ICPAK

Uphold Public Interest

Risk Based Auditing Workshop

Theme: Ensuring objectivity and completeness of Internal Audit Planning

Overview of the COSO ERM and ISO 31000:2018

by:

CPA Erick Audi

Wednesday, 25th August 2021

Facilitator

- CPA, CIA Erick Audi
- MBA-UON (Finance),
- B.Comm. –(UON), Accounting Option
- CPA, CIA), CISA Certifications
- Certified ISO Lead Auditor; ISO 9001:2015
- Member of ICPAK, ISACA & IIA
- Over 16 years working experience from private & public sector institutions.
- Passion for Governance, Risk Management & Control Advisory Services.
- Seasoned Facilitator/Trainer on Internal Audit, Controls, Risk Management and Governance processes for both Audit Committee & Boards.
- Currently, works at **KenGen** as the **Internal Audit & Risk Manager**
- Married with Children and loves watching football and reading.

Presentation Agenda

❑ Definitions

❑ Relevant IIA Standards on Risk Management

❑ Overview of COSO ERM & ISO 31000: 2018 Frameworks

❑ Comparing COSO ERM & ISO 31000:2018

❑ Establishing an ERM Framework

❑ Pre-requisites for effective ERM Implementation

❑ Dos and Don’ts when Implementing ERM

❑ Conclusion

Definitions

- ❑ **Risk is defined by ISO 31000 as**: *"the effect of uncertainty on objectives"*
- ❑ **The IIA's (Institute of Internal Auditors) International Standards define a risk** as *"the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood".*
- ❑ ***Opportunity*** *is the possibility that an event will occur and* *<u>positively affect</u>* *the achievement of objectives.*
- ❑ **Risk Management:**

A process to identify, assess, manage and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

- ❑ **Enterprise Risk Management (ERM):** ***I****s a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives (IIA-Global).*

Definitions

- ❑ **Risk Management Framework:** *The totality of the structures, methodology, procedures and definitions that an organization has chosen to use to implement its risk management processes.*
- ❑ **Risk Management Processes:** *Processes to identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.*
- ❑ **Risk Appetite** ; *The amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives. I**t is the Board's responsibility to define the risk appetite.***

Definitions

- **Risk Appetite Statements** *are used to articulate what risks the organization will take in pursuit of its objectives; the extent to which such risks will be retained; and the risks that will be avoided.*
- It is clearly one of the pre-requisite if the organization is to effectively identify and manage risks within an acceptance level.
- **Risk Tolerance (Definition):**
- *The boundaries of risk taking outside of which the organization is not prepared to venture in the pursuit of its long-term objectives. Risk tolerance can be expressed in terms of absolutes, e.g., "we cannot expose more than x % of our capital to losses in a certain line of business" or "we will not deal with certain types of customers"*

IIA Standard 2120 – Risk Management

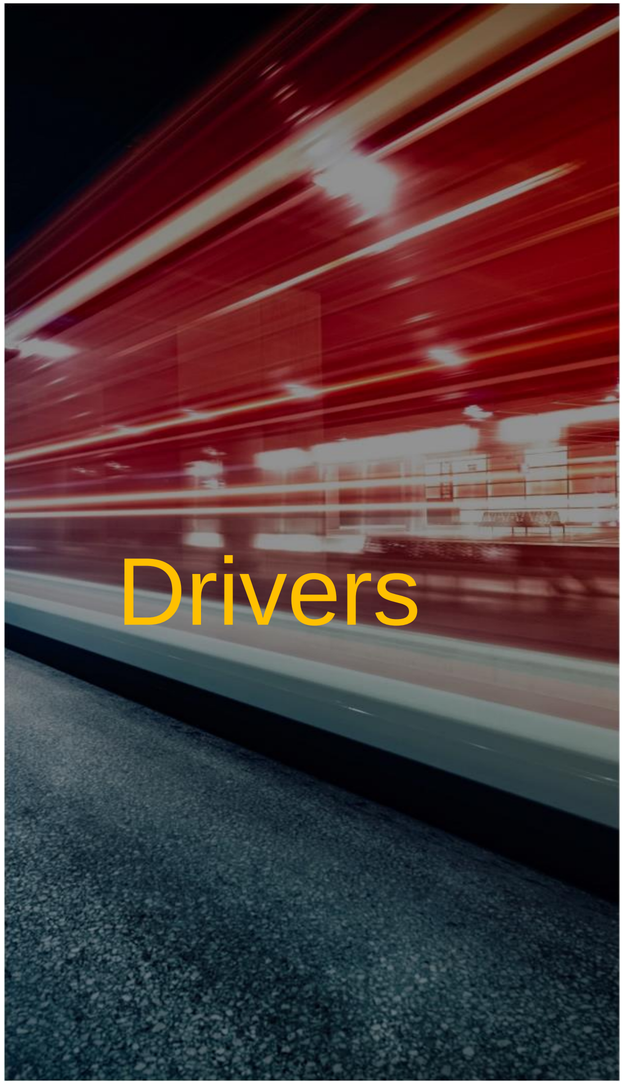
- ❑ ***The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes*. *Specifically, the Standard requires the internal audit activity to assess whether:***
- ❑ *The organization's objectives align with its mission.*
- ❑ *Management assesses significant risks.*
- ❑ *Management's risk responses align risks with the organization's risk appetite.*
- ❑ *Relevant risk information is captured and communicated timely throughout the organization, including to the Board.*

IIA Standard-2010 & 2020

- IIA Standard 2010 which requires ***"The chief audit executive must establish risk-based plans to determine the priorities of the internal audit."***
- IIA Standard 2010.A1 which requires that ***"The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process".***
- IIA Standard 2010.A2 "***The CAE must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions."***
- IIA Standard 2020, ***"The CAE must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The CAE must also communicate the impact of resource limitations."***
- The CAE should take into account the ***organization's risk management framework***, including ***risk appetite levels set by management for the different activities or parts of the organization.***
- If a risk management framework does not exist, the CAE ***uses his/her own judgment of risks after consideration of input from senior management and the board***.
- The CAE must **review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programs, systems, and controls.**

Why ERM?

