GOVERNANCE RISK AND COMPLIANCE (GRC)

PRESENTED BY:
HANAFI BABA-AHMED,CFE, CAMS, FCIN

OUTLINE

- Overview
- Definitions
- Why GRC
- Risk, Types, Assessment, and Controls
- Elements of Effective GRC
- GRC Implementation
- Expectations
- Challenges
- Way Forward

METHOD

ANDRAGOGY

Overview

- GRC is a discipline that aims to synchronize information and activity across governance, risk and compliance in order to operate more efficiently, enable effective information sharing, more effectively decision making, report activities and avoid wasteful overlaps.
- It is also aimed at ensuring an organization reliably achieves its objectives, addresses uncertainty, and acts with integrity.

OVERVIEW

- GRC is also a strategic framework that organizations implement to ensure they operate efficiently, effectively and in adherence to relevant laws, regulations and industry standards. It encompasses the processes, policies and practices that are put in place to manage and mitigate potential risks while also maintaining compliance with internal policies and external obligations .

Definitions

- Governance –refers to the system of rules, processes and structures that guide and control an organizations actions and decision making. It involves defining clear roles, responsibilities and accountability across all levels of the organization.
- Risk management is the process of identifying, assessing and controlling potential threats and vulnerabilities that could affect an organization's ability to achieve its objectives. These risks can arise from various sources, including financial, operational, legal, reputational, and cybersecurity factors.

Definitions cont---

- Compliance means adhering to internal policies, industry standards, external laws and regulations that govern an organization's activities. Organizations must meet legal obligations and industry-specific requirements to avoid potential legal liabilities, reputational damage and financial loss.

Definition-Compliance

It means abiding by a set of rules.

- Laws/Regulations
- Standards/Specific Industry Standard
- Ethical/Professional Conducts
- (The culture of every organization is determined by its level of compliance)
- Compliance refers to adhering with the mandated boundaries (laws and regulations) and voluntary boundaries (company's policies, procedures, etc.).

RISK

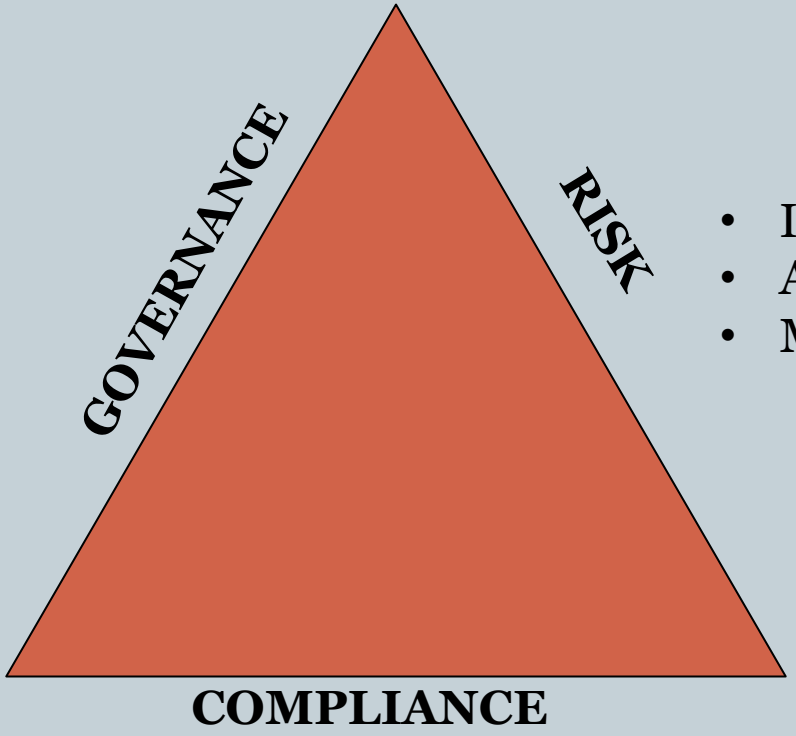
- Threats x Vulnerabilities =RISK
- Risk is measured in terms of Likely x Impact= Risk
- Intent x Capabilities = Threat
- Authority x Monopoly - Transparency = Corruption

(Anything that could have negative consequences on the organization)

Risk management is predicting and managing risks that could hinder the organization from reliably achieving its objectives under uncertainty.

