

What is GRC and Why does it matter?

Norman Marks

Vice President, Evangelist, Business Analytics

London, 2010

The gap between Strategy and Execution



Today, companies struggle to bridge the gap between strategy and execution to optimize their business performance

“Less than 10% of strategies effectively formulated are effectively executed”

– Fortune Magazine

“Defects and breakdowns in planning and execution cited as primary contributing factors to value destruction”

– Harvard Business Review : “Turning Great Strategy into Great Performance”

Why is there a gap?



- Decisions may be made based on unreliable or untimely information
 - Affects setting of strategy as well as planning, execution, and monitoring
- Employees don't understand how the strategy affects them, and how their decisions impact others
- It's unclear who is accountable for ensuring execution of initiatives, projects, and tasks

Why is there a gap?



- There's no link between budgeting and strategy
- There's no link between strategy and risks
 - Risks are not addressed and managed, during strategy definition, planning, execution, or monitoring
- Incentive systems aren't linked to strategy, individual goals are not aligned with the company's
- Plus ... there needs to be Executive Commitment and a culture that embraces performance management

“

... the financial crisis can be to an important extent attributed to failures and weaknesses in corporate governance arrangements. **When they were put to a test, corporate governance routines did not serve their purpose to safeguard against excessive risk taking in a number of financial services companies.**

- Information about exposures did not reach the board and even senior levels of management
- Risk management was activity rather than enterprise-based.
- Boards approved strategy but did not establish suitable metrics to monitor its implementation.
- Remuneration systems have not been closely related to the strategy and risk appetite of the company and its longer term interests.

- 70% failed to identify 50% of 2009 adverse events
- 70% failed to assess 50% of risks adequately

“

In the complex and constantly changing sea of acronyms, abbreviations and other abstractions, there is one that is simultaneously met with affirmation and apathy, confirmation and confusion, and recognition and rejection.

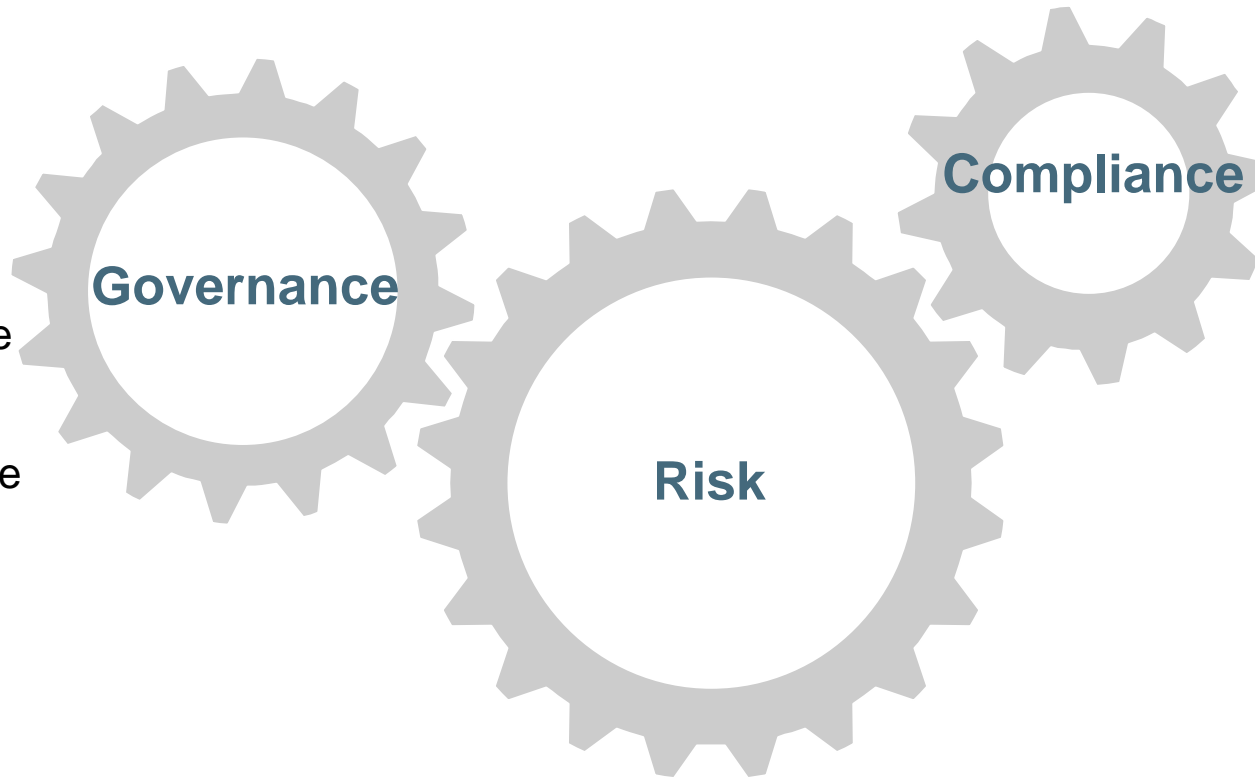
- Lee Dittmar, Deloitte & Touche

“

An academic definition of the word 'mess'.