- ❑ Response to an onset of a risk
- ❑ Operational surprises or losses
- ❑ Fiduciary responsibility of the Board
- ❑ Increased sources and types of business risk
- ❑ Complex systems and business environment
- ❑ Need for increased transparency in the understanding, managing and reporting of important risks to key stakeholders
- ❑ Anticipating and managing new and emerging risks in uncertain times
- ❑ Increase performance predictability through risk management



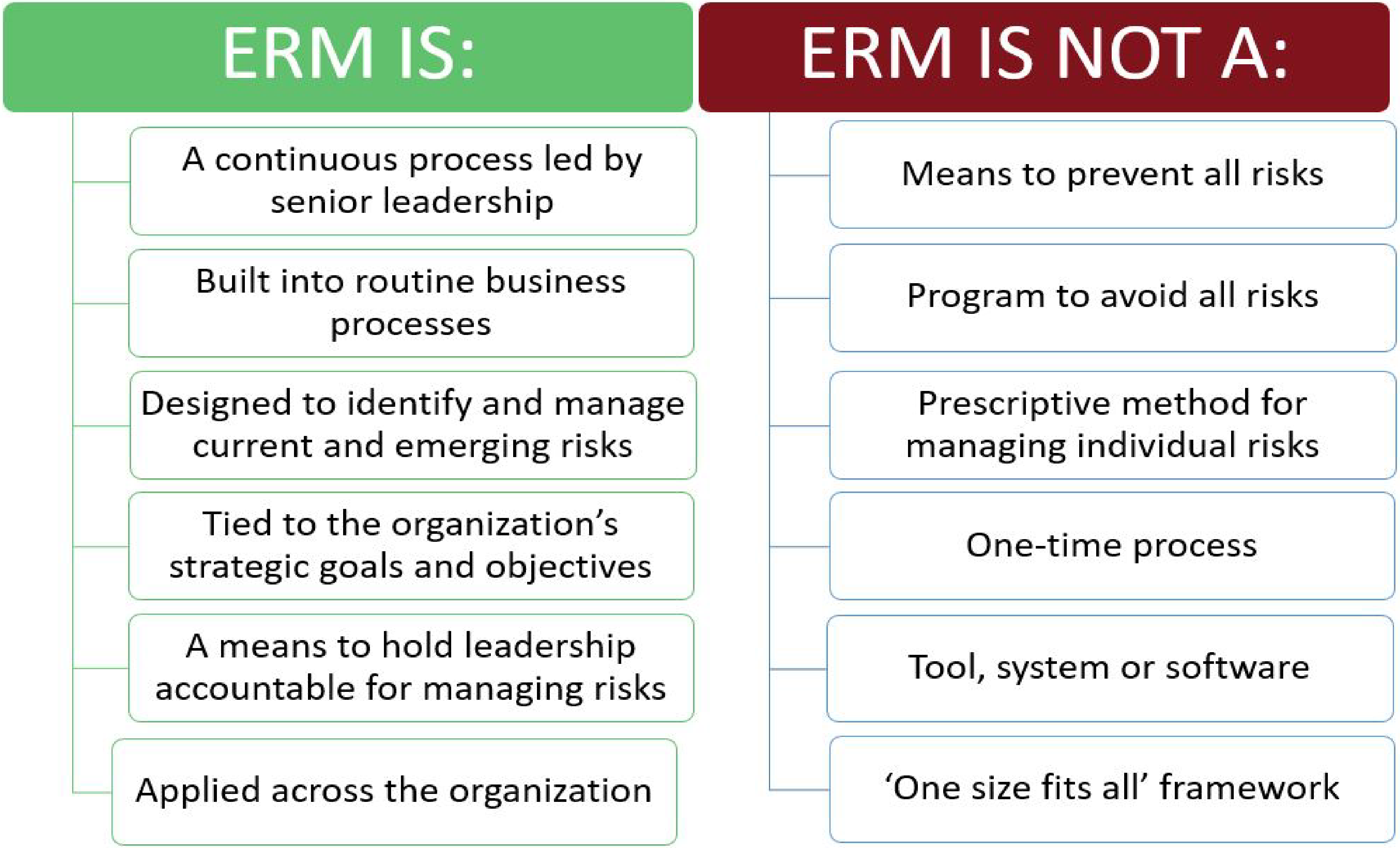
Why ERM?

- Provides a common language for risk management
- Provides an inventory of important risks and opportunities that could inhibit or enable the enterprise in achieving its strategic and related business objectives
- Assesses and prioritizes important risk and opportunities while identifying residual risks that may require further mitigation Aligns management in efforts to efficiently allocate resources
- Establishes a formal framework to gather, assess, manage and report the most risks forming the basis for ongoing risk management program.

