THE ENTERPRISE RISK MANAGEMENT(ERM) MASTERCLASS

Theme: *Demystifying the ERM implementation requirements for success*

Developing the ERM framework.

BY : SAMUEL KIBAARA, CFIRM
Director: Risk Management Consulting
PINEBRIDGE TRAINING AND CONSULTING LTD.

The Facilitator

SAMUEL KIBAARA

- Enterprise Risk Management and Business Continuity professional.

- Certified Fellow of the Institute of Risk Management
- Director at Pinebridge Training and Consulting Ltd.

- Over 22 years Risk Management Experience
- Positions held
  1. Director – Pinebridge Consulting
  2. Head of Risk Management – Kenya Power
  3. Senior Risk Consultant – Aon Risk Global
  4. Risk Surveyor – Safety Surveyors

Who is Pinebridge Training and Consulting?

Pinebridge Training and Consulting Ltd

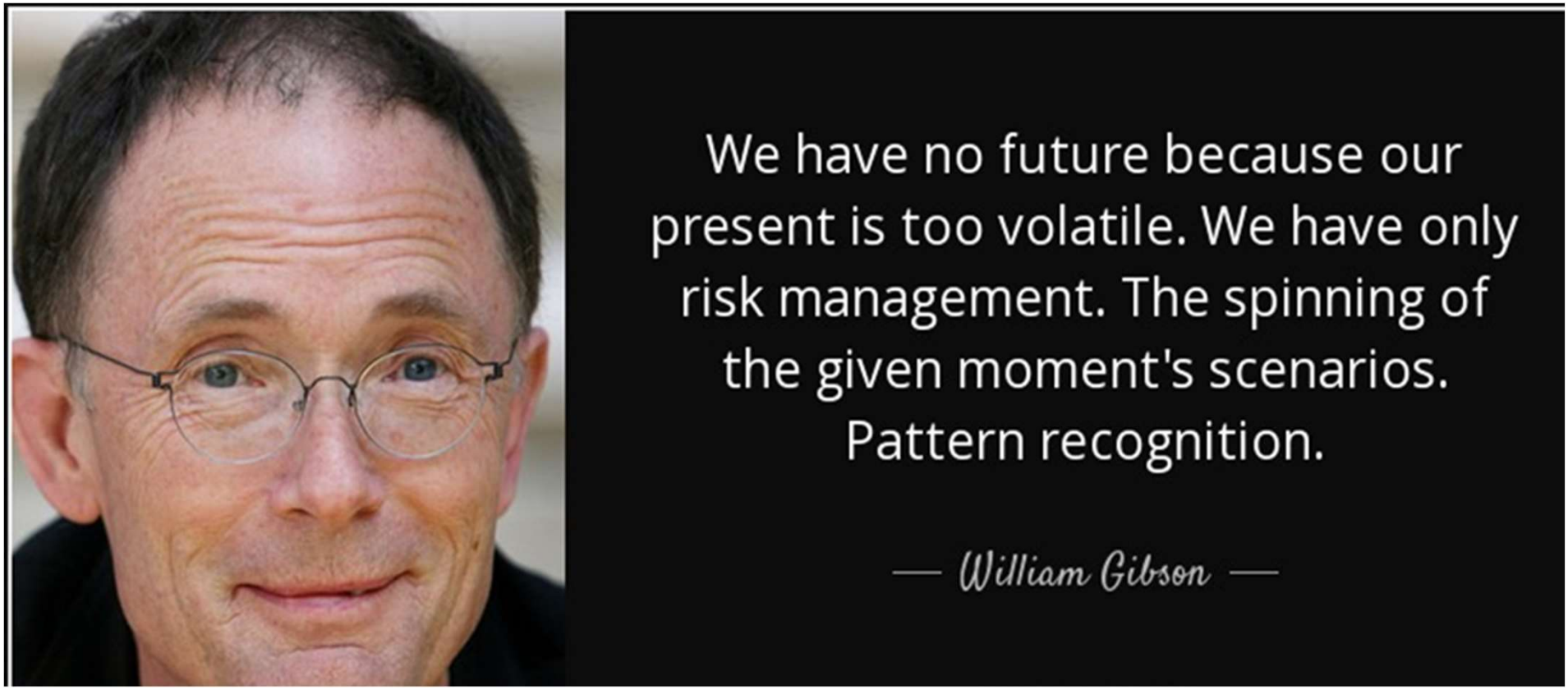
- Training
- Consulting

- Enterprise Risk Management
- Business Continuity Management
- Risk based Strategic Management
- Business Process Analysis
- Retirement Planning
- Crisis Management

info@pinebridgeconsulting.co.ke
+254 742 929 285

"Good risk management fosters vigilance in times of calm and instills discipline in times of crisis."

– Dr. Michael Ong


We have no future because our present is too volatile. We have only risk management. The spinning of the given moment's scenarios. Pattern recognition.
— William Gibson —

