

Governance, Risk and Compliance

An Integrated Approach for the Insurance Industry

International Insurance Foundation

September 22, 2006

Washington D.C.

Governance, Risk and Compliance

1. The Business Issues

2. GRC Key Concepts and Techniques

Appendix: Key Definitions

Global Insurance Companies face several drivers for an integrated approach to Governance, Risk and Compliance (GRC)



Issues We Hear from Our Clients

A more integrated approach to managing governance, risk and compliance issues is needed because of....

- Speed at which new regulatory requirements are enacted
- Expansion internationally and need to customize codes of conduct and performance expectations
- Complex operations using different administrative systems limits consolidated reporting
- Manual processes that increase the risk of non-compliance
- Knowledge gaps in people responsible for reporting on risk and compliance issues
- Board-level reporting must be relevant, informative and at an appropriate level of detail

GRC: From a Defensive Reaction...

GRC has historically been viewed as a major opportunity **driven by avoidance of negative consequences** such as:

- Fines for compliance failures
- Ethical and financial scandals as a result of executive misbehaviour
- Financial results surprises that severely damage corporate reputation and brand image
- Increased cost of capital as a result of poor practices
- Inefficiencies in operations and high operational costs
- High compliance costs due to duplications of controls

To a Proactive Opportunity

Today, the **ability to deal with the future** is at least equally important in driving the need for an integrated GRC approach

Major global insurance companies have recognised that they need to be more **anticipatory and proactive** to be successful

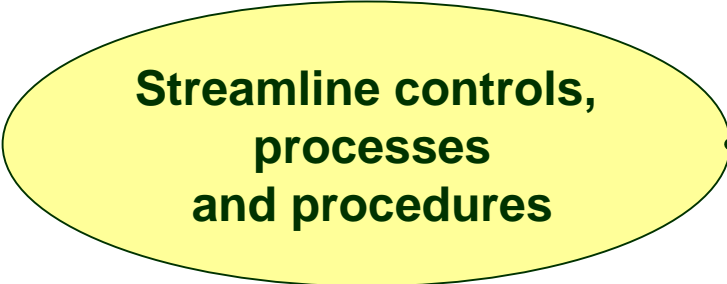
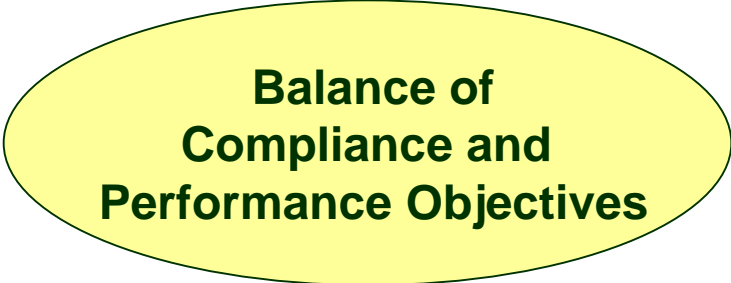
Challenges include:

- Managing more complex business models e.g., multi-territory operations
- Accelerating the rate of change required due to an increase in competitive pressures (new products, methods of distribution)
- Dealing with greater dependency on an increasing variety of different stakeholders to execute strategy
- Anticipating improved financial and non-financial information accountability and transparency demands by investors and other stakeholders
- Introducing higher standards of performance for integrating compliance requirements into the operations.

