GOVERNANCE, RISK & COMPLIANCE

CPD FOR MEMBERS IN COMMERCE & INDUSTRY
AUGUST 2018
A growing regulatory environment, higher business complexity and increased focus on accountability have led enterprises to pursue a broad range of governance, risk and compliance initiatives across their organisations.

However, these initiatives are un-coordinated in an era when risks are interdependent and controls are shared. As a result, these initiatives get planned and managed in silos, which potentially increases the overall business risk for the organisation.

In addition, parallel compliance and risk initiatives lead to duplication of efforts and cause costs to spiral out of control.

Governance, Risk and Compliance process through control, definition, enforcement, and monitoring has the ability to coordinate and integrate these initiatives.
GRC - OVERVIEW

- Governance
  - Keep the Board informed about key risks and changes to the risk profile

- Risk
  - Embed a framework and process for identifying, assessing and controlling risk within an organisation

- Compliance
  - Understand and efficiently allocate resources to satisfy the regulatory and cultural requirements within which your business
GRC - DEFINITION

- GRC is the integrated collection of capabilities that enable an organisation to reliably achieve objectives, address uncertainty and act with integrity.

- GRC represents the capabilities that integrate the governance, management and assurance of performance, risk and compliance activities.

- GRC is viewed as an integrated collection of all capabilities necessary to support Principled Performance and does not burden the business, it supports and improves it.
GRC - DEFINITION

- Corporate Management
- Strategy
- Policy Management

- Identification
- Evaluation and Management of Risks

**common**
- Sources
- Master data
- Target groups

**GOVERNANCE**

**RISK MANAGEMENT**

**COMPLIANCE**

Measures to ensure guarantee conformity with laws, policies and formalities
GRC DRIVERS

- Stakeholders demand high performance along with high levels of transparency
- Regulations and enforcement are ever-changing and unpredictable
- Exponential growth of third-party relationships and risk is a management challenge
- The costs of addressing risks and requirements are spinning out of control
- The harsh (and scary) impact when threats and opportunities are not identified
GRC - OBJECTIVES

**Governance**
- Organization Structure – Authority, responsibility & accountability
- Board compliance capabilities - ethics & policy compliance etc.
- Business performance reporting on BSC, Risk Score Cards, Operational control dashboards
- Policy management, documentation & communication

**Risk Management**
- Identify, Assess and Prioritize risk
- Identify key controls & establish risk mitigation procedures
- Establish a risk reporting & oversight framework & training
- Develop a risk model & risk rating criteria

**Compliance**
- Freezing on Compliance checklist as per Business requirement
- Assigning accountability & responsibility
- Assessment & Audit
- Reporting & Certification
FRAMEWORK FOR EFFECTIVE GRC

- Clear levels of accountability for board, management and key staff responsible for risk management
- Updated at least annually as part of business planning process
- Risk assessment framework is understood and managed by the business
- Optimise investments to update compliance programmes and activities
GRC – IMPLEMENTATION RISKS

- Establishing departments and programmes (performance management; risk management; compliance; corporate social responsibility) which operate as silos
- When implemented in silo it is tend create counter-productive objectives are established, sub-optimal strategies are selected, and performance is not optimised
- High costs
- Lack of visibility into risks
- Inability to address third party risks
- Difficulty measuring risk-adjusted performance
- Too many negative surprises
GRC – IMPLEMENTATION RISKS

CURRENT STATE

- LACK OF EFFECTIVE OVERSIGHT
- ORGANIZATIONAL & FUNCTIONAL SILOS
- DISJOINTED STRATEGY
- SLIPPING THROUGH THE CRACKS
- LACK OF VISIBILITY
- COMPLEXITY
- FRAGMENTATION
- LACK OF INTEGRITY
- HIGH COSTS
- WASTED RESOURCES
- DUPLICATION
- WASTED INFORMATION
- UNNECESSARY COMPLEXITY
GRC – IMPLEMENTATION STRATEGY

- Integrating GRC capabilities does not mean creating a mega-department of GRC and doing away with decentralised management.

- Establishing an approach that ensures:
  - the right people get the right information at the right times;
  - the right objectives are established;
  - the right actions and controls are put in place to address uncertainty and act with integrity.

