Risk Based Approach

Practice in financial institutions

ADVISORY / FINANCIAL SERVICES

Prof. Dr. Peter A.M. Diekman RA
Aruba, 15 November 2010

AUDIT ▪ TAX ▪ ADVISORY

Content

Risk Management Models

Governance Risk & Compliance

Content

Risk Management Models

Governance Risk & Compliance

Risk Management Models

COSO II - ERM Framework

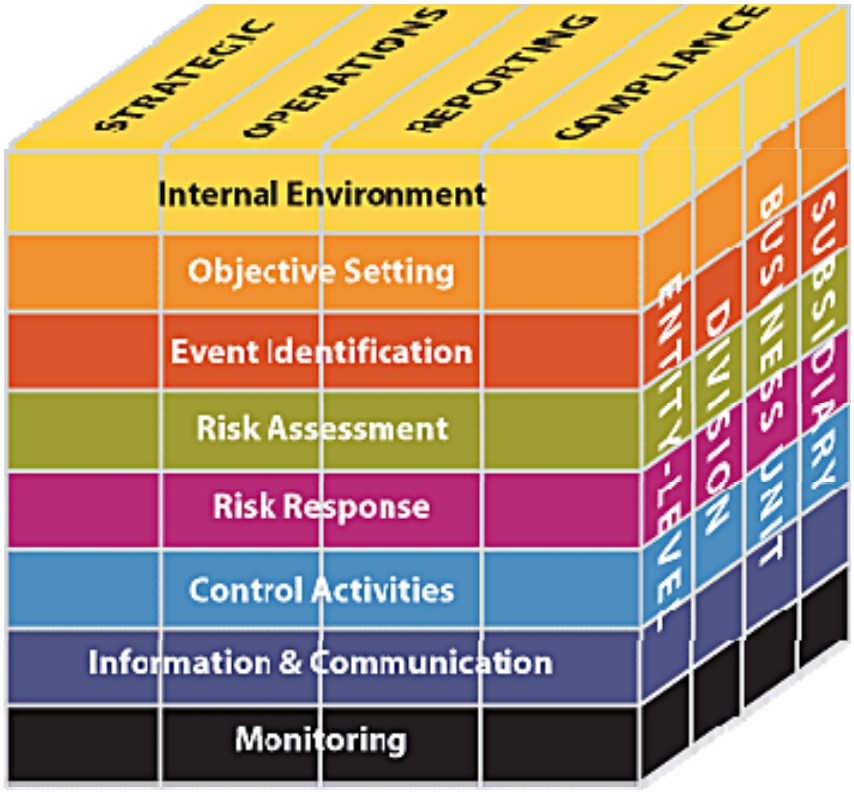
ISO 31000

Lines of Defence

Risk Management Models – What is risk?

- **KPMG**
  - Risk relates to strongly adverse outcomes of uncertain (commercial) processes.
- **The Shorter Oxford Dictionary defines risk as:**
  - Hazard, danger, exposure to mischance or peril
  - The chance of hazard or commercial loss, specifically in the case of insured property or goods
- **Mathematician Bernoulli (1738):**
  - A risk is a random variable
- **Diekman**
  - Risk is an uncertain event causing non achievement of objectives set by an organisation