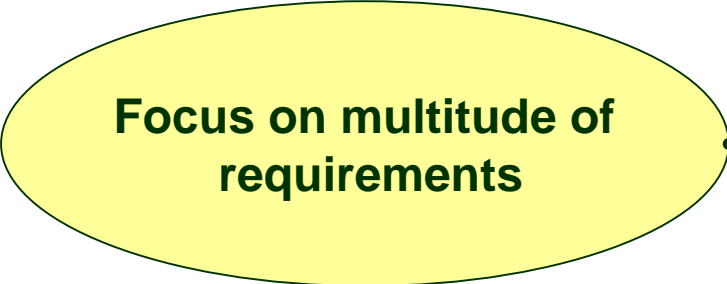
Sustainable Insurance Regulatory Compliance: Shifting from Defensive Reaction to Proactive Opportunity

Reduce compliance costs
Improve Efficiency and Effectiveness

Look at other business commitments



Need to comply with State, NASD, SEC regulations



GRC Challenges - PwC 8th Annual Global CEO Survey

- A majority (54%) consider GRC to be an integrated set of concepts and practices but only 25% state that they are managing GRC effectively
- Very few CEOs (7%) view GRC as related solely to laws and regulations, but while many CEOs say that they adequately address stakeholder concerns that are based on clear-cut legal requirements, fewer feel the same level of comfort with other constituents, whose expectations are more ambiguous
- While a majority of CEOs are very confident that their organisations can respond to GRC matters related to domestic laws and regulations (68%) and to internal policies and procedures in domestic business units (57%), only 26% are very confident that their organisations can respond to similar matters related to foreign laws and regulations and only 24% to matters related to internal policies and procedures in foreign business units
- 58% of the CEOs indicate that GRC expenditures are primarily an investment and 38% view them as a cost, but only 17% of all CEOs state that they can very accurately measure GRC costs

GRC Challenges - PwC/META Group Research

PwC/META Group Research revealed the following:

Strategic View	Operational Issues	Future Trends
<ul style="list-style-type: none">▪ See GRC as a value driver▪ The need for connection among GRC is understood and valued - although operational issues exist▪ Exposure to substantial risk through insufficient commitment to risk management	<ul style="list-style-type: none">▪ Manual processes are instrumental to meet GRC requirements▪ Most do not have significant real-time GRC capability - 1/3 of regulated respondents are “not even close”▪ Growing investment area, but light on cost and value measurement▪ Investment shifting to technology	<ul style="list-style-type: none">▪ Significant improvements are expected in the areas of data accuracy, quality of decision making, task redundancies, etc.▪ Technology will be a critical GRC enabler▪ Effective GRC can realise value in the areas of reputation and brand, employee retention and revenue

PwC View on GRC

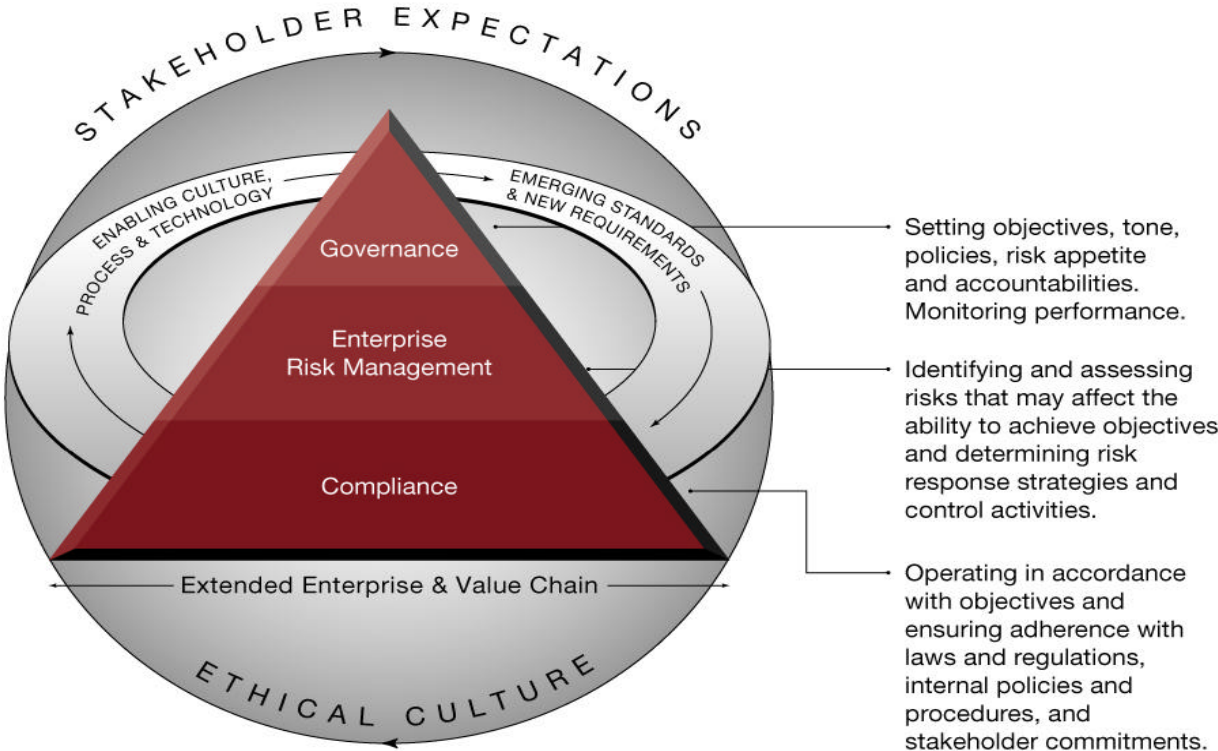
“In itself GRC is not new. As individual issues, governance, risk management and compliance have always been fundamental concerns of business and its leaders. What is new is an emerging perception of GRC as an **integrated** set of concepts that, when applied holistically within an organisation, can add significant value and provide competitive advantage”