- Benefits of implementing GRC correctly:
  - Reduced costs
  - Reduced duplication of activities
  - Reduced impact on operations
  - Achieved greater information quality
  - Achieved greater ability to gather information quickly and efficiently
  - Achieved greater ability to repeat processes in a consistent manner
GRC – IMPLEMENTATION STRATEGY

FUTURE STATE

EFFECTIVE OVERSIGHT

ETHICS

INTEGRATED REPORTING & ANALYTICS

INTEGRITY

INTEGRATED GRC STRATEGY

INTEGRATED RISK & CONTROL ACTIVITIES

INTEGRATED & QUALITY INFORMATION

LEGAL, HR, IT + OTHER

FINANCIAL OFFICER

BUSINESS OPERATORS

AUDIT EXECUTIVE

RISK EXECUTIVE

COMPLIANCE EXECUTIVE

©2012 OCEG. Permission by OCEG is required for reproduction and/or use of material
www.OCEG.org -- Derived from the OCEG GRC Illustrated Series
GOVERNANCE

- With an increase in activism among shareholders and increased scrutiny from the regulatory bodies, corporate boards and executive teams are more focused on governance related issues than ever before.

- Governance is the oversight role and the process by which companies manage and mitigate business risks.

- The governance process within an organisation includes elements such as definition and communication of corporate control, key policies, enterprise risk management, regulatory and compliance management and oversight (e.g. compliance with ethics and options compliance as well as overall oversight of regulatory issues) and evaluating business performance through balanced scorecards, risk scorecards and operational dashboards.
GOVERNANCE - PRINCIPLES

- Openness, transparency and integrity
- Good governance
- Effective collaboration
- Performance orientation
GOVERNANCE FRAMEWORK

Defining Governance Roles
- Role of the board
- Board structure
- Role of individual directors
- Role of the chair
- Role of the company secretary
- Role of the CEO

Key Board Functions
- Strategy
- CEO
- Monitoring
- Compliance
- Risk management
- Policy framework
- Networking
- Stakeholder communication
- Decision making

Board Behavioural Dynamics

Board Effectiveness
- Director protection
- Board evaluation
- Director remuneration
- Director selection
- Director induction
- Director development

Improving Board Processes
- Board meetings
- Board meeting agenda
- Board papers
- Board minutes
- Board calendar
- Committees
RISK MANAGEMENT

- Risk management enables an organisation to evaluate all relevant business and regulatory risks and controls and monitor mitigation actions in a structured manner.

- With the recent increase in regulatory mandates and increasingly activist shareholders, many organisations have become sensitised to identifying and managing areas of risk in their business: whether it is financial, operational, IT, brand or reputation related risk.

- These risks are no longer considered the sole responsibility of specialists - executives and the boards demand visibility into exposure and status so they can effectively manage the organisation’s long-term strategies.

- As a result, companies are looking to systemically identify, measure, prioritise and respond to all types of risk in the business, and then manage any exposure accordingly.
WHAT IS ERM? It is the capability to effectively answer the following questions:

- What else can go wrong and how are risks interconnected?
- What are we doing about the risks?
- How well do we manage the risks?
- How do we determine the size and scope of the risks and report the results?
- What are all the risks to our business strategy and operations?
- How much risk are we willing to take?
- How good are we at overseeing risk taking?
- How do we ensure we have the right information to manage risk?

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key
RISK MANAGEMENT - FRAMEWORK

Risk management framework

- Identify
- Measure
- Manage
- Monitor
- Report
Compliance ensures that an organisation has the processes and internal controls to meet the requirements imposed by governmental bodies, regulators, industry mandates or internal policies.

Compliance is not a one-time event - organisations realise that they need to make it into a repeatable process, so that they can continue to sustain compliance with that regulation at a lower cost than for the first deadline.

When an organisation is dealing with multiple regulations at the same time, a streamlined process of managing compliance with each of these initiatives is critical, or else, costs can spiral out of control and the risk of non-compliance increases.