Why do we need an ERM framework

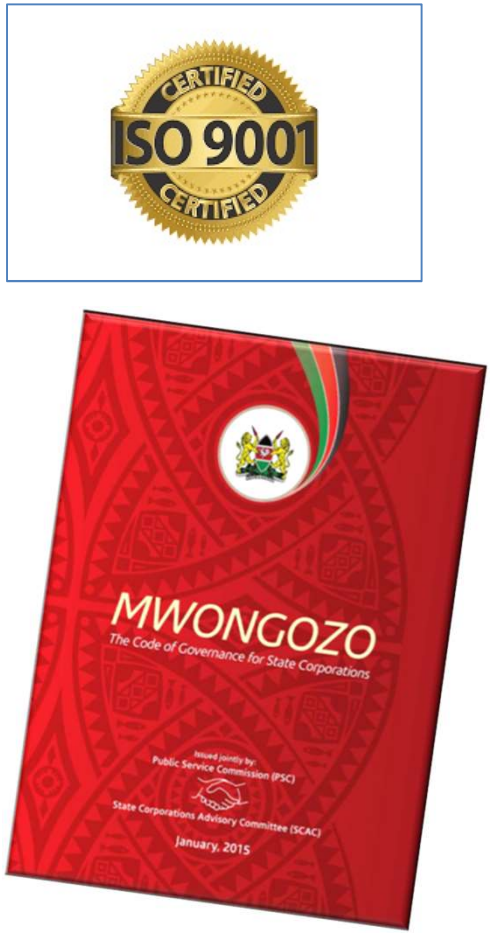
- It brings in a systematic known way for managing risks
- For Compliance Reasons
- To Build Value for the entity
- To Protect the value for the Entity

A Framework

- The definition of framework is a support structure or system that holds parts together.
- Rules, standards and policies and in ERM it means:- Risk policies, Risk Manuals, Risk management plans, Risk registers....

The Architecture!

Basis of Risk Management in the Public Sector



- Treasury Circular No 3/2009 :- *Development and implementation of Institutional Risk Management Policy framework (IRMPF)*
- 'MWONGOZO' *Code of governance for State Corporations.*
- ISO 9001:2015 – *Quality Management System*.
- Public Finance Act.
- Generally the Constitution

The Treasury Circular

MINISTRY OF FINANCE

Telegraphic Address: 22921
FINANCE-NAIROBI
Fax No. 310833
When replying please quote

THE TREASURY
P.O. Box 30007
NAIROBI.

Ref No.: MOF/ IAG/033(75)
2009

Date: 23rd February,

PERMANENT SECRETARY * MINISTRY OF ENERGY
RECEIVED
06 MAR 2009

TREASURY CIRCULAR NO 3/2009

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

DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL RISK MANAGEMENT POLICY FRAMEWORK (IRMPF) IN THE PUBLIC SECTOR

1.0 INTRODUCTION

1.1 As part of ongoing public financial management (PFM) reforms a need has been identified for a more effective corporate governance framework as well as an accountable financial management system in the public sector.

Other Guidelines

- ✓ Banking Sector – CBK guidelines
- ✓ Capital Markets guidelines
- ✓ IRA Guidelines
- ✓ SASRA Risk Management guidelines
- ✓ RBA guidelines

ISO 9001 (2008 Versus 2015)

What are the major **differences** ?

The most noticeable change to the standard is its new structure. ISO 9001:2015 now follows the same overall structure as other ISO management system standards (known as the High-Level Structure), making it easier for anyone using multiple management systems. More information can be found in Annex SL of ISO/IEC Directives Part 1 (the rules for developing ISO standards).

Another major difference is the focus on risk-based thinking. While this has always been part of the standard, the new version gives it increased prominence. More information on how to adapt to this risk-based thinking can be found on the Website run by ISO/TC 176/SC 2, the group of experts behind the standard (www.iso.org/tc176/sc2/public).

Mwongozo sec.3.2

Governance Practice

1. The Board should:

(a) Ensure the development of a policy on risk management, which should take into account sustainability, ethics and compliance risks.

(b) Set out its responsibility for risk management in the Board charter.

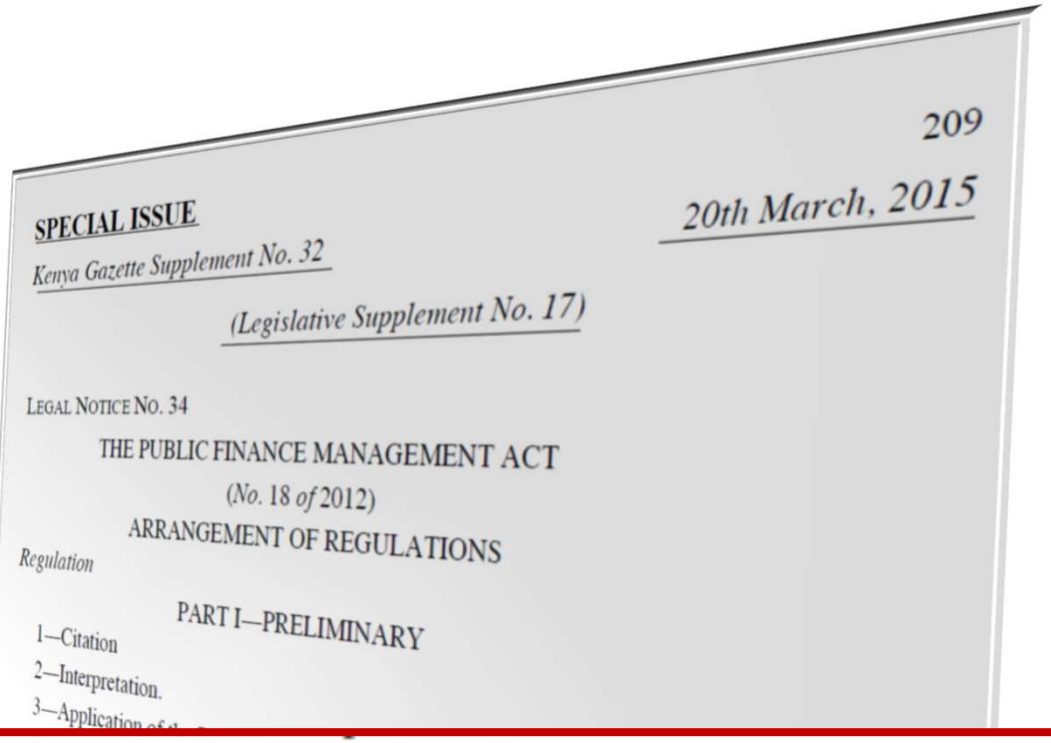
(c) Approve the risk management policy and the risk management framework.

