Women in Insurance Zimbabwe

A Structured Approach to Enterprise Risk Management (ERM)

PRESENTER

WADZANAYI B. PHIRI

CORONATION
RISK ADVISORS (PVT) LTD

STRUCTURE OF THE PRESENTATION

- Introduction
- What is Risk?
- ERM VS Traditional Approach to Risk Management
- Enterprise Risk Management Frameworks
- ERM in Business Strategy
- Why talk about a Structured Approach?
- Risk Culture
- ERM Governance
- Question & Answer

INTRODUCTION

- All organisations Small/SME or Large Conglomerates; Parastatal or NGO/Civic Community; Pension Funds; Listed or Unlisted are faced with RISKS that challenge the business or its objectives.

- The speed of innovation and the highly dynamic business environment create tremendous threats and opportunities for businesses as they pursue value.

- Business leaders manage risks and they have done so for decades. Thus, calls for Enterprise Risk Management aren't suggesting that organizations haven't been managing risks. Instead, proponents of ERM are suggesting that there are benefits from thinking differently about how an enterprise manages risks affecting the business.

- Although the concept of ERM has existed for a number of years, it wasn't until the 2008 Financial Crisis that it gained significant prominence as an integral component of an institution's business strategy.

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

WHAT IS RISK?

WHAT IS RISK?

- An effect of uncertainty on objectives or deviation from the expected (ISO 31 000 Guide 73).
- An **uncertain** event or set of events which, should it occur, will have an effect on the achievement of **objectives**; a risk is measured by a combination of the **probability** of a perceived threat or opportunity occurring and the magnitude of its **impact** on objectives.
- Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative (IRM).

The term RISK is seen differently by different individuals. As you come up with your definition of RISK, try and answer some of these questions?

- What events and risk scenarios could ruin our business?
- Do we have the right counter measures and risk management strategies in place?
- How risky is our strategy?

COMPONENTS OF RISK

- Risk has three components. These components need to be considered separately when determining on how to manage the risk. Risk Components are:
  - ✓The event that could occur – the risk,
  - ✓The probability that the event will occur – the likelihood,
  - ✓The impact or consequence of the event if it occurs – the penalty (the price you pay).

- The natural instinct is to stay away from scenarios that involve risk but the fact is that even with thorough planning, RISKS CAN NEVER BE ELIMINATED.
- We have to balance the possible negative consequences of risk with the potential benefits of the opportunity.
- Risk can be dealt with by using a risk management approach which is proactive and analyses the past and possible future events to identify potential risks.
- The alternative is crisis management that is a reactive and resource intensive process whose options are restricted by the event.

RISK CLASSIFICATION

- Risk classification relates to how an organization defines the risks it faces. Coherent classification is essential to Enterprise Risk Management (ERM), as ambiguity will lead to confused reporting and management of risk.
- Each system represents a risk "language" bespoke to the organisation with organisations using different terminology for the same risks, or the same terminology for completely different risks.

- Classification may be by
  - Risk Type – Systematic or Unsystematic
  - Risk source and scope e.g. environmental, sector, organization, project
  - Risk Impact – eg critical, high, medium, low
  - Activity e.g. credit, operational, political, regulatory, Legal

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

ENTERPRISE RISK MANAGEMENT VS TRADITIONAL APPROACH TO RISK MANAGEMENT

ERM DEFINITION

- ERM is the ongoing proactive process of adopting a holistic approach across the enterprise to all the uncertainty which may affect either positively or negatively the achievement of its key purposes and objectives, leading to action to achieve greater business robustness and flexibility, efficient risk taking and an appropriate risk-reward balance.

