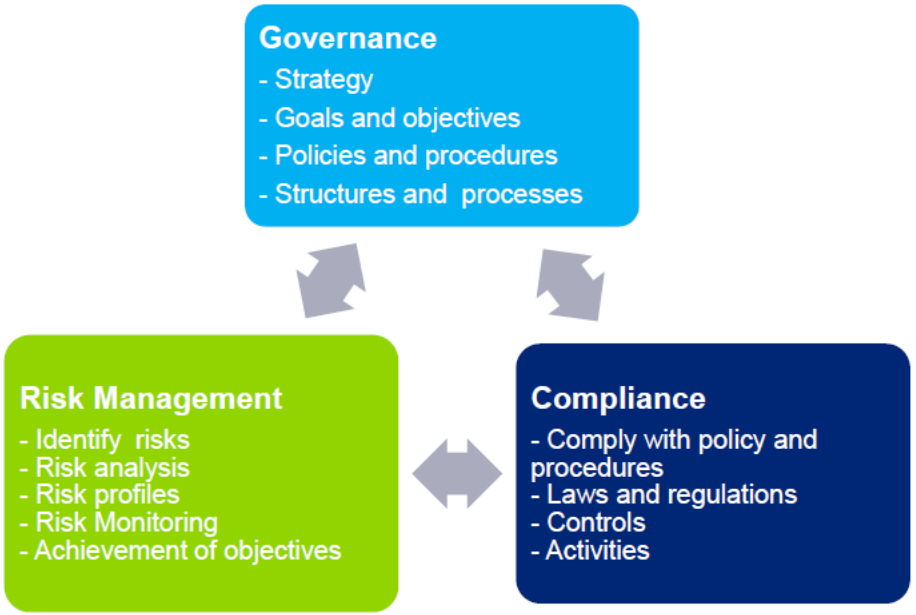
Dr. Yeffry Handoko Putra, S.T, M.T

Integrating Governance, Risk Management and Compliance

Magister Sistem Informasi
UNIKOM

What is GRC

GRC is a management model that promotes the criteria unification, as well as communication and collaboration between different stakeholders in the management and control of the organisation



Governance:

- Manages the ***risks to*** the execution of the company strategy as well as the ***risks from*** the chosen strategy

Risk management:

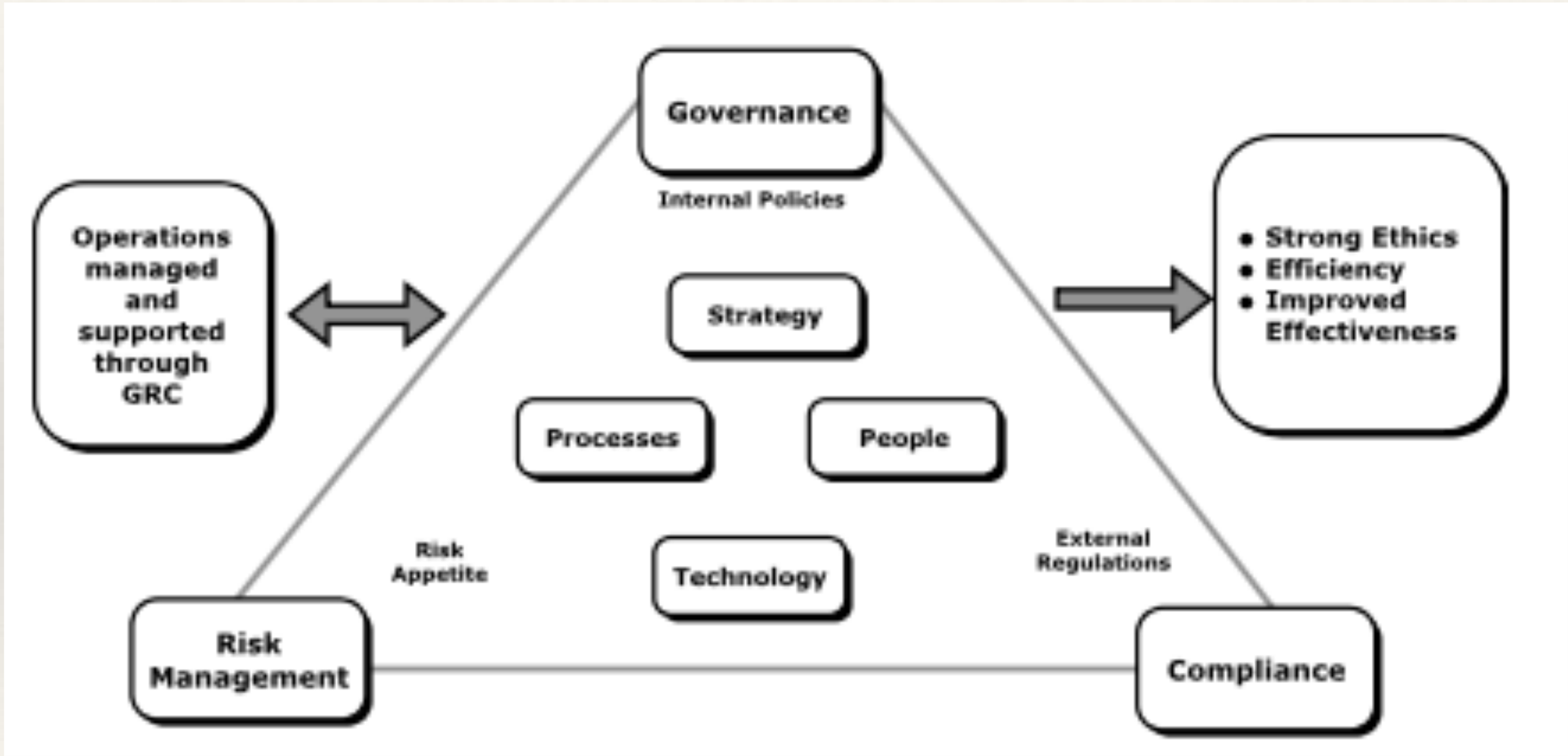
- Determines the areas exposed to potential risks

Compliance:

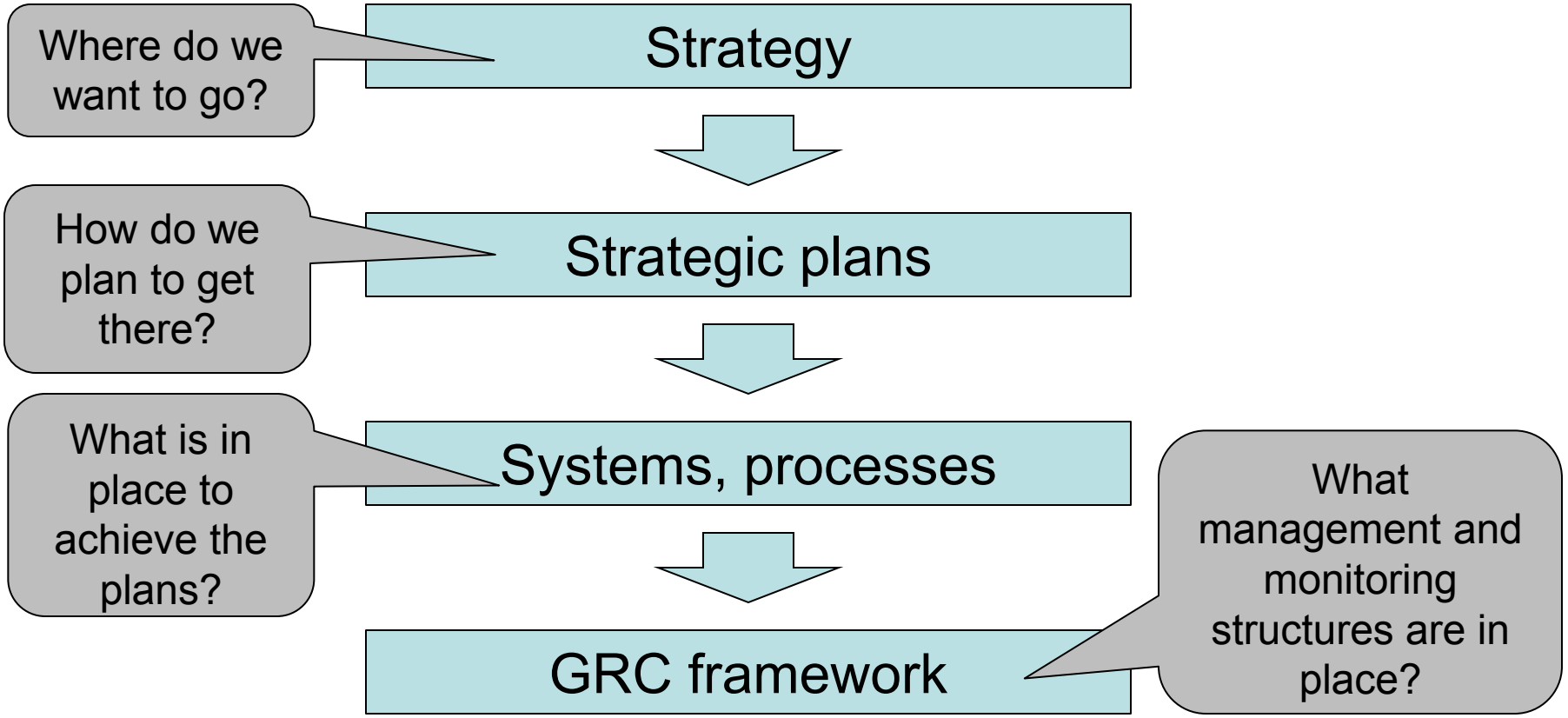
- Is the tactical action to mitigate risk