(d) Delegate to management the responsibility to implement the risk management plan.

(e) Monitor that risks taken are within the set tolerance and appetite levels.

(f) Review the implementation of the risk management framework on a quarterly basis.

PFM Act. 2015 Regulations



209

20th March, 2015

SPECIAL ISSUE

Kenya Gazette Supplement No. 32

(Legislative Supplement No. 17)

LEGAL NOTICE NO. 34

THE PUBLIC FINANCE MANAGEMENT ACT

(*No.* 18 *of* 2012)

ARRANGEMENT OF REGULATIONS

Regulation

PART I—PRELIMINARY

1—Citation

2—Interpretation.

3—Application of

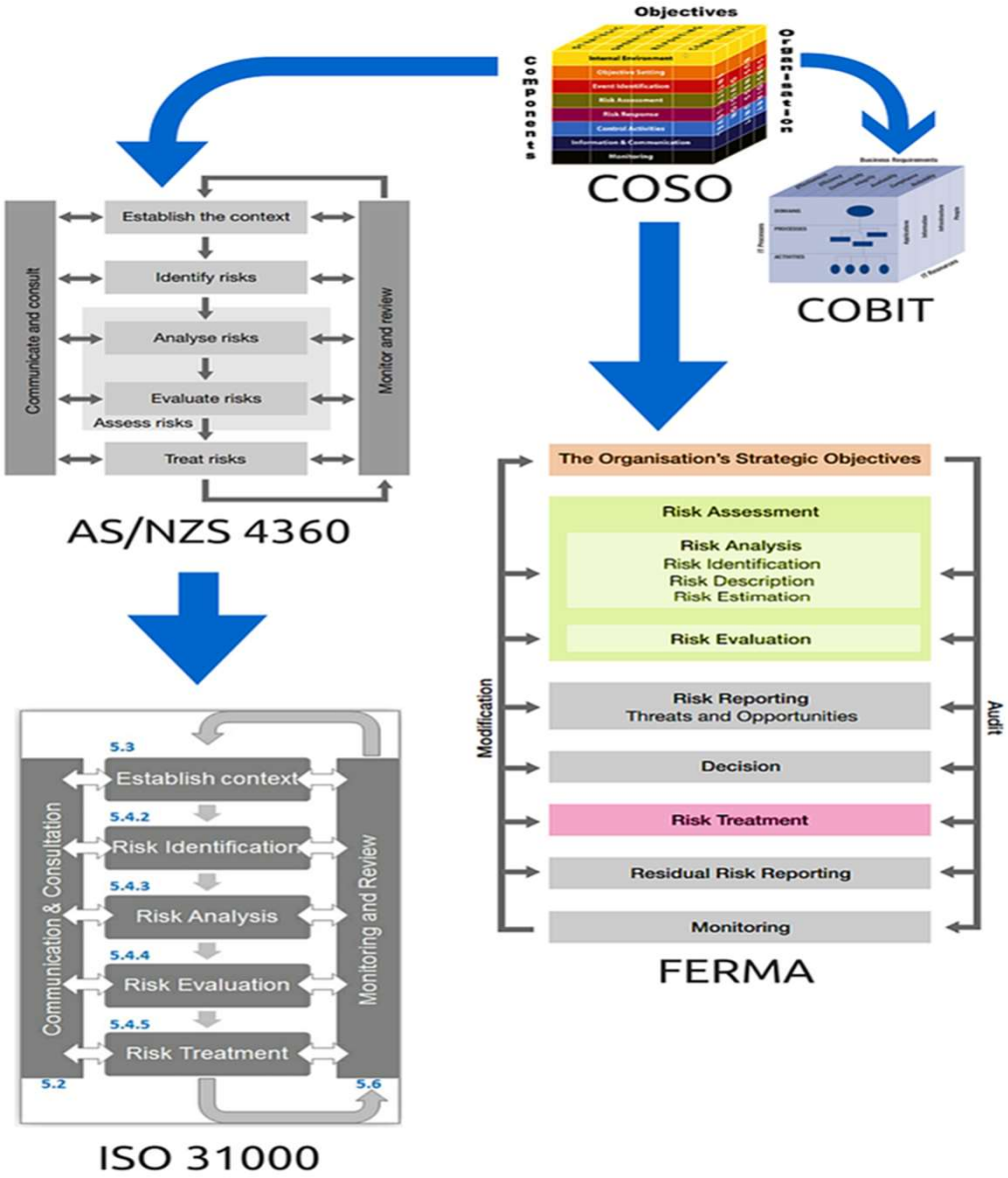
165. (1) The Accounting Officer shall ensure that the national government entity develops—

The role of Accounting Officer in risk management.