Risk Management Models - COSO



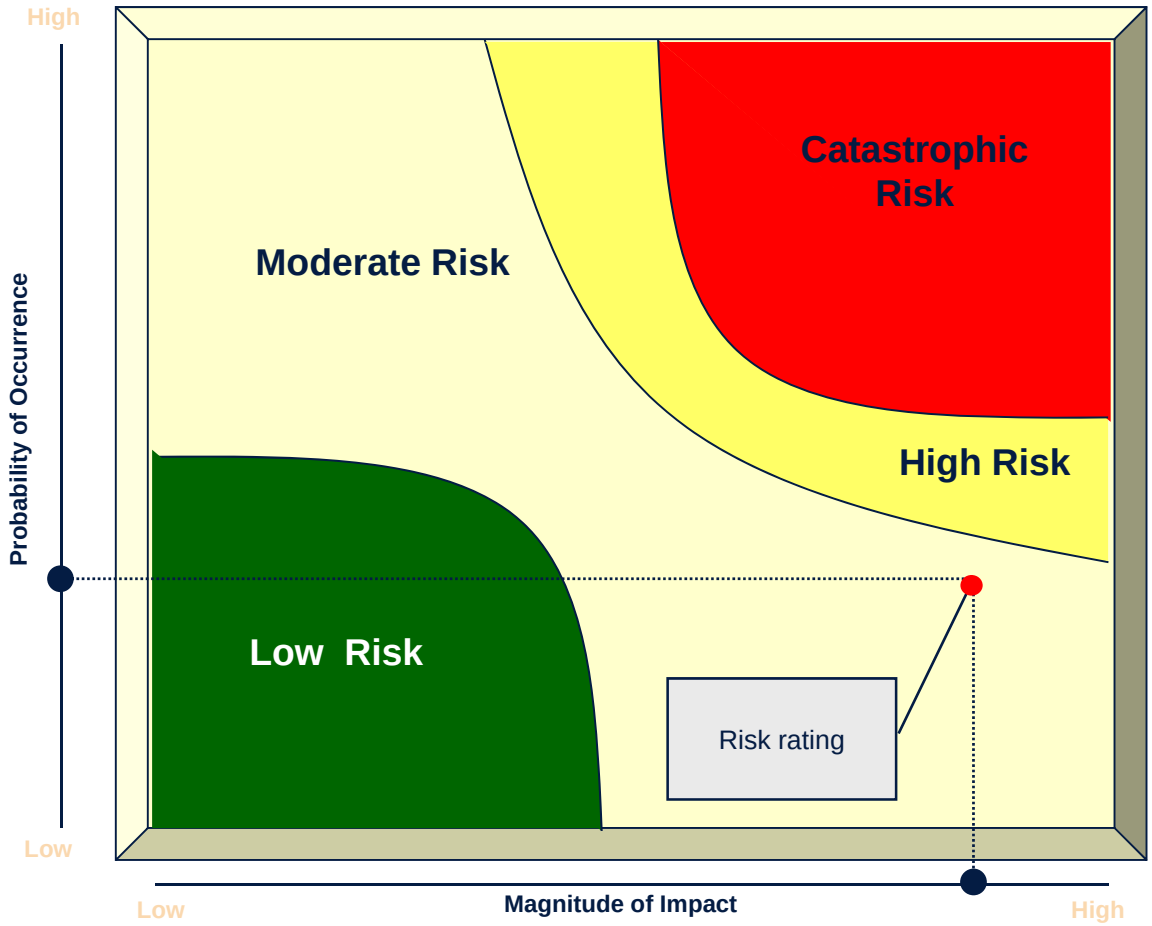
Enterprise Risk Management

"ERM is expected to become widely accepted by companies and other organisations and all stakeholders and interested parties"