The activities included in ERM

- Articulating and communicating the objectives of the organization;
- Determining the risk appetite of the organization;
- Establishing an appropriate internal environment, including a risk management framework;
- Identifying potential threats to the achievement of the objectives;
- Assessing the risk (i.e., the impact and likelihood of the threat occurring);
- Selecting and implementing responses to the risks;
- Undertaking control and other response activities;
- Communicating information on risks in a consistent manner at all levels in the organization;
- Centrally monitoring and coordinating the risk mgt processes and the outcomes
- Providing assurance on the effectiveness with which risks are managed

ERM is not…



ERM IS:

- A continuous process led by senior leadership
- Built into routine business processes
- Designed to identify and manage current and emerging risks
- Tied to the organization’s strategic goals and objectives
- A means to hold leadership accountable for managing risks
- Applied across the organization

ERM IS NOT A:

- Means to prevent all risks
- Program to avoid all risks
- Prescriptive method for managing individual risks
- One-time process
- Tool, system or software
- ‘One size fits all’ framework

Benefits of Enterprise Risk Management

- Greater likelihood of achieving objectives
- Improved understanding of the key risks and their wider implications
- Serves as an early warning system for potential problems-Fewer surprises or crises;
- Leads to more efficient resource allocation (e.g., capital and cash)
- Provides better information on potential consequences, both positive and negative.
- Hence helps identify positive opportunities and avoid threats
- Reduces the risk of loss, builds credibility and creates new opportunities for growth
- Allow management to make/evaluate decisions on a well informed, risk adjusted basis
- Removes silos in risk management
- Consolidated reporting of disparate risks at board level

ERM frameworks

- **Enterprise Risk Management—Integrated Framework,** issued in September 2004 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- **ISO 31000 - Risk management—Principles and guidelines**, issued in 2009 by the International Organization for Standardization (ISO).
- Both frameworks were developed by internationally recognized thought leadership (COSO) and standards-setting (ISO) bodies, and, during development, ***each received significant input and vetting from a wide range of risk management experts and professionals.*** As such, both frameworks have received much recognition and are used in practice.

Related standards

- The International Organization for Standardization (iso) is an international, membership-based NGO based in Geneva, represented in 165 member countries has published over 19 000 international standards.
- The International Organization for Standardization (ISO) was established in 1946. It came about when delegates from 25 countries who met at the Institute of Civil Engineers in London agreed to institute a new organization that would form and unify industrial standards.

The ISO 31000:2018 Standard

- An International standard that provides **principles** and **guidelines** for **effective risk management** published in 2009, revised in 2018.
- **Generic approach:**
- ➢ not specific to any industry or sector
- ➢ can be applied to any type of risk (financial, technological, natural, project)
- ➢ can be applied to any type of organization
- ➢ **A brief standard (24 pages)**
- ➢ Provides foundations for discussing risk management and undertaking a critical review of an organization's risk management process
- ➢ It can be applied throughout the life of an organization and to a wide range of activities.