The GRC

- Policies
- PODSCORB
- Discipline



- Identification
- Assessment
- Mitigation/Controls

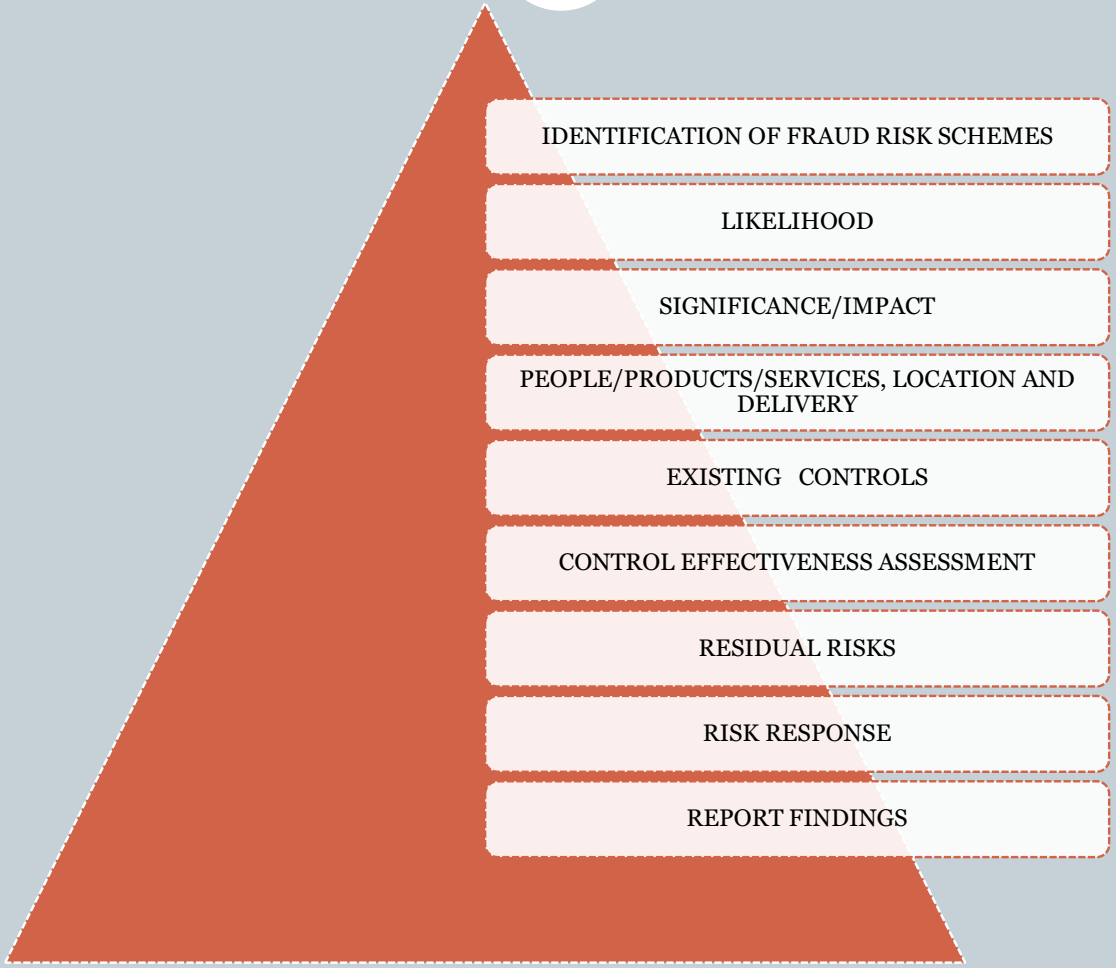
- Laws/regulations
- Standards/best practices
- Cooperation/collaborations