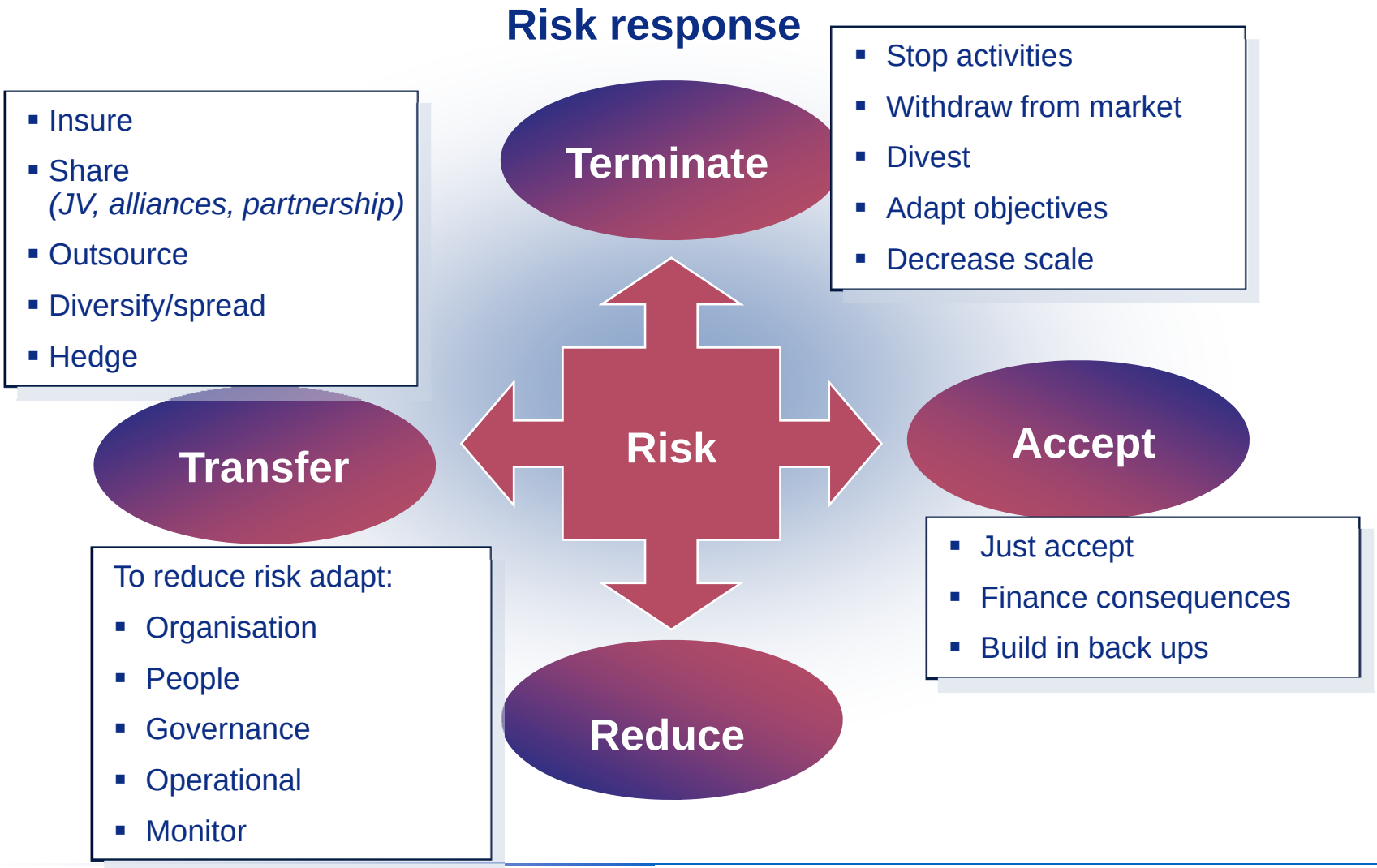
COSO – Committee of Sponsoring Organizations of the Treadway Commission (September 2004)

Risk Management Models - COSO

- Risk Analysis
  - Risk is a combination of the probability of an event and its consequence
  - An event is the occurrence of a particular set of circumstances (e.g. market developments, acts of institutions or individuals, functioning of technical systems)
  - A consequence may be positive or negative and may be expressed qualitatively or quantitatively