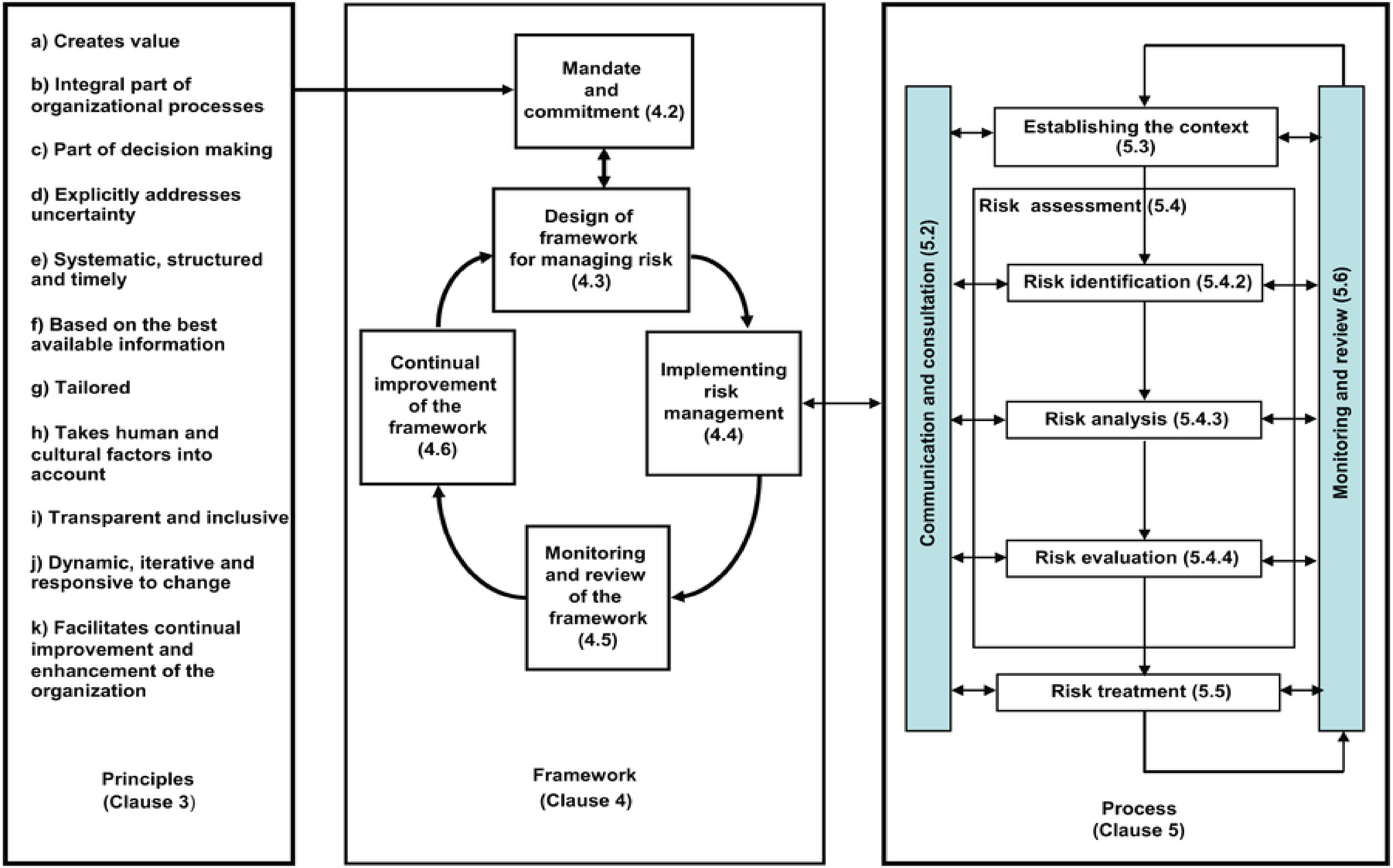
ISO 31000:2018

- Streamlined and easy to understand
- Proactive approach, rather than a compliance approach
- Emphasizes top-down implementation
- Links risks to strategy and the achievement of objectives
- Addresses both the upside and downside of risk
- Provides a consistent approach that can be tailored to any type of operation in any location and integrated with other standards and guidelines

The advantages of ISO 31000 over all the other systems

- ❑ ISO 31000 is a systematic and logical process for managing risk
- ❑ It's a simple blueprint for implementing in your organization
- ❑ A methodology that focuses on the company vision, mission, and objectives
- ❑ It is an all-inclusive framework; any organization can implement the principles, regardless of the organization's size or sector
- ❑ High-quality standards; ISO is internationally recognized for codifying exceptional standards
- ❑ Continuous improvement; ISO 31000 can be used throughout the life of an organization because of its cyclical nature and focus on long-term success
- ❑ Easily applicable; they guidelines can be applied to all aspects of an organization, and it uses simple terminology
- ❑ Tailored information; ISO 31000 considers human and cultural factors to make the principles fit into organizations globally

The ISO 31000:2018 Standard



a) Creates value

b) Integral part of organizational processes

c) Part of decision making

d) Explicitly addresses uncertainty

e) Systematic, structured and timely

f) Based on the best available information

g) Tailored

h) Takes human and cultural factors into account

i) Transparent and inclusive

j) Dynamic, iterative and responsive to change

k) Facilitates continual improvement and enhancement of the organization

Principles (Clause 3)

Mandate and commitment (4.2)

Design of framework for managing risk (4.3)

Implementing risk management (4.4)

Monitoring and review of the framework (4.5)

Continual improvement of the framework (4.6)

Framework (Clause 4)

Communication and consultation (5.2)

Establishing the context (5.3)

Risk assessment (5.4)

Risk identification (5.4.2)

Risk analysis (5.4.3)

Risk evaluation (5.4.4)

Risk treatment (5.5)

Monitoring and review (5.6)

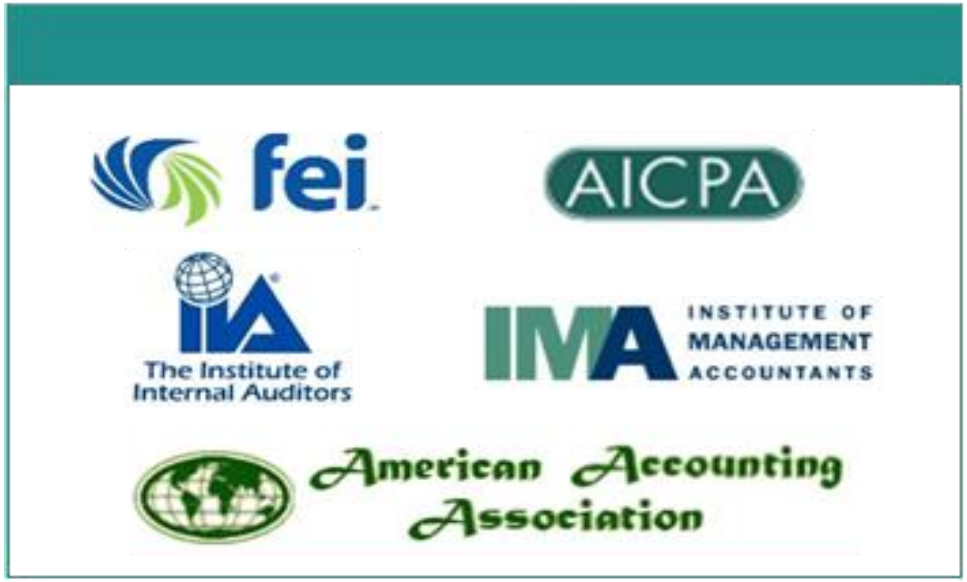
Process (Clause 5)

ISO 31000:2018 risk management processes:

- **Communication and Consultation:** Emphasizes the importance of promoting awareness and understanding of risk across key stakeholders.
- **Scope, Context, and Criteria:** Highlights the importance of customizing the risk management process to the organization.
- **Risk Assessment:** Describes that the risk assessment consists of risk identification, risk analysis, and risk evaluation.
- **Risk Treatment:** Reminds business leaders of the importance of selecting and implementing responses to manage risks.
- **Monitoring and Review**: Emphasizes the importance of improving the effectiveness of the risk management process.
- **Recording and Reporting:** Highlights the importance of effective communication of risk information for decision-making.

