internal control can **provide only reasonable assurance** - not absolute assurance - regarding the achievement of an organization's objectives

Internal Control- Primary Objectives

- **C**ompliance to laws and regulations
- **A**ccomplishment of Goals & Objectives
- **R**eliability & Integrity of Information
- **E**conomical & efficient use of resources
- **S**afeguarding of assets
- **I**nherent risks are properly managed

Who has Responsibility for Internal Control?

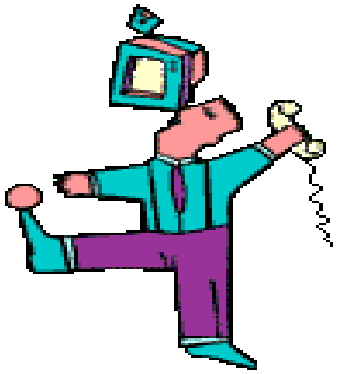
- Everyone in the organization has responsibility for ensuring the internal control system is effective by being cognizant of proper internal control procedures associated with their specific job responsibilities.
- Roles will vary depending on level of responsibility and the nature of involvement by the individual.
- The strength of the system depends upon employees' attitude toward internal control and their attention to it.
- **A weak link in the organizational structure can create a weakness in the Internal control system**

Who has Responsibility for Internal Control…….

- The Board is responsible for providing important oversight
- The MD/CEO is responsible for providing leadership and direction to Senior Management
- The Board of Directors, MD/CEO and senior managers, are responsible for establishing the presence of …
  - ✓ *Integrity*
  - ✓ *Ethics*
  - ✓ *Competence*
  - ✓ *Positive Control Environment*
- The MD/CEO and senior managers are responsible for establishing major operating policies that form the ***foundation of the internal control system***
- Department heads are responsible for executing those major Company-wide control policies and procedures.

Internal Control - Golden Rule

There is no greater waste than doing with great efficiency that which should not be done at all!



Limitations of Internal Control

- Misunderstanding of Instructions
- Mistakes of Judgment
- Personal Carelessness
- Distraction
- Fatigue
- Management Override
- Staff size Limitations
- Collusion among Individuals

Internal Control Failures Result From ……

- Lack of Integrity
- Weak Control Environment
- Inconsistent Objectives
- Poor Communication
- Inability to understand and react to changing conditions

The Five Components of Internal Controls

- ❑ Control **E**nvironment
- ❑ **R**isk Assessment
- ❑ **C**ontrol Activities
- ❑ **I**nformation & Communication
- ❑ **M**onitoring

Remember these with acronym "CRIME

All five (5) internal control components must be present to conclude that internal control is effective.

Components & Principles of Internal Controls….

Component	Summarised Principles
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies relevant objectives 7. Identifies and analyze risk 8. Assesses fraud risk 9. Identifies and analyzes significant changes
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations of monitoring activities 17. Evaluates and communicates deficiencies

1.0 Control Environment includes….

The control environment sets the tone of an organization influencing the control consciousness of its people. **It is the foundation for all other components of internal control, providing discipline and structure.**

An Effective control environment includes….

- ✓ Board Oversight
- ✓ Integrity and Ethical Values
- ✓ Management's Philosophy & Operating Style-morale & supportive attitude
- ✓ Sound Organizational Structure
- ✓ Assignment of Authority & Responsibility
- ✓ Human Resource Policies & Practices-Performance evaluation & reward systems
- ✓ Competence of Personnel-Trainings

What is your role in the control environment?

- ✓ Actions speak louder than words
- ✓ Communicate written policies and procedures, a code of ethics, and standards of conduct
- ✓ Do not entice employees to breach their ethics
- ✓ Demonstrate how important internal controls are to you and organization
- ✓ Set clearly defined consequences while reinforce positive behaviour
- ✓ Managers must support adherence to policies and procedures … if they expect employees to have that attitude
- ✓ Disciplinary action should be consistently applied to all employees.

2.0 Risk Assessment

- Is the identification and analysis of relevant risks associated with the achievement of objectives.
- Risk is the uncertainty of an event occurring that could have an impact on the achievement of objectives.
- Risk is measured in terms of consequences and likelihood.
- Risk can pertain to external & internal factors
- External risk factors are outside of the Company, usually beyond management's span of control while Internal risk factors are within the Company, usually within management's control.

Managers must determine …

✓ What can go wrong
✓ What areas have the most risk
✓ What assets are at risk
✓ Who is in a position of risk

3.0 Control Activities……..

Control activities are the policies & procedures that help ensure that management directives are carried out.

Principles of effective control activities

- Implement control activities designed to reduce risk based on what the organization *has defined to be acceptable risk levels*. Develop these control activities to ensure you're on track to achieve organizational goals and objectives.
- Select and develop control activities specific to information systems, especially in the area of IT.
- Develop clearly stated documentation in the form of a manual or employee handbook), outlining the policies and procedures required to implement and put control activities into action.

Types of control Activities….