Risk Management Models - COSO



ISO 31000

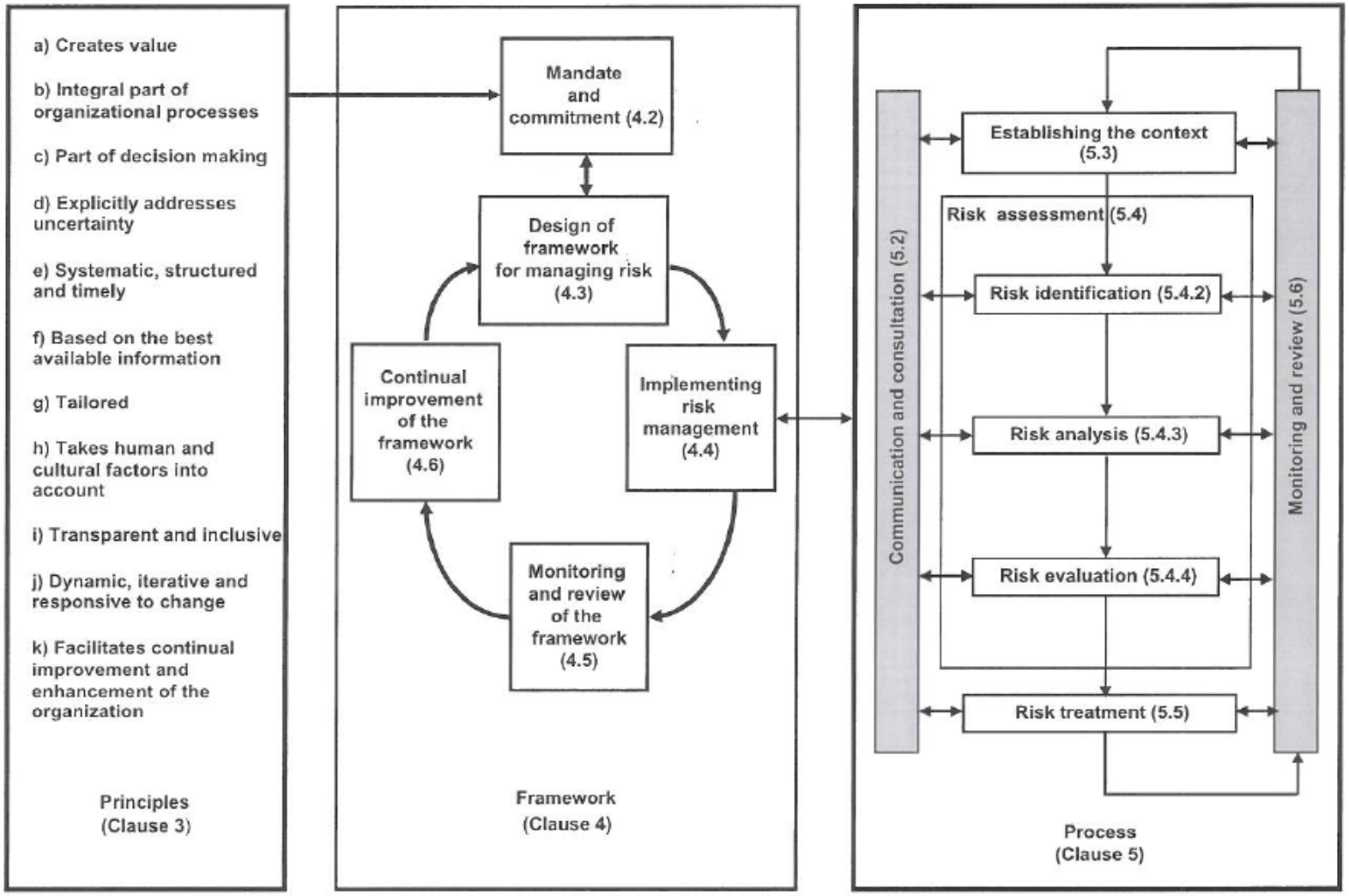
- New (*December 2009*) ISO Standard aimed at managing risk in a structured way
- Applicable on all kind of organisations
- ISO 31000 - a systematic and logical approach to Risk Management

Systematic and logical approach

- Communication and consultation during the process
- Establishing an infrastructure for
  - Identification
  - Analysis
  - Evaluation
  - Treatment