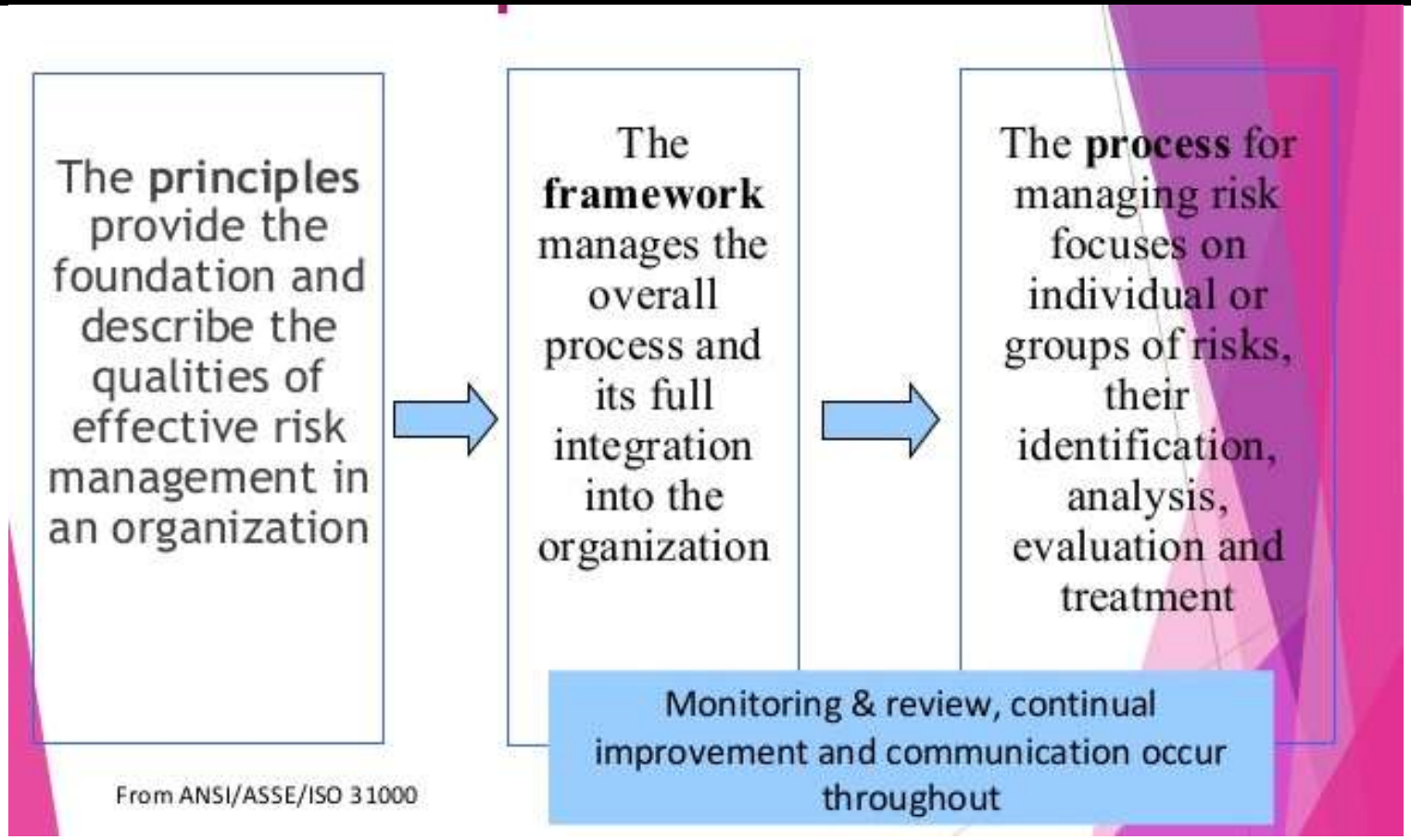
(a) risk management strategies, which include fraud prevention mechanism; and

(b) a system of risk management and internal control that builds robust business operations.