Source: Deloitte – May 2013

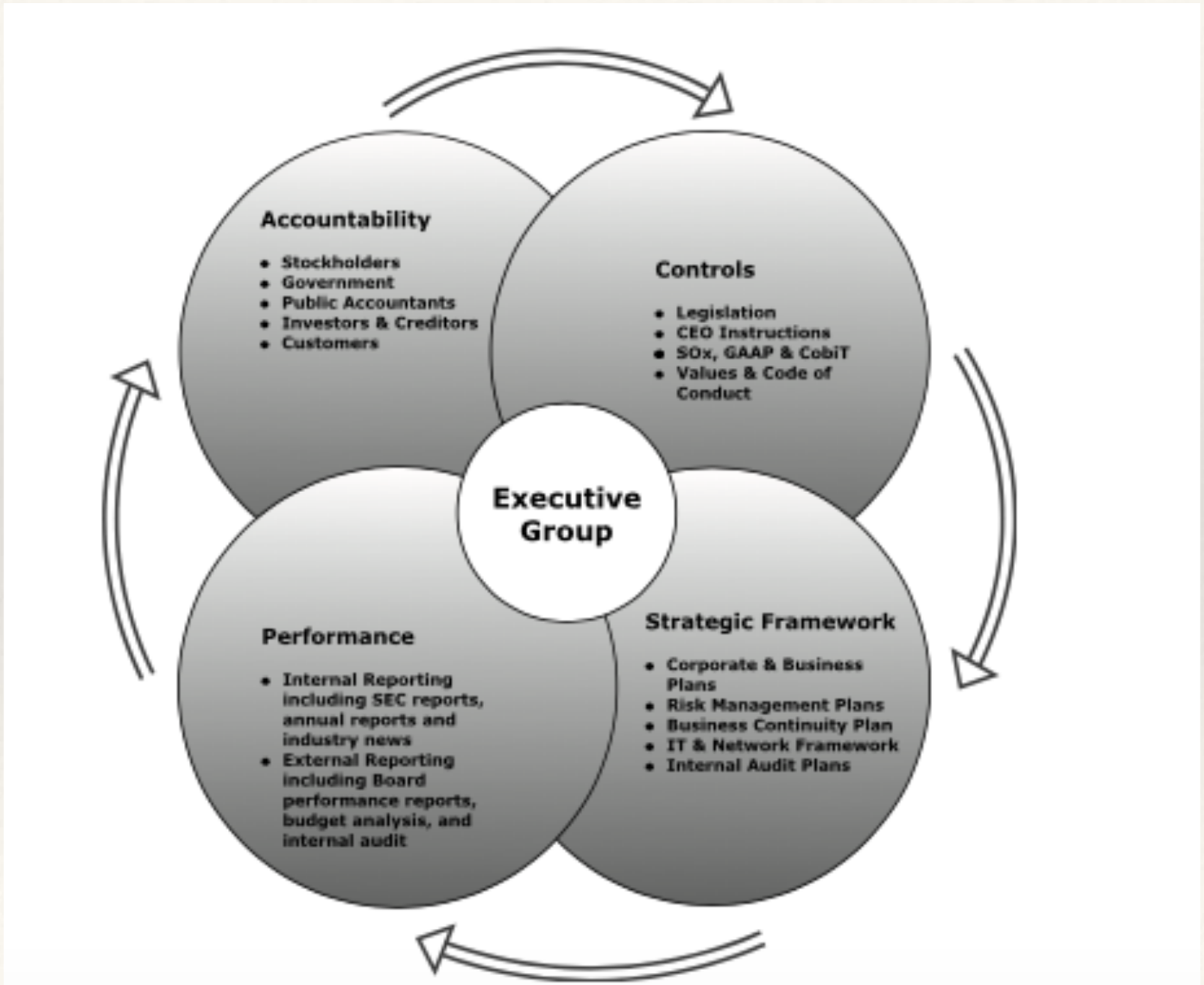
GRC Concept


Operations managed and supported through GRC
Governance
Internal Policies
Strategy
Processes
People
Technology
Risk Appetite
External Regulations
Risk Management
Compliance
• Strong Ethics
• Efficiency
• Improved Effectiveness