COSO ERM Framework

- **Private sector initiative** sponsored by 5 organizations
- **Provides thought leadership** through frameworks and guidance on;
- **Enterprise risk management (ERM)**
- **Internal control**
- **Fraud detection**


fei
AICPA
IIA
The Institute of Internal Auditors
IMA
INSTITUTE OF MANAGEMENT ACCOUNTANTS
American Accounting Association

ERM Framework (issued in 2004 and updated in 2017)

Establishes a standard with a common risk definition and framework that is readily usable by management in evaluating and improving their organization's enterprise risk management processes

COSO ERM Framework

- COSO is a joint initiative of five (5)sponsoring organizations;

✓ *American Accounting Association (AAA)*

✓ *American Institute of Certified Public Accountants (AICPA)*

✓ *Financial Executives International (FEI)*

✓ *Institute of Management Accountants (IMA)*

✓ *Institute of Internal Auditors (IIA)*

- Gained wide acceptance following financial control failures of early 2000's
- Most widely used framework in the US & also widely used around the world

COSO ERM FRAMEWORK

What is it?

ERM framework starts by defining enterprise risk management as follows:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Key COSO ERM Points:

- ❑ ERM is a Process
- ❑ ERM Processes are Implemented by People in the Enterprise.
- ❑ ERM Is Applied by Setting Strategies Across the Overall Enterprise.
- ❑ Concepts of Risk Appetite must be considered.
- ❑ ERM Provides Only Reasonable, Not Positive Assurance on Objective Achievements

COSO ERM Framework

COSO 2004 ERM Framework

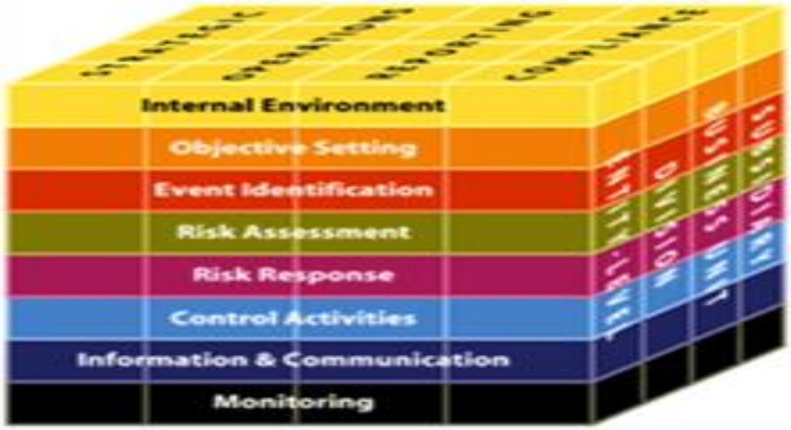
(Updated by 2017 Framework)

Enterprise Risk Management – Integrated Framework

COSO 2017 ERM Framework

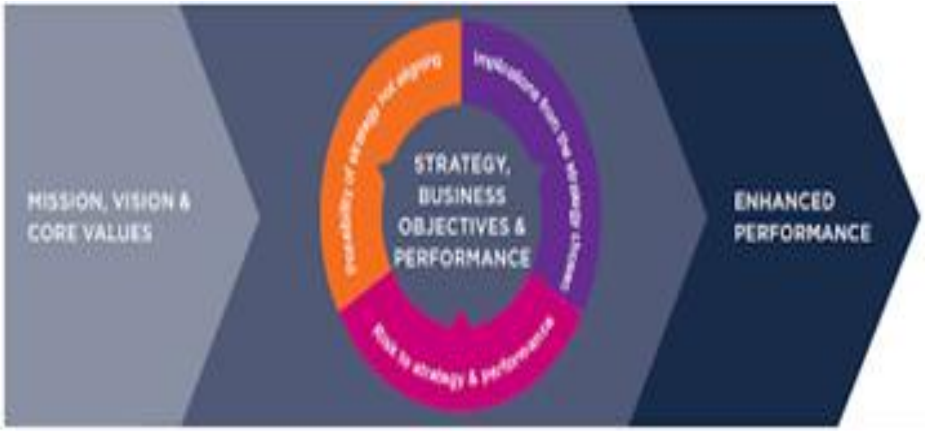
Enterprise Risk Management – Aligning Risk with Strategy and Performance

Old ERM Graphic



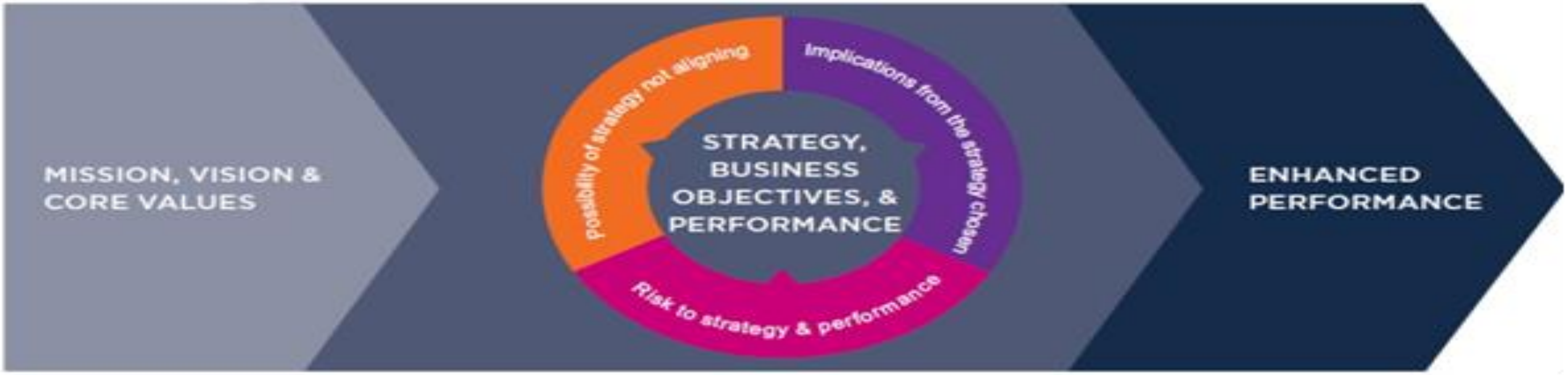
Framework provides reasonable assurance of achieving objectives through control & monitoring components.