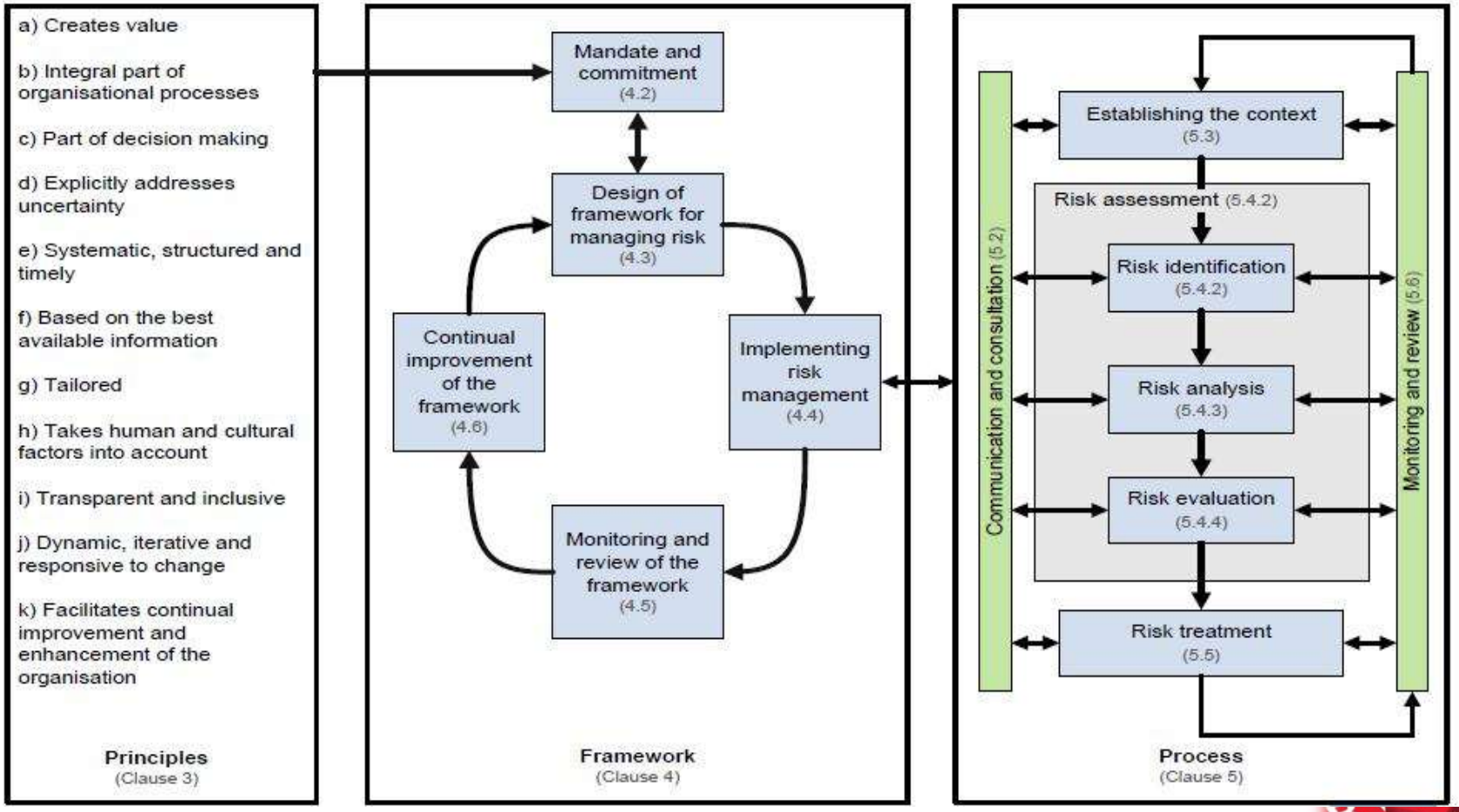
Common ERM frameworks



Critical components of ISO 31000



ISO 31000 Risk Management :
Principles and Guidelines.



COSO Internal Controls Framework

The framework consists of:

- Three objective categories
  - Operations
  - Reporting
  - Compliance
- Five components
  - Control Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring Activities
- 17 principles

Comparison of the ERM frameworks

Differences

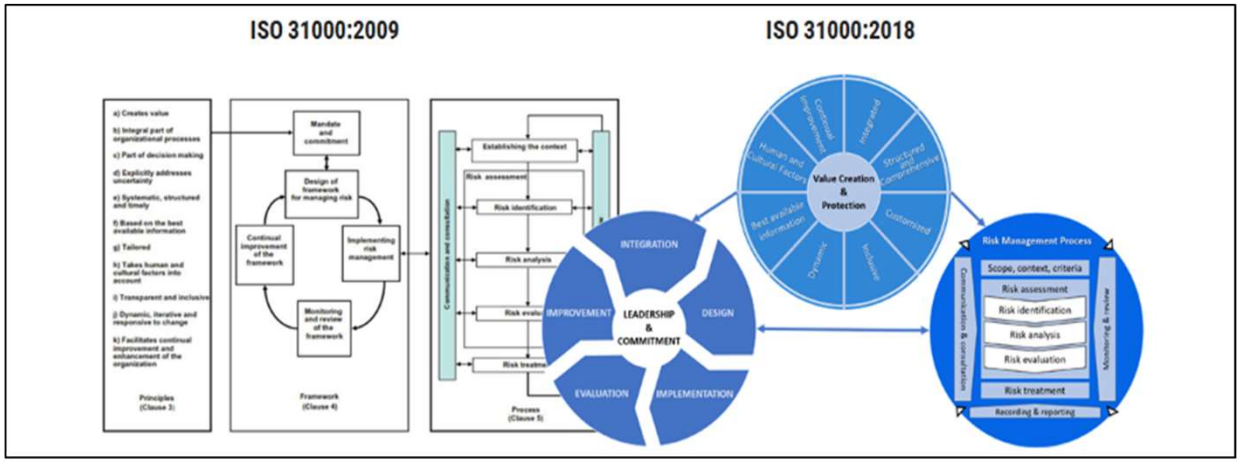
- COSO ERM framework is complex
- ISO provides a more streamlined approach
- COSO model is control and compliance based
- ISO is based on a management process
- COSO was authored by auditors, accountants, and financial experts
- ISO was authored by risk management practitioners and international standards experts
- COSO focuses mainly on the negative aspects of risk
- ISO focuses on negative and positive

COSO vs. ISO 31000 Framework

Source: COSO

Source: ISO

Recent reviews



About COSO

AICPA

American Accounting Association

fei

ima

The Institute of Internal Auditors North America

> 600,000 professionals

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM) internal control and fraud deterrence

COSO

The Committee of Sponsoring Organizations of the Treadway Commission

Timeline

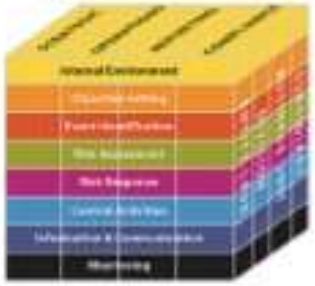
1987: Treadway Commission Report

1992: Internal Control – Integrated Framework

1996: Internal Control Issues in Derivatives

1999: Fraud Study I - Fraudulent Financial Reporting: 1987-1997

2004: Enterprise Risk Management Framework



2006: Guidance for Smaller Businesses on Internal Control over Financial Reporting