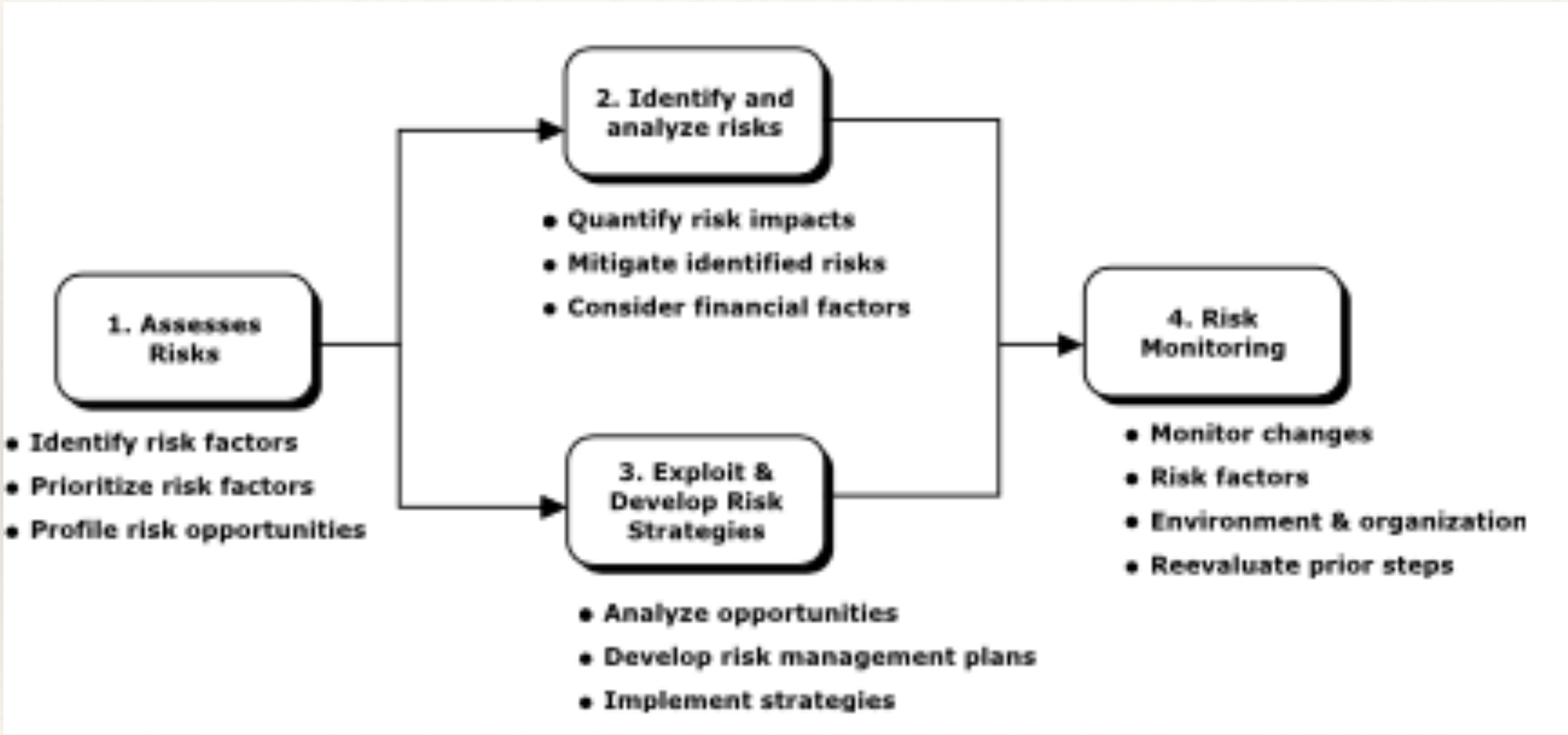
Strategic link



GRC Governance Concept

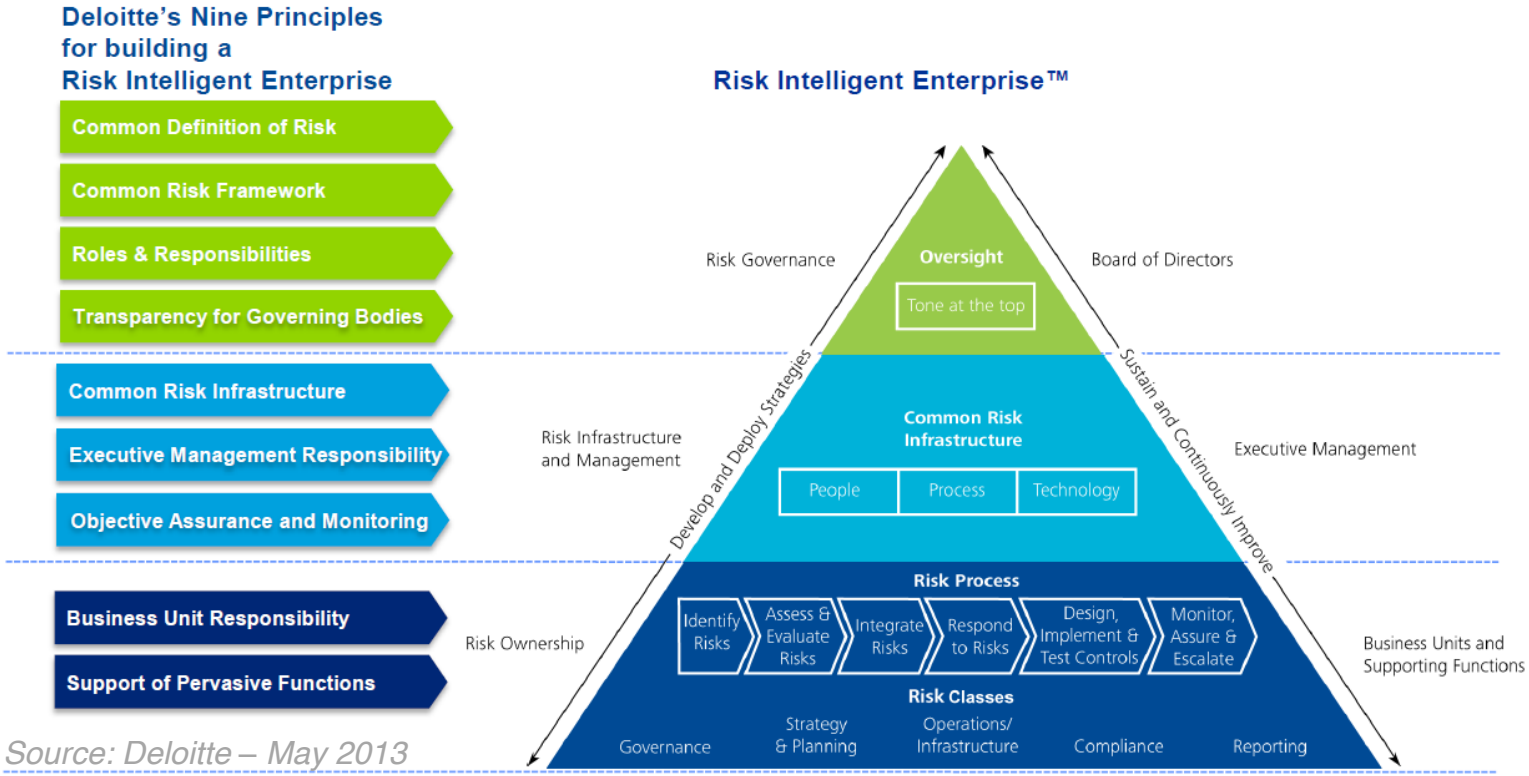


GRC Risk Management Process



Risk and GRC

A GRC approach focuses on maintaining the right balance between risk and reward. An effective risk management program focuses simultaneously on value protection and value creation. Deloitte refer to an organisation that has attained an advanced state of risk management capability as a “Risk Intelligent Enterprise™”



Source: Deloitte – May 2013

What is Scope of Compliance

Scope of Compliance	Area for Considerations