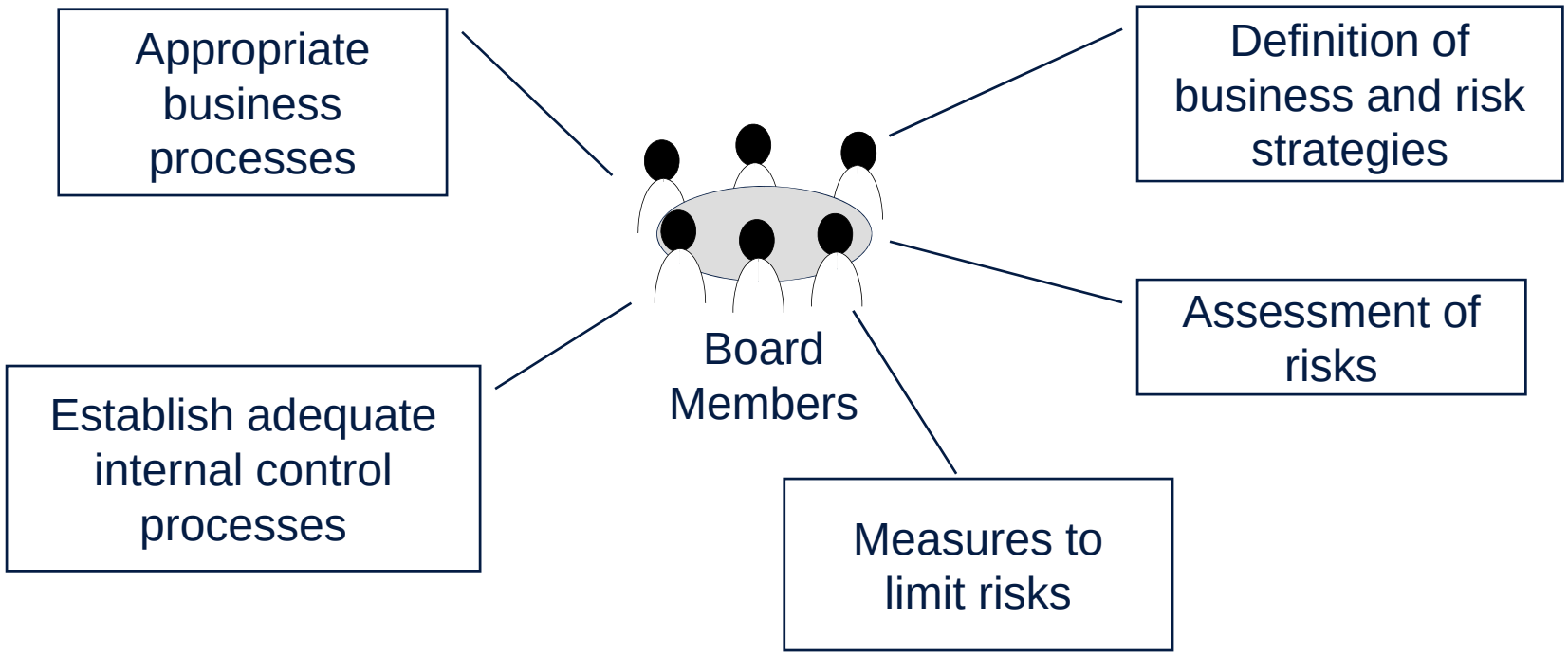
  } of risk
- Focused monitoring and review of risk
- Recording and reporting of risk