- "ERM is a process, effected by an entity's **board** of directors, **management** and other personnel, applied in strategy setting and 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." *(Source: COSO, 2004)*

- Risk management contributes to the **demonstrable achievement of objectives and improvement** of, for example, human health and safety, legal and regulatory compliance, public acceptance, environmental protection, financial performance, product quality, efficiency in operations, **corporate governance and reputation**. *(Source: ISO 31000, 2009)*

- ERM is increasingly considered an essential component for organisations' success and growth since it adopts a more strategic, integrated and proactive perspective that enables companies to increase firm value **not only by protecting against negative events but also by exploiting opportunities.**

TRADITIONAL RISK MANAGEMENT APPROACH

Approach is also referred to as silo or stove- pipe risk management. Organisations manage risks by placing responsibilities on business unit leader to manage risks within their areas of responsibility e.g Chief Technology Officer is responsible for managing risks related to IT operations. While assigning functional experts makes good sense, the approach has some limitations:-

- There may be risks that fall between siloes that none of the leaders can see. Risk don't follow management's organisational chart and can emerge anywhere in the business.
- Some risks can affect multiple siloes in different ways. While a silo leader might recognise a potential risk, he or she might not realise the significance of that risk to other aspects of the business.
- Individual silo owners may not understand how an individual response to a particular risk might impact other aspects of the business.
- Often times this approach has an internal lens to identifying and responding to risks i.e management focusing risks related to internal operations with minimal focus on risks that may emerge from the external environment.
- While business leaders understand the fundamental connection between "risk and return" most struggle to connect their efforts in risk management to strategic planning.

TRADITIONAL RISK MANAGEMENT VS ERM

Traditional Risk Management	Enterprise Risk Management
Segmented / Departmentalized	Holistic approach
Each department/business unit/silo deals with own risk	Emanates from the "top" – typically the Board of Directors
Little or no knowledge of overall organizational risks	Broad perspective on overall organizational risks
Focus is on preventing loss within the business unit (tactical)	Focus is on lowering risk, increasing sustainability and providing savings/value across the entire organization (strategic)
Manages uncertainties around physical and financial assets	Assesses entire asset portfolio including intangibles such as customers, employees, suppliers, innovative processes, proprietary systems
Solutions to mitigating risk based on each silo's expertise and decision-making skills	Solutions to mitigating risk based on strategy-setting across the entire organization

WHY ERM FOR YOUR ORGANISATION?

- Provide greater awareness about the risks facing the whole organisation
- Embed the correct risk culture
- Ensure risk taking is within appetite
- Aide avoidance/reduction of losses
- Ensure significant risk identification and mitigation
- Improves operational efficiency and allocation of resources
- Support compliance with regulatory requirements
- Protect the organisation's reputation
- Ensure business continuity/resilience

ERM IN AN EVER-CHANGING & UNCERTAIN ENVIRONMENT

- The ability to navigate a dynamic risk landscape that changes rapidly and materializes in unexpected ways is critical for success.
- These changes modify known risks, create new ones and open new opportunities.
- There is need to scan the horizon for future risks including the detection and assessment of emerging risks. Proactivity is key.
- In this changing environment, ERM targets risks that are material and may affect its ability to achieve its business objectives.
- Having an ineffective emerging risk identification and assessment process leads to a false sense of security, inadequate or inappropriate risk transfer and mitigation programs, as well as financial and reputational damage to the organisation.

CHARACTERISTICS OF EMERGING RISKS

- Completely new risks that have never been seen before.
- Previously known risks that are evolving in unexpected ways with unanticipated consequences.
- Significance may be uncertain and not well understood.
- Difficult to quantify due to lack of data and/or volatility.
- Consequences and implications can be ambiguous.
- Interactions and interconnectedness with other risks can be complex.
- May be systemic and outside of organizational control.

From a Global Perspective, the following risks are considered as emerging:

Global Geopolitical risks, Failed or Failing States, Global Food Shortages, Global Societal Risks, Global economic Risks, Pandemics; Global Technological Risks and Global Environmental Risks including climate change.

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

ERM FRAMEWORKS

ERM FRAMEWORKS

By definition a framework is a guide that provides an overview of different interconnected activities within an organisation to achieve its targets. A framework helps in the implementation of ERM.