New ERM Graphic

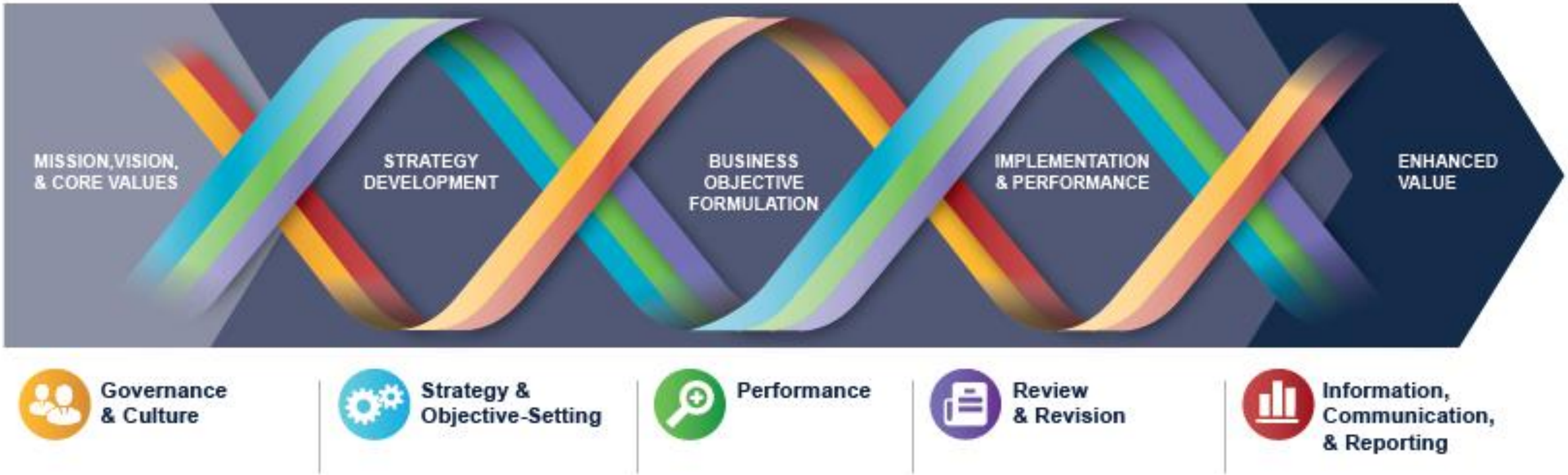

MISSION, VISION & CORE VALUES
Possibility of strategy not aligning
Implications from the strategy chosen
STRATEGY, BUSINESS OBJECTIVES & PERFORMANCE
Risk to strategy & performance
ENHANCED PERFORMANCE

Framework provides reasonable expectation of achieving objectives no control or monitoring components

COSO ERM Framework


MISSION, VISION & CORE VALUES
STRATEGY, BUSINESS OBJECTIVES, & PERFORMANCE
Possibility of strategy not aligning
Implications from the strategy chosen
Risk to strategy & performance
ENHANCED PERFORMANCE

ENTERPRISE RISK MANAGEMENT


MISSION,VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting

COSO ERM Framework

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

The COSO ERM Framework

- **Governance and Culture.** Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for ERM. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

- **Strategy and Objective Setting.** ERM, strategy, and objective setting work together in the strategic planning process. A risk appetite is established and aligned with strategy. Business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

- **Performance.** Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. **The results of this process are reported to key risk stakeholders.**

- **Review and Revision.** By reviewing entity performance, an organization can consider how well the ERM components are functioning over time and in light of substantial changes, and what revisions are needed.

- **Information, Communication, and Reporting.** ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Comparing ISO 31000 to COSO

Similarities: ISO 31000 to COSO ERM

- Seek to enhance opportunities while managing uncertainty
- Analyze risk across all aspects of an organization’s activities
- Enhance organizational resilience and decision making
- Both standards expand the scope of risk management – *encourage risk taking in order to achieve objectives.*
- Both versions are meant to be guidelines, and none targets compliance certification.
- They both focus on evaluating risk, treating risk and continually monitoring risk.
- They are very insistent on assessing risk and revising as threats constantly evolve.
- ISO 31000 offers wider directives that enable organizations to fit COSO’s principles of ERM into overarching corporate governance.