Strategy	■ As an organization develops its strategy, it must determine which regulations are relevant. ■ Compliance sustainability needs to be an integral part of any compliance strategy.
Organization	■ The organizational structure must be established to meet the specific requirements (or intent) of each regulation (e.g., Sarbanes-Oxley recommends the Chief Executive Officer and President be two different people).
Processes	■ Key processes must be documented and practiced. ■ Audits or reviews must take place to ensure documented processes are effectively being used to address compliance/regulation requirements.
Applications and data	■ Applications must be designed, implemented and continuously tested to support the requirements of each regulation. ■ Data must be properly protected and handled according to each regulation.
Facilities	■ Facilities must be designed and available to meet the needs of each regulation (i.e., some regulations may require records to be readily available at an off-site location).

GRC stakeholders

Board and support committees

- Clear dissemination and consistent strategy, culture, policies and objectives
- Fast decision making and informed

Management team

Visions and uniform approaches

- Roles and responsibilities defined
- Ethics Program disseminated and applied uniformly

Relationship with regulators

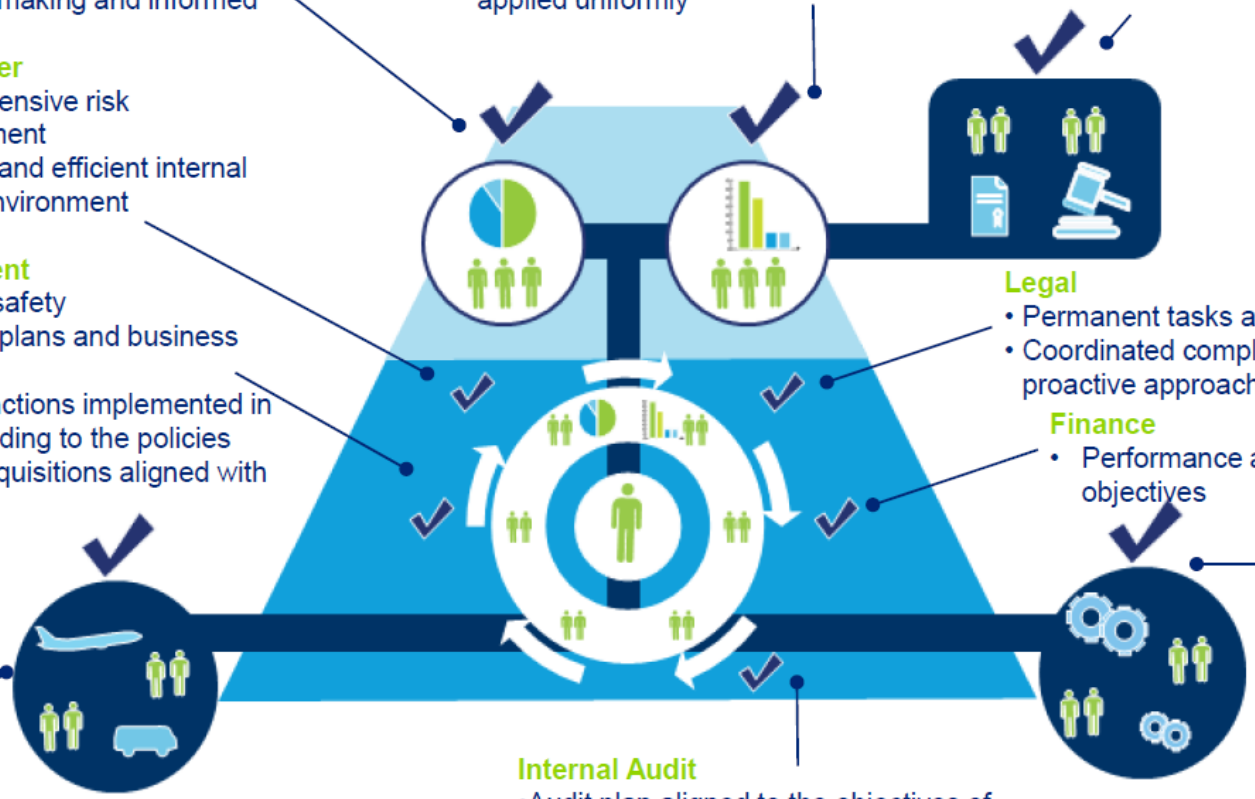
- Constant communication and collaboration "No surprises"