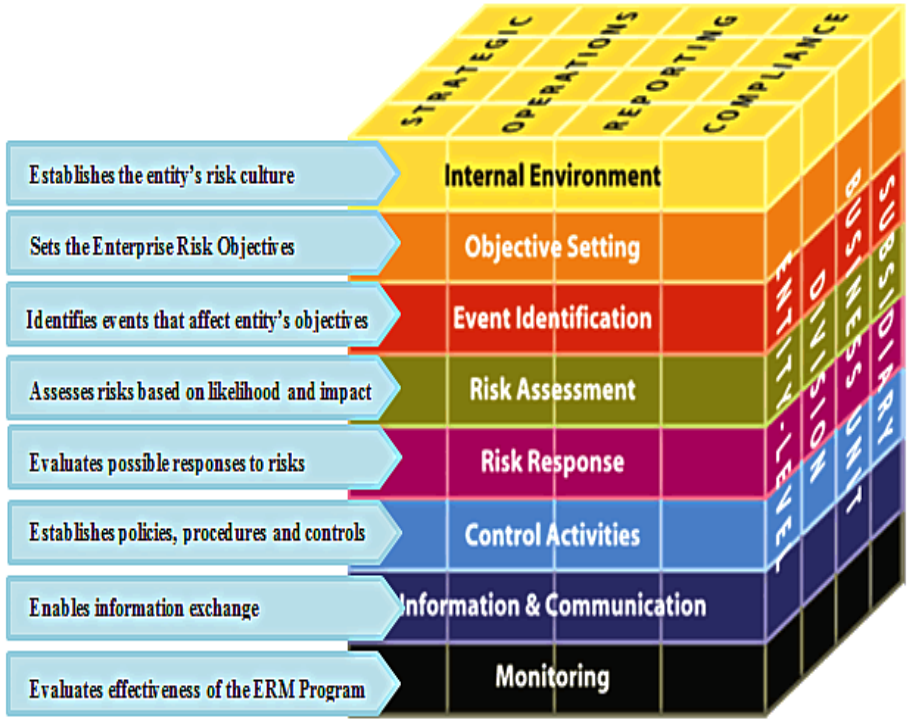
The focus on ERM has led to the development of various ERM frameworks, each of which describes an approach for identifying, analysing, responding to, and monitoring risks and opportunities, within the internal and external environment facing the enterprise. The following frameworks/standards have been developed and are widely used:

- ISO 31000: 2009 - Risk Management - Practices and Guidelines
- COSO: 2004 - Enterprise Risk Management - Integrated Framework
- Risk & Insurance Management Society (RIMS) Risk Maturity Model
- FERMA 2002
- BSI 31100:2008 etc

Each framework/standard is useful for organisations to understand a complete picture of ERM and gives an idea of how to implement ERM in an effective way.