- CFO.com magazine

The culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.



Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

The effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organization to recognize opportunities while managing negative events.

“A system of people, processes and technology that enables an organization to:

- understand and prioritize stakeholder expectations;
- set business objectives that are congruent with values and risks;
- achieve objectives while optimizing risk profile and protecting value;
- operate within legal, contractual, internal, social and ethical boundaries;
- provide relevant, reliable and timely information to appropriate stakeholders; and
- enable the measurement of the performance and effectiveness of the system.”

Source: OCEG

The goal: Principled Performance



MANDATED BOUNDARY

boundary established by external forces including laws, government regulation and other mandates.

OPTIMIZE PERFORMANCE

strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES

strategic, operational, customer, process, compliance objectives

OBSTACLES

VOLUNTARY BOUNDARY

boundary defined by management including public commitments, organizational values, contractual obligations, and other voluntary policies.

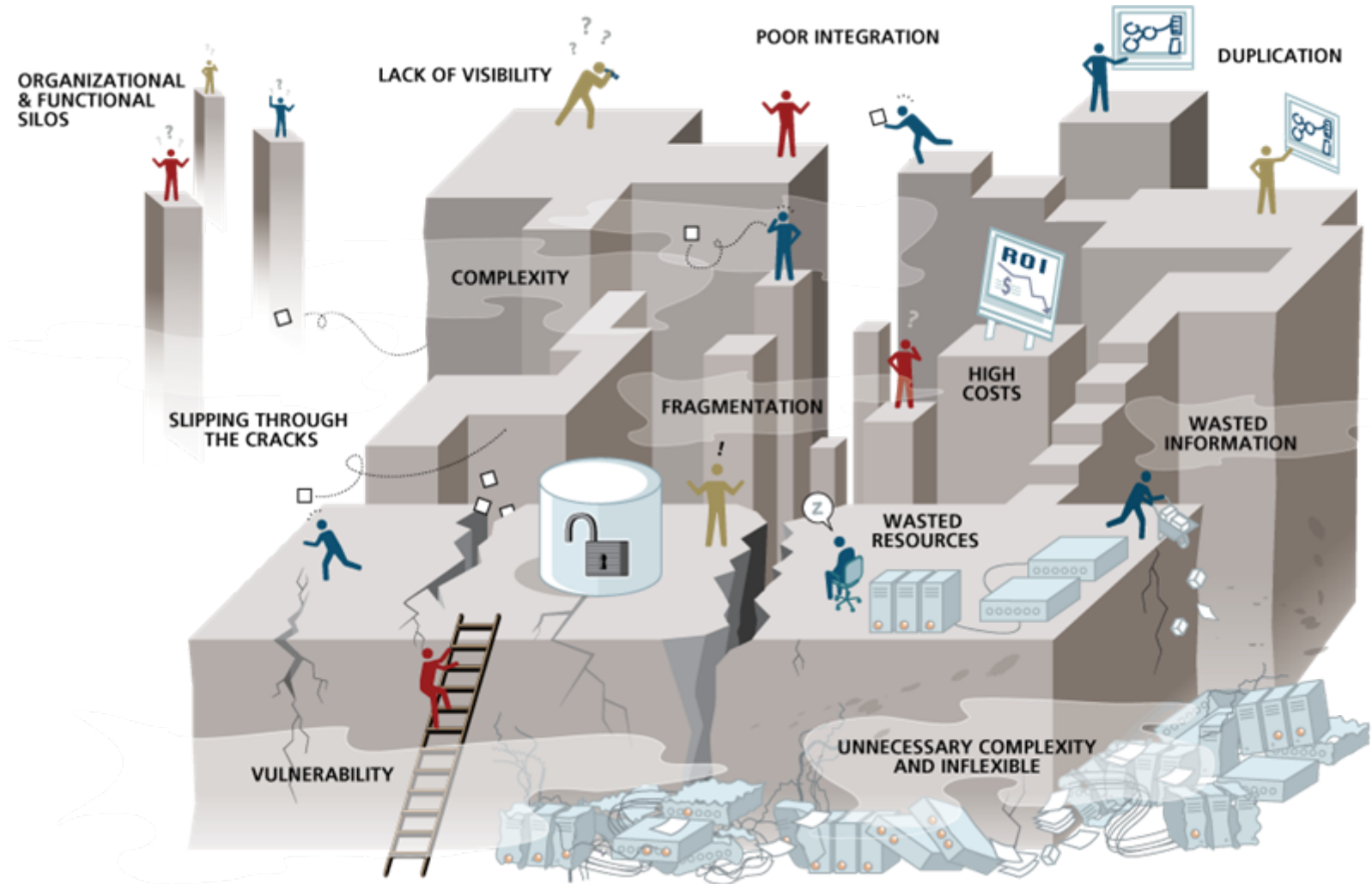
GRC typically includes:



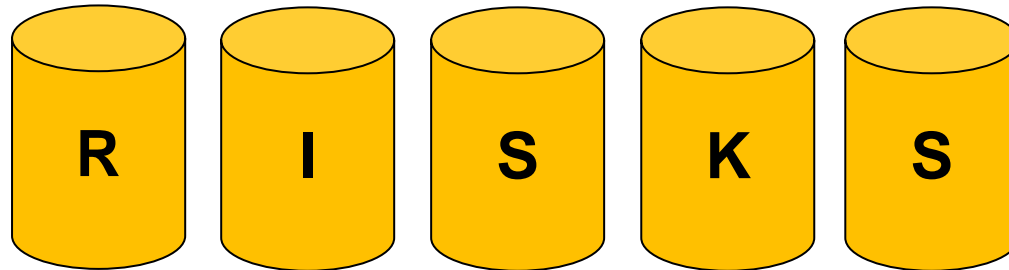
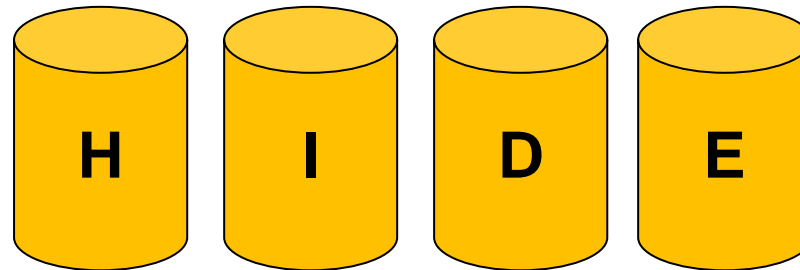
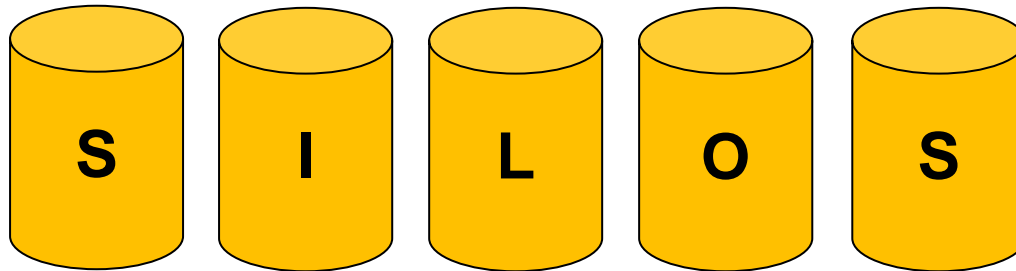
- Governance
- Strategy and Business Performance Management
- Risk Management
- Compliance
- Internal Control
- Corporate Security
- Legal
- Information Technology
- Business Ethics
- Sustainability and Corporate Social Responsibility
- Quality Management
- Human Capital and Culture
- Audit and Assurance
- Finance

Source: OCEG Red Book

A grim view of the current state...