Comptroller

- Comprehensive risk management
- Effective and efficient internal control environment

Systems department

- Optimum level of safety
- Disaster recovery plans and business continuity plans
- Segregation of functions implemented in the systems according to the policies
- IT projects and acquisitions aligned with business strategy



Legal

- Permanent tasks and coordinated
- Coordinated compliance efforts With a proactive approach

Finance

- Performance aligned to business objectives

Customer Relationship

- Clear vision of market trends and needs

Relations with suppliers

Scheduled and timely delivery

Internal Audit

- Audit plan aligned to the objectives of the organization
- Efficient audit programs

Source: Deloitte – May 2013

The value of GRC

GRC promote the criteria unification, the effort coordination and collaboration between different characters involved in the direction of the organisation through:

- The integration of the organs / government officials, administration and risk management, internal control and compliance
- Role and responsibility assignation to key personnel
- Communication channels formalisation
- Applying a risk-based approach
- The implementation of a compliance program

GRC

Why are organisations seeking a better approach to GRC:

- Uncertainty due to economic instability
- Concern about the risk environment – greater focus on effectiveness and adequacy of internal controls
- Rise in complexity and regulation
- Business performance
- Sustainability
- Stakeholder demands
- Integrated approach supports decision making

Source: Institute of Chartered Accountants in Australia / KPMG – 2012

GRC

Convergence of GRC is evolving:

- Response to market uncertainty and complexity
- Not about a technology tool
- Different way of thinking
- Drive maximum value from complementary activities
- Information to drive performance and achieve compliance
- Audit/ risk committees play pivotal role:
  - Key sponsors
  - Alignment to strategy
  - Integrated framework supports GRC requirements

Source: Institute of Chartered Accountants in Australia / KPMG – 2012

GRC

Integrating GRC:

- Strategic approach
- Improved alignment of GRC components
- Link GRC components to strategy
- Risk component critical
- Common language, methodology and approach to risk identification and assessment
- Risk appetite – helps focus GRC efforts and concentrate compliance and assurance activities

Source: Institute of Chartered Accountants in Australia / KPMG – 2012

GRC

Implementing a strategic approach to GRC:

- Consider the big picture first
- Form a cross-functional team / committee
- Define roles and responsibilities early in the process
- Beware of building another silo
- Get the process worked out before investing in the technology
- Seek out overlaps and build efficiencies
- Create a common language and understanding around risk
- Don’t lose the detail in the convergence process
- Remember that GRC is a gradual process

Source: Institute of Chartered Accountants in Australia / KPMG – 2012

Any Questions?