Differences: ISO 31000 to COSO

Key Term or Description	ISO 31000:2018	COSO ERM Framework
Scope.	This International Standard provides principles and generic guidelines on risk management… **it can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.**	This definition (of ERM) is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Differences: ISO 31000 to COSO

Key Term or Description	ISO 31000:2018	COSO ERM Framework
Risk management, defined.	Coordinated activities to direct and control an organization with regard to risk.	Enterprise risk management is **a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.**

Differences: ISO 31000 to COSO

Key Term or Description	ISO 31000:2018	COSO ERM Framework
Risk, defined.	The effect of uncertainty upon objectives.	The possibility that an event will occur and adversely affect the achievement of objectives.
Risk Appetite, defined.	The amount and type of risk that an organization is willing to pursue or retain.	A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.
Simplicity and Use	ISO provides a more streamlined approach that is easier to digest.	The COSO ERM Framework is a complex, multilayered and complicated directive that many organizations have found difficult to implement.
Basis of preparation	ISO is based on a management process, and through tailoring the process for each organization, it integrates into existing management and strategic initiatives.	The COSO model is control and compliance based, and that contributes to it being difficult for traditional risk managers to embrace.

Differences: ISO 31000 to COSO

Key Term or Description	ISO 31000:2018	COSO ERM Framework
Authors	ISO was authored by risk management practitioners and international standards experts	COSO was authored by auditors, accountants and financial experts
Simplicity in use	Latest version of ISO 31000 is more standardized than COSO and is only 24 pages and can be read in less than one hour.	COSO is over 100 pages long
Mode of preparation	ISO 31000 has been adopted as the official risk management standard by national standards organizations in approximately 57 countries as of the end of 2015.	COSO on the other hand was developed in partnership with PWC, one of the big four and all the principal contributors are all located in Washington DC or New York City.
Point of Focus	ISO 31000 is written for anyone interested in risk management. Many organizations heavily rely on it because of numerous other ISO standards they may be using.	COSO is targeted more towards people in accounting and audit though ***the 2017 version places greater emphasis on strategy***

Differences: ISO 31000 to COSO

Key Term or Description	ISO 31000:2018	COSO ERM Framework
Risk assessment, defined.	The overall process of risk identification, risk analysis and risk evaluation.	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risk are assessed on an inherent and a residual basis.
Risk management process	Continually and iteratively: Communicate and consult • Establish the context • Risk assessment: ✓Identification ✓Analysis ✓Evaluation • Risk treatment Continually & iteratively: Monitor and review	Internal environment Objective setting Event identification Risk assessment Risk response Control activities Information & communication Monitoring

Other ERM Frameworks

- **CoCo** – Stands for "Criteria of Control" and is a risk management tool developed by the *Canadian Institute of Chartered Accountants* to assist managers and internal auditors in designing, assessing, and reporting on control systems of an organization

- **Cadbury Report** – Published in 1992 and sets recommendations that focus primarily on practices related to transparency and accountability at the top levels of an organization rather than throughout the organization as a whole.

Other Frameworks

- **Australian and New Zealand Standard on Risk Management (AS/NZS 4360:2004**, or ASNZS) Considered by some to be the gold standard for all other risk management standards. ASNZS is widely used internationally; desirable for its simplicity.

- **Other used frameworks:**

✓ Basel III

✓ Solvency II:2012

✓ FERMA: 2002

✓ BSI 31100:2008 etc

“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

Poll Questions

Which one is better? ISO 31000 or COSO?

Those who prefer ISO 31000:2009 offered these opinions	Those who prefer COSO ERM did so because, in their view:
✓ Easier to understand and explain to others. User friendly ✓ Written by practitioners instead of accountants and auditors ✓ Clear, logical, intuitive, and practical ✓ A better 'how to' guide, easier to use when implementing risk management ✓ More focused on risk and less on audit and controls than COSO ERM ✓ Represents best practice and the collective wisdom of global risk leaders ✓ Flexible, less prescriptive, easily tailored ✓ Has a top-down approach to risk management	✓ It is comprehensive and has stood the test of time ✓ Is the standard that has been adopted by their regulators ✓ Their organization previously adopted it ✓ It links to the COSO internal control framework ✓ It has a better discussion of risk appetite ✓ It is stronger on corporate governance ✓ There is a better linkage to strategies and objectives

Which one is better? ISO 31000 or COSO?

“It Depends”

Which one is better? ISO 31000 or COSO?

- Reviewing ISO and COSO together may provide the opportunity for risk management practitioners and auditors to integrate and strengthen their activities.
- **The question is not about which one is a better standard!**. It comes down to which ***one fits your organization and culture. If you think they both do, the good news is that you could use both.***
- In deciding which standard to use, **it can be useful to read both standards and take some training to help you make the best decision.**

- *Keep in mind that if you have implemented a standard and you are struggling, it may be that the standard is not the right fit for your organization and it's ok, and you should, try a different standard.*

Steps in Establishing an ERM Framework

- □ Establish Common language around Risk
- □ Establish Risk Management Steering Committee
- □ Roles & Responsibilities must be clearly defined and understood throughout the organization.
- □ Develop a methodology for the ERM Framework including *definitions of key risk terms, descriptions of roles and responsibilities, and clear procedures for risk identification, assessment, measurement, mitigating, monitoring, and reporting.*

Steps in Establishing an ERM Framework…..