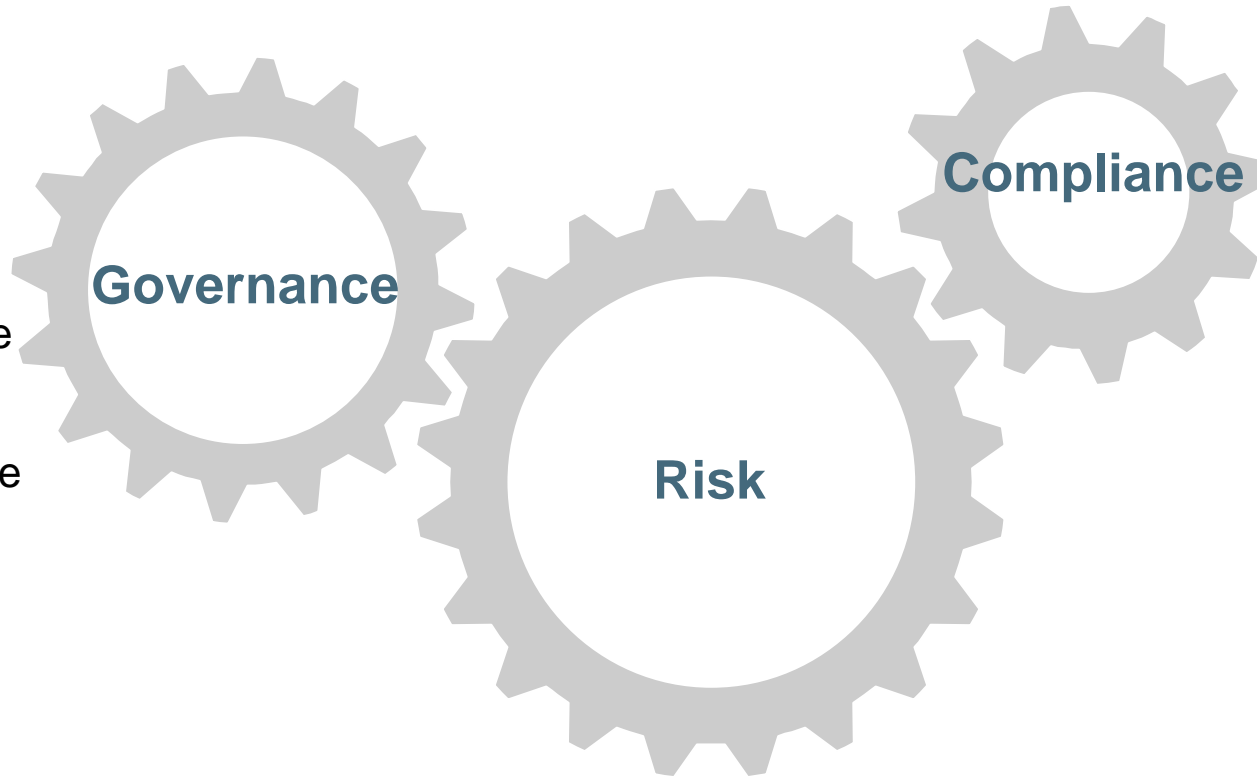
Eliminate Silos



Governance, Risk, and Compliance - In Harmony



The culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.



Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

The effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organization to recognize opportunities while managing negative events.

Fragmentation



Incomplete global risk profile



“

- A prickly tangle of controls and practices..
- buried inside functional or geographic silos with hundreds – or even thousands – of isolated activities.
- Bewildering complexity and duplication, even as it leaves major gaps uncovered and fails to deliver the desired results.