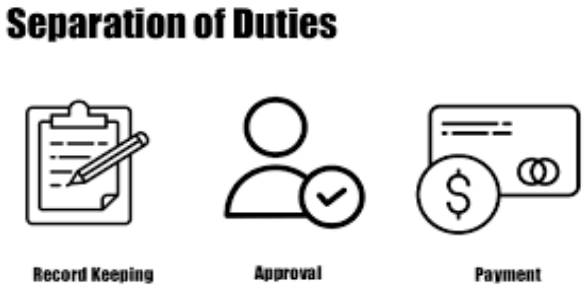
Types of Controls	What It Does	Examples
Preventative	Prevents errors or irregularities from occurring.	Segregation of duties, Approvals, authorizations and verifications, Physical control over assets, Maintaining and regularly reviewing inventories and records, Updated anti-virus software documentation, regular staff training & Password protection for all financial information & On-going risk management activities
Detective	Identifies errors or irregularities after they have occurred.	Exception reports, Reviewing performance objectives, forecasts, Reconciliations, physical inventory counts of assets, internal audits, Employee performance reviews, variance analyses.
Corrective	Identifies ways to react to the risk after the error has occurred.	Monitoring programs to identify non-compliance or weakness in controls, Using automated systems with built-in checks that reject non-conforming or unallowable processes. Enforcing employee discipline policies, Realigning separation of duties, Retraining staff on policies and procedures, Performing additional risk assessment and introducing revised or new internal controls.

Types of control Activities

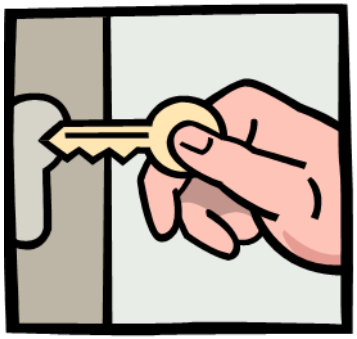
Types of Controls	What It Does	Examples
Directive	To ensure that a particular outcome is achieved or an undesirable event is avoided.	Wearing of Protective clothing Staff be trained with required skills before working unsupervised. Written, distributed policy and procedures, Well defined job descriptions
Performance	To orientate and motivate the organization's people to focus on the achievement of targets that are appropriate for the achievement of objectives	Despatching all orders on day of receipt of order, or allowing that less than 2% of production should fail quality control checks.

Common Control Activities

Generally, control activities (procedures) fall within **five broad categories;**



- ✓ Authorizations
- ✓ Segregation of Duties (A, R & C)
- ✓ Recording
- ✓ Safeguarding
- ✓ Reconciliations



Controls over Information Systems

Grouped into two categories;

1. Generals Controls;

Includes controls over controls over software acquisition and maintenance, access security and application system development and maintenance.

2. Application Controls;

- ✓ Computer matching and edit checks
- ✓ Completeness & Accuracy of Input
- ✓ Completeness & Accuracy of updates
- ✓ Authorization
- ✓ Maintenance
- ✓ Security

4.0 Information & Communication

The purpose of the information and communication system is to help ensure that employees are aware of …

- ✓ *The company's goals and objectives.*
- ✓ *How the company's goals and objectives are to be accomplished.*
- ✓ *Who is responsible for the specific tasks to accomplish them.*

Information and Communication System includes…….

- ✓ *Company's written/documented policies and procedures*
- ✓ *Company's Goals and Objectives*
- ✓ *Organizational Charts*
- ✓ *Position/job descriptions*
- ✓ *Performance evaluations*
- ✓ *Training Programs*
- ✓ *Periodic Progress Reports (Goals & Objectives Accomplishment)*

5.0 Monitoring

- Is a process that assesses the quality of the system's performance over time to ensure that the internal control system is operating as expected and that the organization's goals and objectives are achieved.
- Monitoring includes the *supervising, observing, testing & reporting to responsible Individuals*
- *Monitoring should focus on the following major areas: Control Activities, Mission, & Control Environment, Risks and Opportunities & Communication*

- **Managers should:**

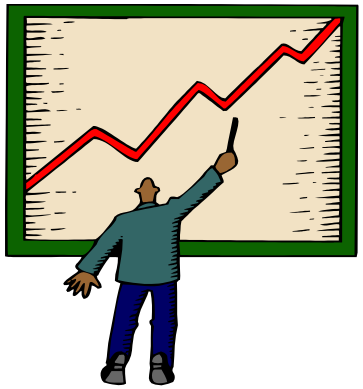
✓ *Promptly evaluate findings from audits and other reviews*

✓ *Determine proper actions in response to findings and recommendations from audits and reviews;*

✓ *Complete within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.*

Monitoring activities includes…….

- Reviews of financial reports (variance analysis) such as comparisons of budgeted to actual revenues and/or expenditures & comparisons of current to prior months and/or years activities
- Spot checks of transactions to ensure compliance with policies and Procedures
- Evaluation of trends
- Review of supporting documentation
- Review of software licenses
- Surprise cash & other asset counts
- Follow-up on complaints-reporting channels established



Role of Internal Auditors as monitoring agent

- Internal auditors are responsible for examining the adequacy and effectiveness of the Company's internal controls, and making recommendations where control improvements are needed.
- Internal auditors contribute to the effectiveness of the controls, but they are not responsible for establishing or maintaining them.
- Internal auditors are a part of the internal control system & they;

  ✓ *Appraise the adequacy of the Internal Control System.*

  ✓ *Act as an in-house consultant on Internal Control Matters*

The only alternative to risk management is crisis management --- and crisis management is much more expensive, time consuming and embarrassing.

JAMES LAM, Enterprise Risk Management, Wiley Finance © 2003

Without good risk management practices, government cannot manage its resources effectively. Risk management means more than preparing for the worst; it also means taking advantage of opportunities to improve services or lower costs.

Sheila Fraser, Auditor General of Canada

ERM Is a Journey…It Is Not a Destination!

Thank You!!!