ISO 31000



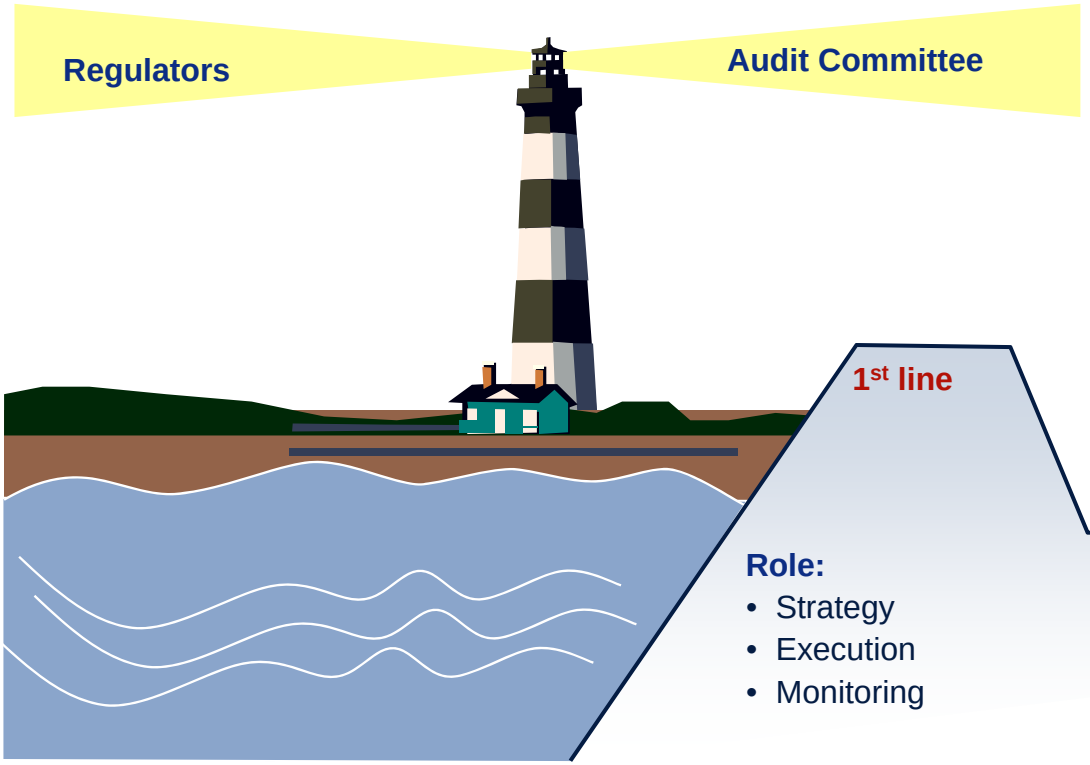
Risk Management

Overall Responsibility of the Board of Management



The responsibility for the determination of strategies cannot be delegated!

Lines of Defence



Stakeholders

1st line

Role:
- Strategy
- Execution
- Monitoring

Executive Board

Senior Management

2nd line

Role:
- Oversight and support
- Preparing standard setting (Legal, Compliance, Risk, Finance, HR)

Senior Management

In charge of control functions

3rd line

Role:
- (Internal) Audit
- Provide assurance to executive mgt and audit committee