- ❑ Embark on the Risk identification via risk control self-assessment (RCSA) approach
- ❑ Using the results of the RCSA, prioritize key risks based on the residual risk levels.
- ❑ Discuss all high residual risks with the risk management steering committee and set risk mitigation plans (RMPs).
- ❑ RMPs must be established by taking a risk-based approach to address the areas with the greatest control weaknesses and largest potential for loss.
- ❑ Key risks that were identified must be monitored and periodically reported to Senior Management and Board of Directors

Pre-Requisites For Effective Implementation of ERM

1) Risk Management Policy

- ✓ Strategy for identifying, measuring, and responding to internal and external risks;
- ✓ Roles of the organization's oversight and stewardship organs in risk management;

Pre-Requisites For Effective Implementation of ERM

Risk Management Policy should contain:

- Organizational Mandate, Objectives and Functions;
- Purpose, Rationale and Objectives of ERM;
- ERM Process for Risk Identification; Assessment & Ranking; Mitigation;
- Roles & Responsibilities for ERM: Board; Audit Committee; Management; RM Committee or Function; Internal Audit

Pre-Requisites For Effective Implementation of ERM

2) Risk Management Framework that documents:

- Organization's risks and the causes of such events /outcomes (risk universe)
- Assessment and categorization of the identified risks
- Risk Mitigation Strategies and Controls
- Assignment of Responsibility for management of the risks
- Implementation Timelines
- Monitoring and Review Timelines

Pre-Requisites For Effective Implementation of ERM

3) Monitoring and Reporting system

Effective implementation of ERM requires collaborative engagement between:

Governance Organ

- Board and Audit & Risk Committee

Functions that own and manage risks

- Executive and Operating Management

Functions that oversee risks

- Risk Management and Compliance Sections

Functions that provide independent assurance

- Internal Auditors

Developing The Institutional RMF

Process of developing and implementing Institutional Risk Management Framework:

1) Establishing & Identifying the Risk Universe

   - Potential sources of risks from the Internal & External Environment;
   - The specific risks facing the institution (risk events), and their causes (risk drivers).

2) Assessing / Categorizing the identified risks:

   - Analysing the risks – likelihood /consequence.
   - Evaluating the Risk Level (likelihood x impact).

Developing The Institutional RMF

3. Risk Treatment

Strategies may include:

- Avoidance; Transfer / Sharing; Acceptance; Control **(ATAC)**
- Developing and implementing the requisite policies, procedures and internal controls to mitigate the identified risks

4. Assigning Responsibility for requisite control activities

5. Monitoring operation and effectiveness of controls.

6. Feedback and Reporting Mechanism

Draft Action Plan for an ERM Initiative

- ❑ Seek Board and Senior Management Involvement and Oversight
- ❑ Identify and Position a Leader to Drive the ERM Initiative
- ❑ Establish a Management Working Group
- ❑ Inventory the Existing Risk Management Practices of the Organization
- ❑ Conduct an Initial Assessment of Key Strategies and Related Strategic Risks
- ❑ Develop Consolidated Action Plan and Communicate to Board and Management
- ❑ Develop/Enhance Risk Reporting
- ❑ Develop the Next Phase of Action Plans and Ongoing Communications.

Do’s & Don’ts when Implementing ERM Framework

Actions to take / Dos	Actions to Avoid / Don'ts
▪ Gain support of top management and the Board ▪ Engage a broad base of managers and employees in the process. ▪ Start with a few key risks and build ERM incrementally ▪ Use/leverage on existing knowledge, skills and resources in management, internal audit, compliance etc. ▪ Build on Existing Risk Management Activities ▪ Embed ERM into the fabric (decision making) of the organization ▪ Take a holistic, portfolio view of risks across the enterprise ▪ Ensure the role & objective of ERM is understood and communicated. ▪ Provide ongoing ERM updates and continuing education for Leadership and Senior Management	▪ Never treat ERM as a project – ERM is a process ▪ Don’t get bogged down in details and history – ERM should be strategic and forward-looking ▪ Avoid relying only on a few key staff – make ERM everyone’s job. ▪ Don’t take a silo or stove-pipe approach to risks. Don’t ignore how risks might impact on other parts of the business. ▪ Avoid obsessing too much about categorizing risks – rather than ensuring that the key risks have been identified and mitigation plans developed. ▪ Never assume that the risk register is complete – there will always be ‘unknown unknowns’ and the biggest enemy of effective ERM is complacency.

Conclusion

❑ Risk management is a fundamental element of corporate governance. Management is responsible for establishing and operating the Risk Management Framework on behalf of the Board.

❑ Enterprise-Wide Risk management brings many benefits as a result of its structured, consistent and coordinated approach.

❑ The wealth of available Standards describing ERM demonstrates that it is an emerging and essential business discipline.

❑ The fact that all the Standards share more characteristic similarities than differences demonstrates that ERM is also an evolving discipline that has meaningful applications to all sectors, whether organizations are structured for profit, not for profit, governmental or non-governmental purposes. ***Since ERM is not about certification, what really matters is its application to the institution.***

❑ Internal Auditor's core role in relation to ERM should be to provide assurance to Management and to the Board on the effectiveness of risk management.

❑ Internal Auditors must clarify their roles in ERM, then can undertake workshops on risk controls, tests whether controls are working or adequate, evaluate whether changes to risk rankings do make sense and give assurance that key risks have been identified and are being addressed.

References

- ❑ IIA Practice Guide: ***Assessing the Risk Management Process***

- ❑ IIA Position Paper: ***The Role of Internal Auditing in Enterprise-wide Risk Management.***

- ❑ COSO ***Enterprise Risk Management—Integrating with Strategy and Performance, 2017***

- ❑ ***ISO 31000: 2018 Risk Management*** available from www.iso.org.

- ❑ ***International Professional Practices Framework*** (IPPF) 2017 Edition.

ERM Is a Journey…It Is Not a Destination!

Questions & Answers

CPA, CIA, Erick Audi
Contacts: Email –audi.otieno@gmail.com
Cellphone: 0702 949 960/0721 693 705

COFFEE BREAK
Coffee
CLASHOT