Source: “8th Annual Global CEO Survey, Bold Ambitions, Careful Choices”, PricewaterhouseCoopers

Integrated GRC means...

Understanding the demands of the organisation's stakeholders in terms of performance and conformance, and aligning the organisation to deliver against these objectives, in consideration of the risk appetite and risk tolerance of the organisation

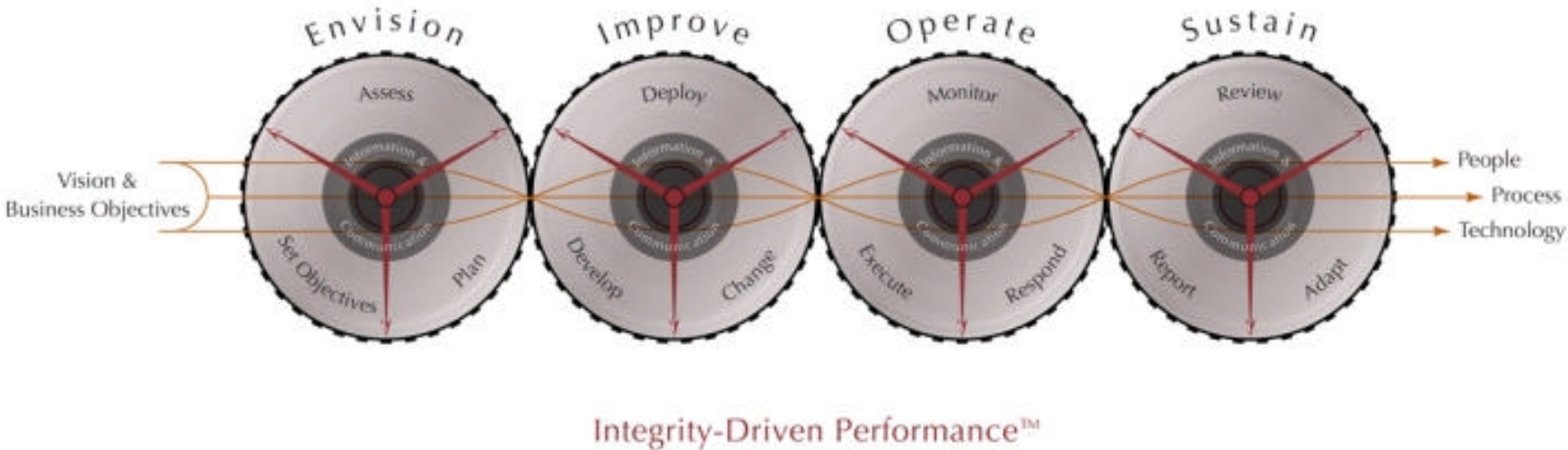
The people, processes and technology should be designed and deployed such that the achievement of objectives are measured, risks assessed and continuous improvement realised in support of effective governance, risk management and compliance