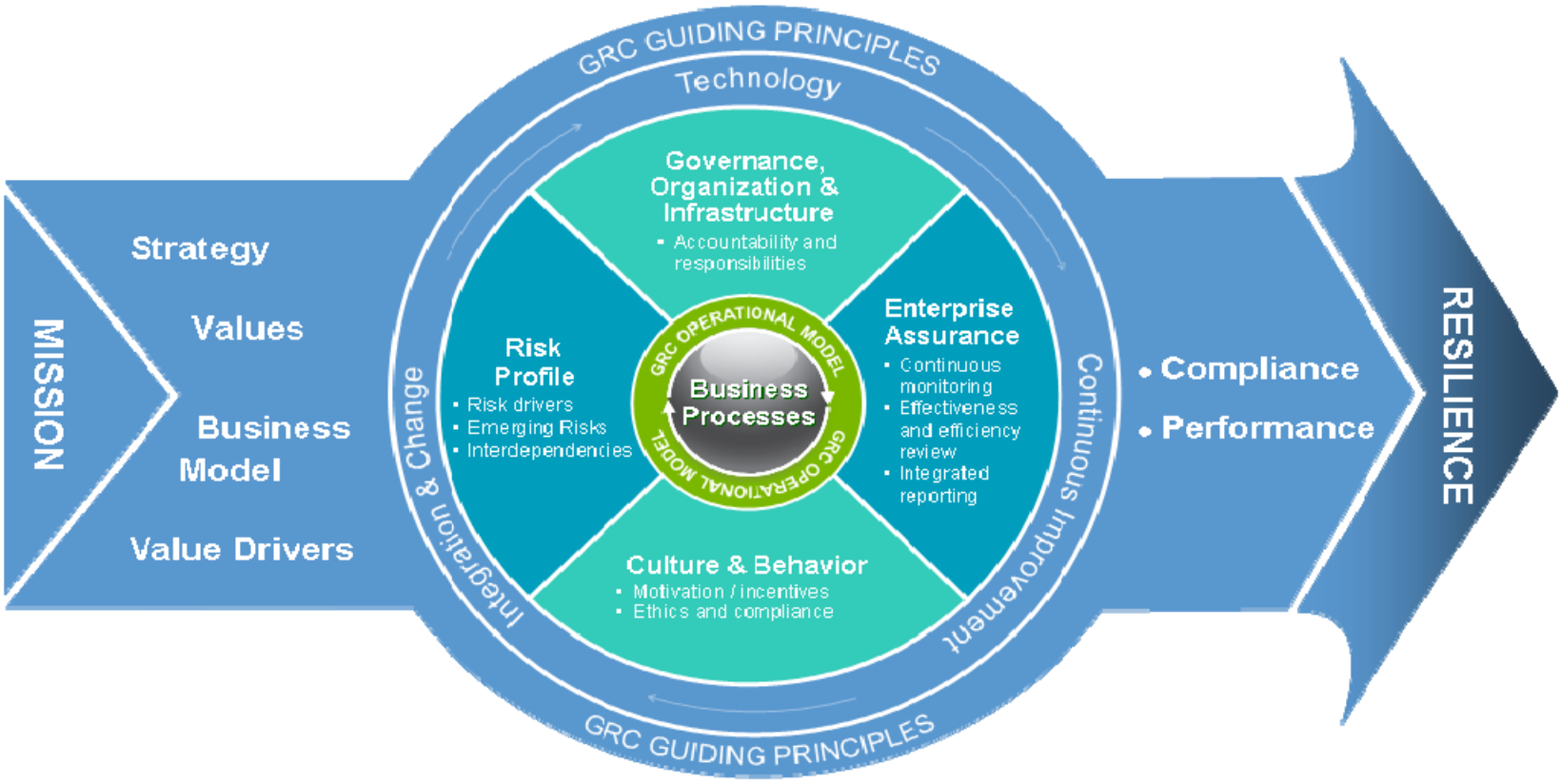
(Internal) Audit

Content

Risk Management Models

Governance Risk & Compliance

GRC – A Holistic Model



Business Performance

GRC Measures

Integrated Reporting, Performance and Compliance

KEY OBJECTIVES

Compelling reasons to drive towards an integrated GRC approach

- **Proven tools and methodologies are available**
- **Major internal obstacles to overcome**
- **Early benefits are easy to realise**

DISCUSSION OUTLINE

- What is governance, risk and compliance (GRC)
- Driving forces for change
- Barriers to implementation
- What we are seeing in the market
- Benefits – tactical and strategic
- Conclusions

GOVERNANCE, RISK AND COMPLIANCE (GRC)