Types of Risk

WHY GRC

Reduce Risk	Reduce Cost	Avoid Duplication of Functions	Enable Business	Protects	Ethic/Integrity

FRAUD RISK DOCUMENTATION

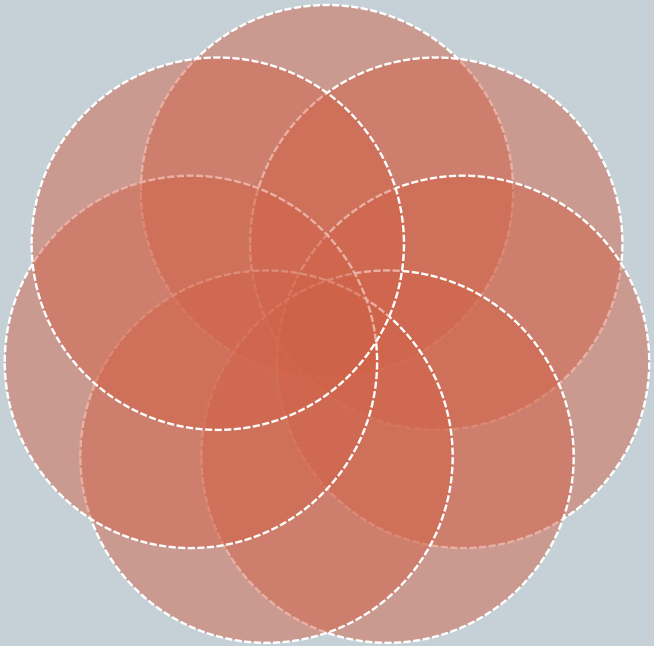


CONTROLS

Segregation of duty/Clear Reporting line

Follow up on Audit findings and remediation

Set Access controls/Authorization limits



Proper record keeping, Retention/ Archiving and Retrival

Proper controls for acquisition and disposal of assets

Regular reconciliation of Books/Accounts

Accurate Fixed Assets Register

Controls the 3lines of defence

- First line (business operations and all having first contact with customers)
- Second line (compliance monitoring, control and report)
- Third line (Internal Audit independent assurance, review, findings, reporting to board and follow up)

GRC IMPLEMENTATION STEPS

- Understand the Issues
- Define Stakeholders Requirement
- Determine Scope
- Governance Principles/Compliance Policy
- Identify Obligations/Risks
- Develop Plans to Meet Obligations and Address Risks
- Establish Accountability/Responsibility

Expectations

- High Level of Cooperation and Collaboration
- Development of Risk Assessment Report
- Have Effective Controls Commensurate to Risks
- Development of Comprehensive Operation Manual.
- Appointment of the Right CCO
- Submission of Quality Reports
- Create Fraud Awareness Among all Employees
- Conduct Proper CDD on All Beneficiaries on a Risk Sensitive Basis

Cont----

- Monitor Accounts
- Monitor Transactions
- Screening of Beneficiaries
- Proper Record-keeping and Retrieval of Information
- Efficient Internal Control System
- Prompt Response to Requests
- Maintenance of Confidentiality of Information
- Attachment of Required Documents
- Rendition of Regulatory Returns.

CHALLENGES

- Clear Absence of Compliance Function/Risk Assessment Report
- Lack of Comprehensive Policy Manual/SOP
- Not Appointing the Right CCOs/Auditors
- Poor Record-Keeping
- Not Screening Beneficiaries and Their Transactions on the Spot
- Lack of Understanding of Legal and Regulatory Requirements
- Difficulty in Accepting Change and Adoption to Changes

Way forward

- Good Understanding of Laws/Regulations
- More Cooperation and Collaboration
- Improved Quality and Quantity of Statutory Reports
- Development of Comprehensive Risk Assessment Report and Policy Manuals
- Conducting Proper Internal Investigation Before Filing and Responding to Requests/Reports
- On-the-Spot Screening of Beneficiaries and Transactions

CONCLUSION

PLAN

- PROFESSIONALITY
- LEGALITY
- ACCOUNTABILITY
- NECESSITY

THANK YOU FOR LISTENING