2009: Guidance on Monitoring Internal Control Systems

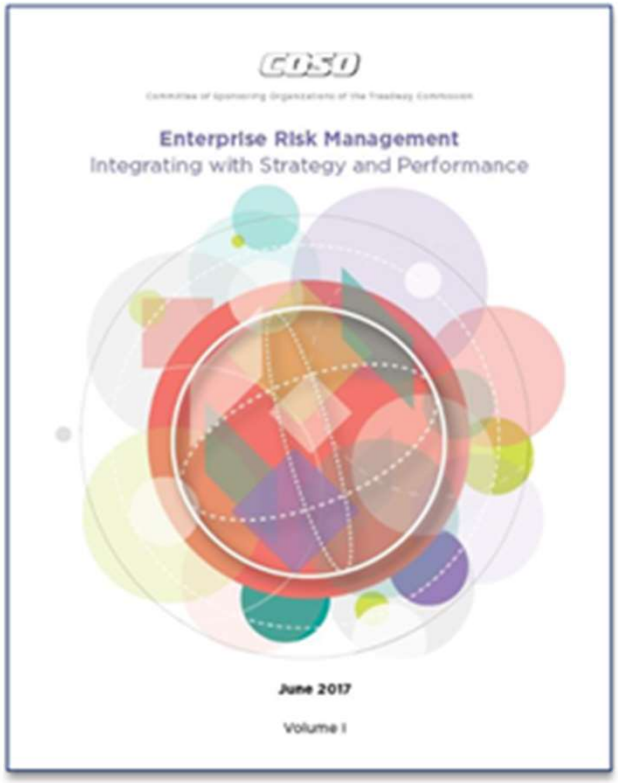
2010: Fraud Study II - Fraudulent Financial Reporting: 1998-2007

2010-2013: Recent ERM thought papers on current issues

1985 1990 1995 2000 2005 2010

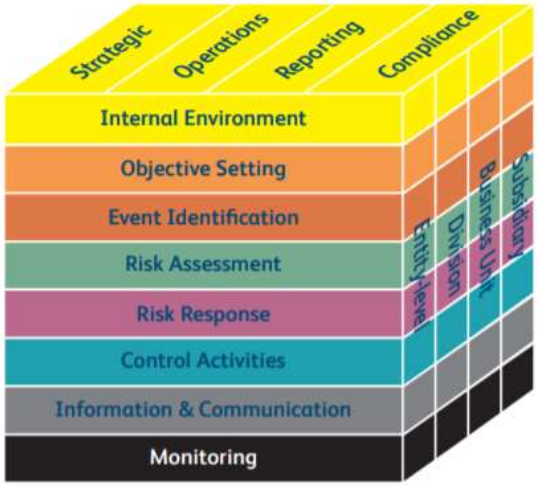
COSO 2017

A New Title



- Retitled as *Enterprise Risk Management—Integrating with Strategy and Performance*
- Recognizes the importance of strategy and entity performance
- Further delineates enterprise risk management from internal control