Integrated GRC in Operation

The GRC Operating Model represents PwC's view of what an organisation that has successfully integrated GRC has in place.

Governance, Risk & Compliance Operating Model™



Underpinning Principles of Integrated GRC

- Integrated GRC implies a holistic view of governance, risk and compliance - one which identifies synergies among the structures and activities required to support the business
- Organisations should broaden their vision of corporate governance
- Organisations should embrace a new vision of compliance - one that focuses not only on laws and regulations, but also on internal standards and policies and stakeholder expectations and regards compliance as an outcome, not a function
- Organisations should regard risk management as an integral part of business decision making
- Objectives across the organisation should be aligned to support the mission, business objectives, strategy and values of the organisation

Underpinning Principles of Integrated GRC

- Governance, risk and compliance objectives should be linked not only to conformance/compliance responsibilities but also to performance objectives
- Organisations need to define an appropriate balance between conformance (meeting compliance requirements) and performance
- Organisations should have a way of managing the increasingly complex array of business commitments to which they are to comply. GRC-related activities should be performed in a cost optimal way
- Key GRC enablers are people, processes and technology

Appendix

Key Definitions

GRC Key Definitions - GRC

“The organisation’s practices and the various roles that the board and senior management, line management and the rest of the organisation play in relation to oversight, strategy, risk management and strategy execution regarding compliance with laws and regulations and internal policies and procedures”

Source: “8th Annual Global CEO Survey, Bold Ambitions, Careful Choices”, PricewaterhouseCoopers

GRC Key Definitions - Governance

“Corporate Governance refers to the process and structure used to direct and manage the business and affairs of an organisation with the goals of ensuring its financial viability and enhancing shareholder value. Equally important, it encompasses the impact of key strategic decisions on *all* stakeholders, from investors and employees to customers, suppliers and the public.”

Source: PricewaterhouseCoopers working definition

GRC Key Definitions: Enterprise Risk Management

“Enterprise risk management is a comprehensive, systematic approach for helping all organisations, regardless of size or mission, to identify events and measure, prioritise and respond to the risks challenging its most critical objectives and related projects, initiatives and day-to-day operating practices“

Source: “Enterprise Risk Management Methodology Overview/Baseline v1.2”, PricewaterhouseCoopers, p.1

“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”

Source: “Enterprise Risk Management - Integrated Framework”, COSO II

GRC Key Definitions - Compliance

“Compliance is a desired outcome, with regard to laws and regulations, internal policies and procedures and commitments to stakeholders that can be consistently achieved through managed investment of time and resources “.

Source: “Integrity-driven Performance, A New Strategy for Success Through Integrated Governance, Risk and Compliance Management, A White Paper”, PricewaterhouseCoopers, p.25



GRC Key Definitions - Rule Base

A Rule Base is an agreed upon set of business commitments which reflect an organisation's corporate strategy and objectives and risk appetite. This set of commitments should:

- Support the achievement of the organisation's value proposition
- Be based on stakeholder expectations
- Be designed to achieve the required balance between performance and conformance objectives
- Reflect the organisation's key business drivers, attitude to risk, constraints and enablers

Defined in this way, it is a key element of an organisation's management framework that allows visibility to be created for the management of challenges and opportunities relating to business performance and conformance requirements

Integrated GRC