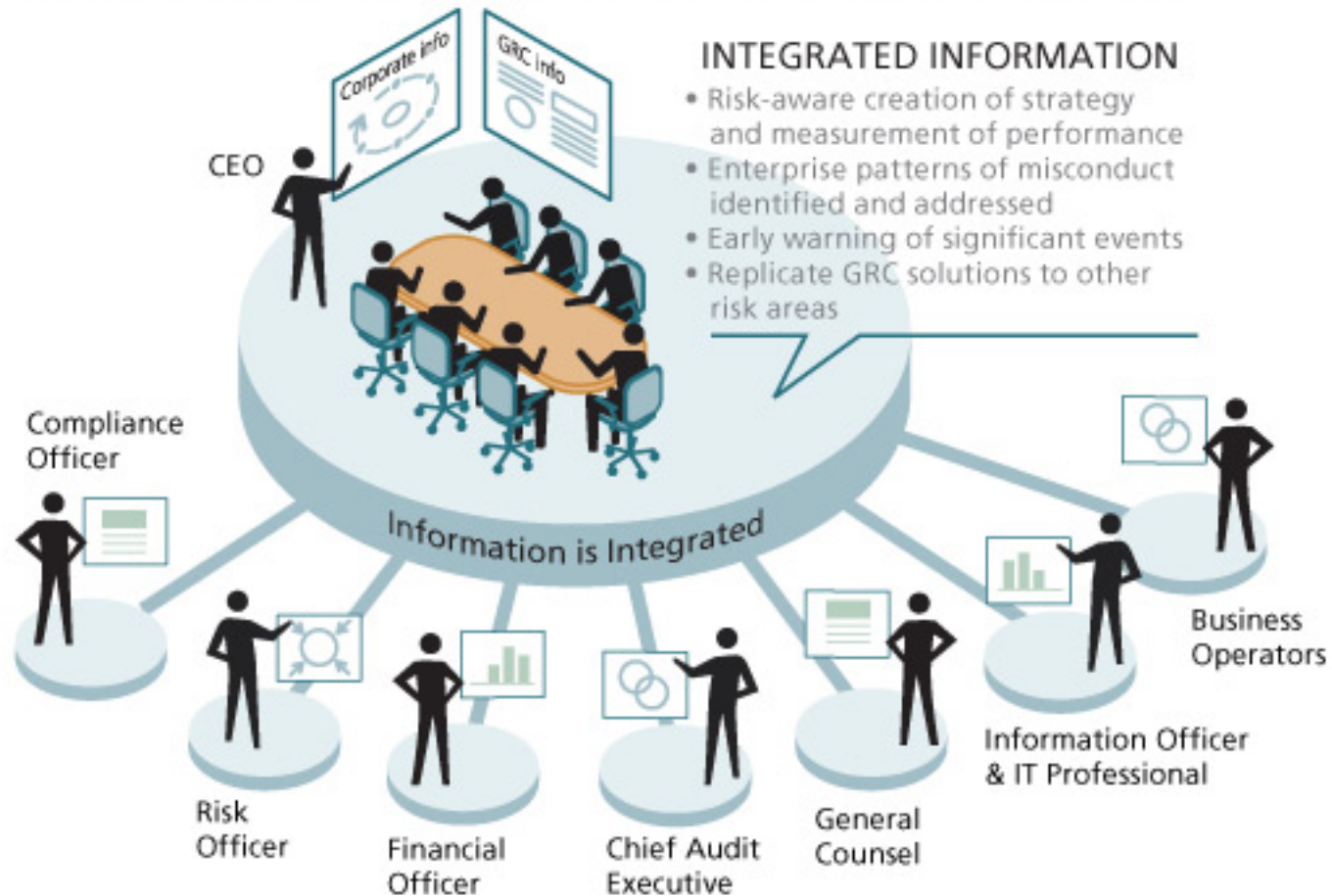
- Deloitte & Touche

The more efficient model is where everybody involved works together, in harmony

- Share best practices
- Use common tools
- Rely on each others work
- Single source of truth

The model does not require single ownership, only cooperation and coordination

Consistent flow of trusted, consistent information



“

..a federation of professional roles – the corporate secretary, legal, risk, audit, compliance, IT, ethics, finance, line of business, and others – **working together in a common framework, collaboration, and architecture** to achieve sustainability, consistency, efficiency, and transparency across the organization.

- Michael Rasmussen, Corporate Integrity

- Technology can enable improvements in GRC processes
- Technology can be the hammer for convergence
- Increasing functionality for each process, such as risk management
- Increasing integration, between GRC functions and with ERP
- Multiple platforms can be addressed through BI
- “A fool with a tool is still a fool”
- Moving to effective GRC processes requires a commitment from executives
- Optimize overall IT environment, not just GRC technology

- GRC is how you run the organization to optimize results, by managing risks and seizing opportunities, while staying in compliance
- GRC is not about technology, it is about the business
- It is a way of looking at how you run the business, pointing out the issues around:
 - Fragmentation and the need for convergence
 - The need to connect strategy and risk, performance, controls, budget, etc
- Optimize your GRC process and solve your business problems. Don't focus on a "GRC solution"

Focus on the Business Problems: Strategy to Execution Issues



- Unreliable or untimely information
- Cascading of strategy throughout organization
- Accountability for execution
- Link budgeting and strategy
- Link strategy and performance
- Link between strategy and risks
- Link company goals, incentive systems to strategy
- Risk and performance culture
- Risk oversight
- Enterprise-wide risk management

- Focus on solving business problems, not on a “GRC” solution
- Do you have weaknesses in Strategy to Execution?
- What elements require improvement?
 - Strategy?
 - Performance management?
 - Information?
 - Risk management?
 - Compliance management?
- Pay attention to “harmony” and “fragmentation”
- These might be GRC issues, but where is a single GRC solution?

Questions – need more information?



How to contact me

Norman Marks

SAP

Palo Alto, California

norman.marks@sap.com

<http://www.theiia.org/blogs/marks/>

<http://normanmarks.wordpress.com/>

Twitter: normanmarks