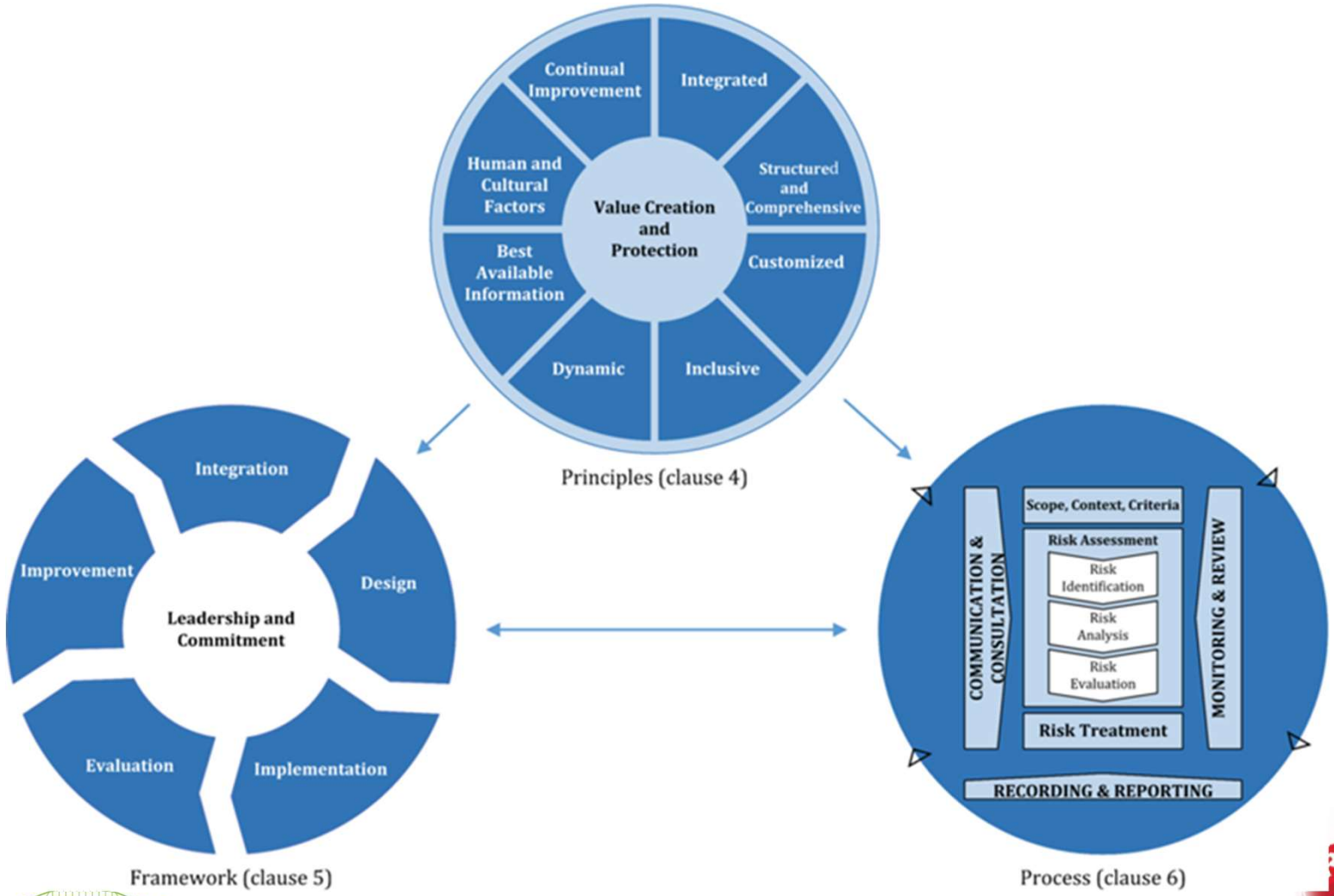

MISSION, VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
Governance & Culture
Strategy & Objective-Setting
Performance
Review & Revision
Information, Communication, & Reporting


Strategic
Operations
Reporting
Compliance
Internal Environment
Objective Setting
Event Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring
Entity-level
Division
Business Unit
Subsidiary

Details under the COSO

Mission, vision & core values	Strategy Development	Business Objective Formalation	Implementation & Performance	Enhanced Value
Governance & Culture	**Strategy & Objective-Setting**	**Performance**	**Review & Revision**	**Information, Communication, & Reporting**
1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commintment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14 Develops Portfolio View	15. Assesses Sustantial Change 16. Reviews Risk and Performance 17. Purses improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

The New ISO 31000: 2018



ISO 31000:2009 - 2018

The ISO standard has only been around for 10 years, its origins dates back to 1995 when the AS/NZS 4360 standard from Australia and New Zealand was first published.

It was then adopted and revised by ISO and Principles and Guidelines

Principles

a) Creates value

b) Integral part of organisational 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 organisation

Principles
(Clause 3)

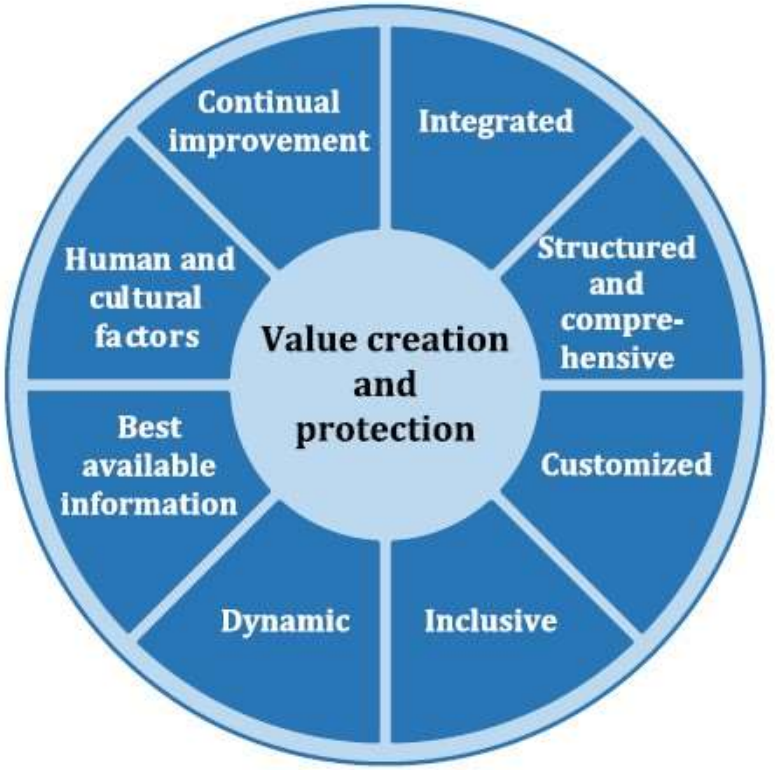
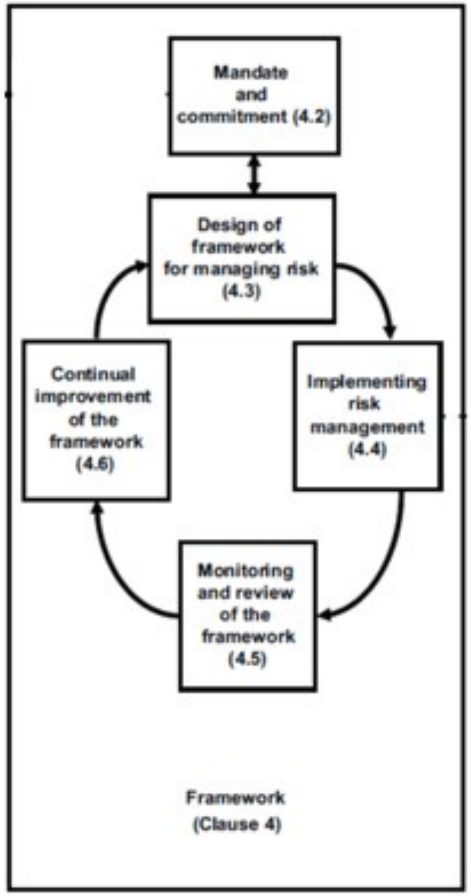