ERM FRAMEWORKS - COSO FRAMEWORK

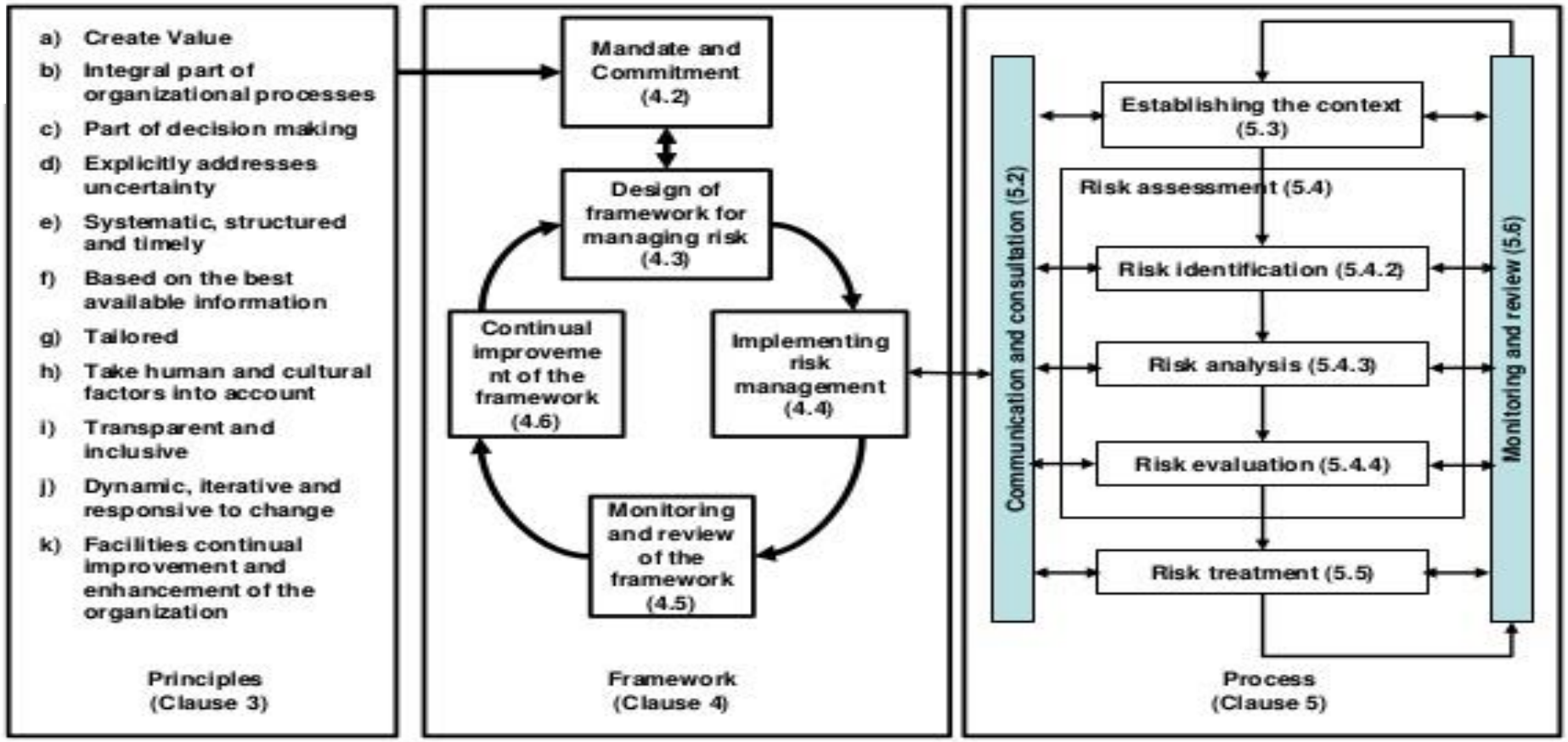
The Committee of Sponsoring Organisations of the Treadway Commission (COSO framework) is a joint initiative dedicated to guide executive management and governance entities on relevant aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.



- This enterprise risk management framework is geared to achieving an entity's objectives which are:
  - ✓ Strategic: high-level goals, aligned with and supporting its mission
  - ✓ Operations: effective and efficient use of its resources
  - ✓ Reporting: reliability of reporting
  - ✓ Compliance: compliance with applicable laws and regulations
- The framework applies to activities to all levels of the organization regardless of the structure

ISO 31000

Published in 2009 (revised 2018) as an internationally agreed standard for the implementation of risk management principles. It is defined as “a process that provides confidence that planned objectives will be achieved within an acceptable degree of residual risk.”