The compliance process enables organisations to make compliance repeatable and hence enables them to sustain it on an ongoing basis at a lower cost.
COMPLIANCE - FRAMEWORK

**Commitment**
- Governing Policy
- Top-down commitment
- Aligned to objectives
- Resources allocated
- Obligations identified & assessed

**Implementation**
- Roles & responsibilities assigned
- Training undertaken
- Culture & behaviours encouraged
- Controls established

**Monitoring**
- Compliance performance monitored & reported
- Compliance demonstrated through both documentation & practice

**Improvement**
- Compliance Framework regularly reviewed & continually improved
COMPLIANCE - FRAMEWORK
GRC - PROCESS

GOVERNANCE RISK AND COMPLIANCE PROCESSES

- Governance:
  - Document Process and Risks
  - Define and Document Controls
  - Assess Effectiveness of Controls
  - Disclosure & Certification of Compliance Processes
  - Remediate Issues

- Risk Management:
  - Identify and Categorize Risk
  - Assess Risk
  - Mitigate Risk
  - Report on Containment of Risk

- Compliance:
  - Document Process and Risks
  - Define and Document Controls
  - Assess Effectiveness of Controls
  - Disclosure & Certification of Compliance Processes
  - Remediate Issues
GRC - PROCESS

Efficient and Effective utilisation of resources

- Governance
- Management
- Operations

- Performance
- Risk
- Compliance
- Principle, Strategy, Policy
- Organisation Structure
- People
- Process
- Technology
- Information
- Physical, Financial, Intellectual assets
- Third Party - Suppliers

- Business Functions
- IT Functions
- Support Functions (HR, Admin, Legal, Marketing, Procurement, Audit..)

Optimise Business attributes
GRC - BENEFITS

- Cutting costs – The integrated approach of GRC often brings real financial benefits as unnecessary spending can be cut, while the clearer focus can help boost revenue at the same time. The bigger the business, the more likely it is that there will be plenty of areas where there is crossover and wastage, so a process like this can transform efficiency.

- Less duplicated work – This is where most of the cost-cutting can be made, but it’s about more than just the money. Having similar processes duplicated across a business is a hugely inefficient way to operate and GRC can free up whole teams to work on other projects.

- Less negative impact – Having too many procedures, especially ones that aren’t working in a logical manner, can waste a lot of time for staff across a business. Tying everything together in an GRC strategy cuts down on the paperwork and bureaucracy, which will boost your staff’s productivity, not to mention their morale.
GRC - BENEFITS

- Greater information quality – A more centralised and consistent approach to governance, risk management and compliance helps to not only speed up the processes for gathering the necessary information, but also improve the quality of what is gathered, helping decisions be made more rapidly and with greater confidence.

- More ability to repeat processes – Another huge benefit is that processes can be standardised across these areas, allowing for them to be repeated more easily and with greater consistency and efficiency.

- Reputation security – Risk management and compliance are both essential parts of any attempts to secure your business’s reputation, so it goes without saying that managing these aspects more efficiently provides a more effective method of reputation security.
GRC - BENEFITS

- Better allocation of resources – Getting more information and understanding more about areas that are duplicating work can help determine the most effective directions for your business to go in.

- No more silos – Any large business has numerous issues with staff working in ‘silos’ where information doesn’t flow in or out in a productive manner. GRC won’t completely eradicate these issues, but it will certainly minimise their potential impact on key areas.
GRC - TECHNOLOGY

- Governance
  Culture, politics, processes & laws that determine how a company should conduct itself.

- Risk
  Effect of uncertainty on organizational objectives.

- Compliance
  Act of adhering & demonstrating adherence to laws, regulations, corporate policies & procedures.

- IT Security
  Integration of Governance, Risk, and Compliance elements.
GRC - INTEGRATION

Source: KPMG LLP
GOVERNANCE, RISK AND COMPLIANCE
Governance, Risk, Compliance At-A-Glance

**Governance**
- Set and evaluate performance against objectives
- Authorize business strategy & model to achieve objectives

**Risk Management**
- Identify, assess and address potential obstacles to achieving objectives
- Identify / address violation of mandated and voluntary boundaries

**Culture**
- Establish an organizational climate and individual mindset that promotes trust, integrity and accountability

**Compliance**
- Encourage /require compliance with established policies and boundaries
- Detect non-compliance and respond accordingly