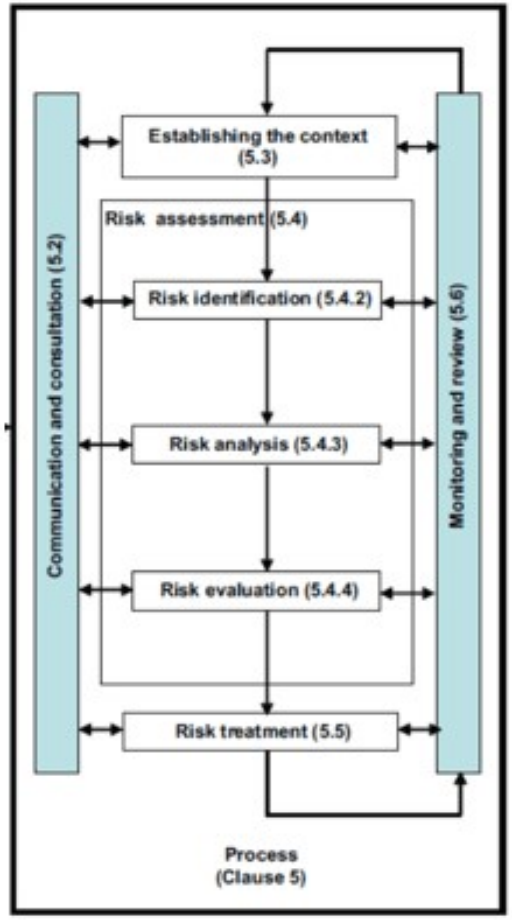
Figure 2 — Principles

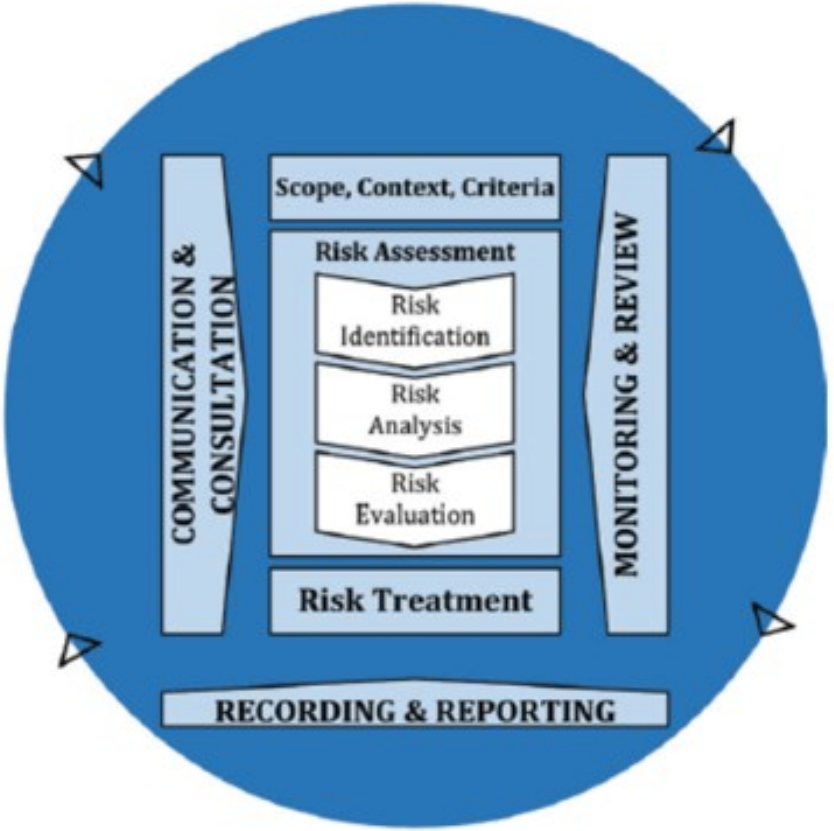
Framework


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)


Integration
Design
Implementation
Evaluation
Improvement
Leadership and Commitment
Framework (clause 5)

Process





Process (clause 6)

RISK GOVERNANCE STRUCTURE

GOVERNANCE LEVEL

Board of Directors

- Monitor effective risk management procedures
- Approve overall annual risk profile and appetite

Audit Committee

- Evalution of effectiveness of risk management procedures
- Review of overall risk profile and appetite
- Review of mitigating activities

EXECUTIVE LEVEL

Executive Management Board

- Managing risk management framework and effectiveness
- Ensure key risks and strategies are appropriately managed
- Appoint risk owners on all identified risks

OPERATIONAL RISK MANAGEMENT LEVEL

Risk responsible

- Ensure that appointed risks are analysed
- Underlying risk drivers are defined
- Mitigation plans are developed, implemented and monitored

ERM implementation

1) Develop a risk management framework and policy to ensure consistency of understanding across the organization
2) Establish a communications plan and stick with it
3) Don't underestimate the level of effort or shortchange the planning process
4) Customize ERM strategy, approach, and methodology based on the specific requirements of your organization
5) Ensure support from senior leadership which is critical to effectively identifying and addressing risks and opportunities
6) Train your staff and the Board

The risk management paradox

"The task of managing risks effectively is confounded by a classical paradox. That is, if risks are being effectively managed as a matter of routine, there will be very few surprises. Nobody becomes aware of just how effective careful risk-management actions have proven to be. Nobody slaps the manager on the back and congratulates them for a job exceedingly well done. In stark contrast, however, if risks are managed poorly, the whole world lines up to say so".

What does this tell us?

Lastly to note

For more inquiries on in-house or regular scheduled training

www.form.pinebridgeconsulting.co.ke

SAMUEL N KIBAARA; CFIRM, ACBCI

Enterprise Risk & Business Continuity professional

Director: Pinebridge Training and Consulting

Contacts: Email –
skibaara@pinebridgeconsulting.co.ke

Samkibaara@gmail.com

Cellphone: +254 722 606 497