CORONATION

RISK MANAGEMENT ADVISORY

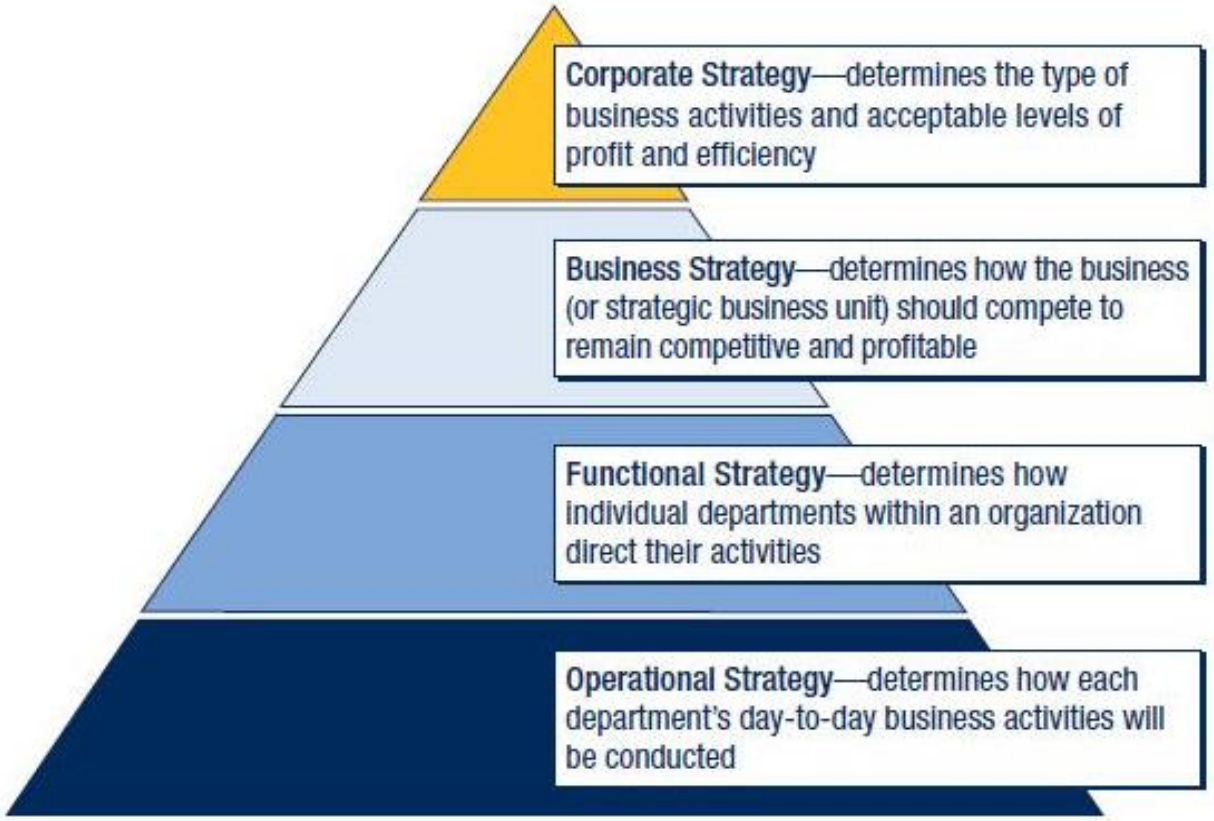
Your Trusted Advisors

ERM IN BUSINESS STRATEGY

RISK IN STRATEGY SETTING

- In many cases, risk management activities are not linked or integrated with strategic planning, and strategic risks can be overlooked creating dangerous “blind spots”
- The challenge, as well as opportunity, for council is to embed risk thinking and risk management explicitly into the strategy development and strategy execution processes.
- Strategic priorities often change over time, and if risk management activities do not address these changes and priorities to ensure that strategic alignment is maintained, associated efforts can become reactive, misaligned and compliance-focused rather than supportive of strategic decision-making.

RISK IN STRATEGY SETTING -
ORGANIZATIONAL LEVELS



STRATEGIC RISK ASSESSMENT

- An assessment of the strategy at strategy setting itself will assist the Council's focus on understanding and providing guidance on strategy and associated risk and monitoring senior management's performance in both carrying out the strategy and managing risk
- A simple process for strategic risk assessment involves four steps:

✓Risk assessment of plans including an understanding of how they drive value and the key assumptions those plans are based on including scenario analysis

✓Identify critical risk scenarios and considering the severity and likelihood of the events and scenarios that might occur, especially those outside management's control, such as systemic risks.

✓Identify possible countermeasures for managing the critical risk scenarios consider the cost/benefit of the countermeasures.

✓Establish a process for continuous monitoring of the risk profile of the council, including the use of key risk indicators (KRIs).

RISK APPETITE

- Risk appetite can be defined as ‘the amount and type of risk that the Council is willing to take in order to meet their strategic objectives.
- Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.
- A clearly defined risk appetite will ensure that decisions made are in line with the overall strategic objectives of the Council.
- The Council must understand how much risk it is willing to take and how it plans to balance risks and opportunities before designing and executing a set strategy.
- The Councillors/Board should take into account the risk expectations of shareholders, regulators, and the risk capacity of the council, including the amount and type of risk the council is able to support

RISK TOLERANCE

- Risk tolerance is the range of risk council is able to withstand and is within the risk appetite level. It involves weighing a number of factors that affects the decision of whether or not to accept a risk.
- The acceptable or “tolerable” deviation from the level set by the risk appetite which the council is willing to allow as it pursues its objectives e.g. 2% drop in revenue collection may be allowable and therefore tolerable.
- Therefore risk appetite and risk tolerance go hand in hand
- Risk tolerance is defined at the council level and is reflected in the various policies formulated at the executive level.
- At the operational or tactical level, exceptions can be tolerated or are allowable as long as the overall risk exposure does not exceed the set risk appetite.
- Thresholds are set for each risk to ensure that risks faced are within the acceptable or tolerable range and are expressed in the form of key risk indicators.

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

RISK MANAGEMENT PROCESS

- Recognition or identification of risks
- Ranking or evaluation of risks
- Responding to significant risks
    - tolerate
    - treat
    - transfer
    - terminate
- Resourcing controls
- Reaction planning
- Reporting and monitoring risk performance
- Reviewing the risk management framework

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

RISK CULTURE

RISK MANAGEMENT CULTURE

- Culture – It is our way of doing things.
- Risk culture describes the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose.
- Risk management must be integrated into the culture of the organisation and includes mandate, leadership and commitment from the Board.
- Leadership must be the driver of the correct risk culture.
- It must translate risk strategy into tactical and operational objectives, and assign risk management responsibilities throughout the organisation.
- It should support accountability, performance measurement and reward, thus promoting operational efficiency at all levels.
- An effective risk culture is one that enables and rewards individuals and groups for taking the right risks in an informed manner.

HOW DO YOU EMBED A RISK CULTURE - THE PROCESS

- Review current risk culture & risk maturity level and determine a target level – a vision.
- Risk management awareness, training and induction process (applies to all members of staff)
- Secure and maintain support and buy-in from senior management. Promote a strong tone from the top.
- Develop risk management policies for the company and ensure implementation across the organization.
- Report and communicate regularly and consistently aligned to other organisational processes e.g. monthly budgeting, quarterly reviews etc
- Ensure there are clear descriptions of risk management roles, responsibilities, processes and language.
- Integrate risk into performance management process –appraisals, compensation / rewards, balanced scorecards, reporting of near misses.

ERM GOVERNANCE: THREE LINES OF DEFENSE MODEL

Source: FERMA/ECIIA

ERM GOVERNANCE – ROLES AND RESPONSIBILITIES

Risk Governance Roles and Responsibilities

Board of Directors

- Sets organization's risk appetite
- Stays informed of the most significant risks to the organization and of senior management's responses

Chief Executive Officer

- Ensures the organization has a positive internal environment and risk culture
- Provides leadership to operational management and monitors risk activities in relation to risk appetite
- Realigns risk appetite to evolving and emerging risks

Senior Management

- Converts strategy into operational objectives
- Identifies and assesses risks' impact on objectives' achievement
- Effects risk response consistent with risk tolerance

Chief Risk Officer

- Establishes risk management policies, defines roles and responsibilities, and sets goals for implementation
- Develops functional risk management framework
- Promotes risk management competence in the organization
- Establishes common language, reporting, and monitoring mechanisms

Internal Audit

- Assures the board and senior management that risks are understood and managed
- Proposes improvements in governance, risk management, and control structure

Operational Management

- Assigns risk management procedures for day-to-day functions and internal controls

"Monitoring the Effectiveness of Internal Control, Internal Audit and Risk Management Systems," Guidance on the 8th EU Company Law Directive, Article 41, FERMA, ECIIA, September 2010, pp. 7–8. [DA10420]

CORONATION

RISK MANAGEMENT ADVISORY

Your Trusted Advisors

Managing risk well is the essence of good business practice and is everyone's responsibility.

To succeed at risk management, you have to embed it in the organisation through its structure and culture and get the right people!


WIZ
Women in Insurance Zimbabwe