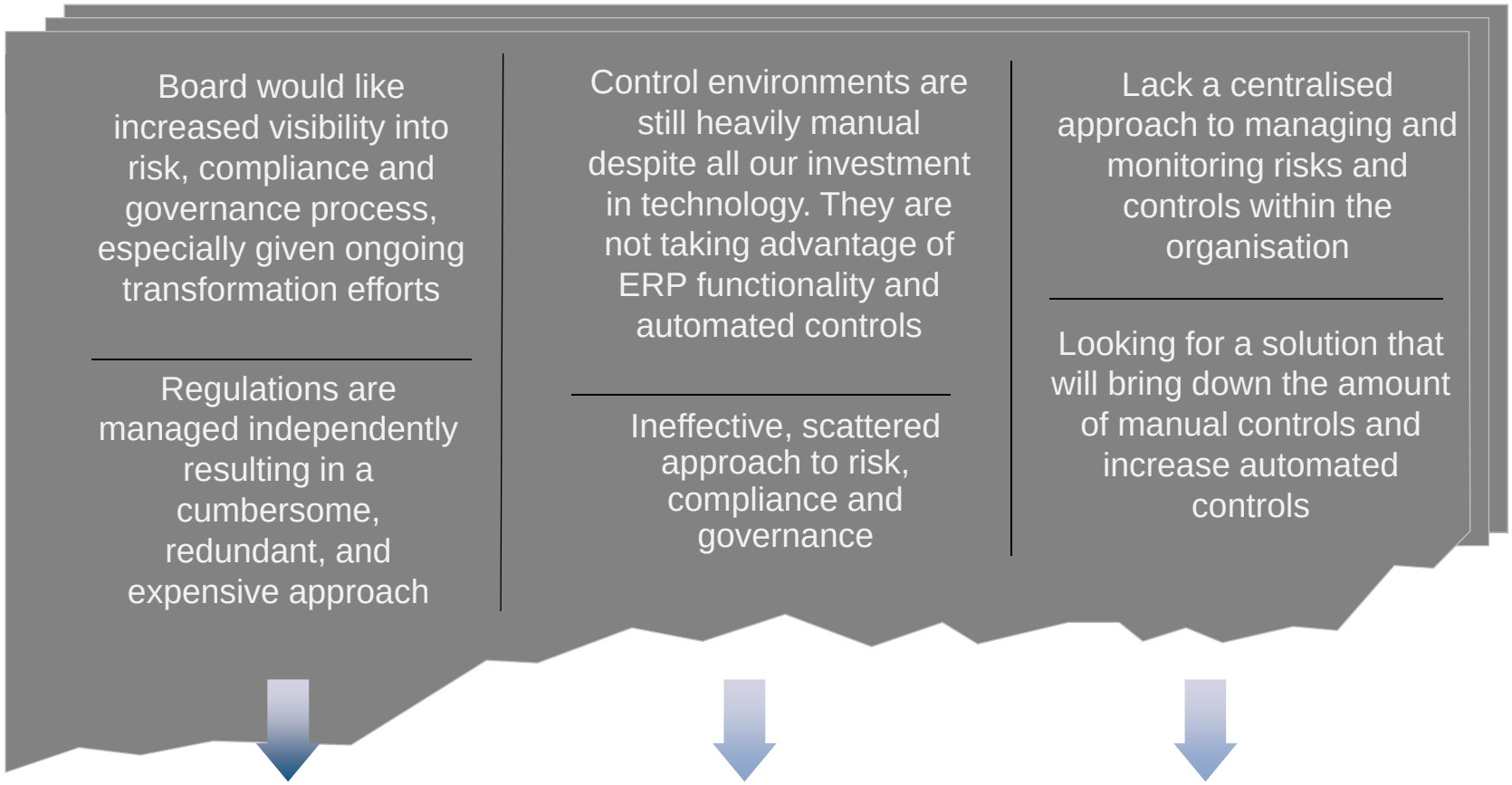
What it is

- Starts with understanding strategic objectives, mission, business value and business model
- Comprehensive view of the oversight functions
- Converging risk related information from various oversight functions
- Encompasses people, processes and technology considerations

What it is NOT

- Not just a technology solution, but frequently involves technology enablement
- Not just another name for enterprise risk management
- Does not eliminate the need for or consolidate existing functions (e.g., compliance, audit, SOX)
- Not just conceptual – Must be practical

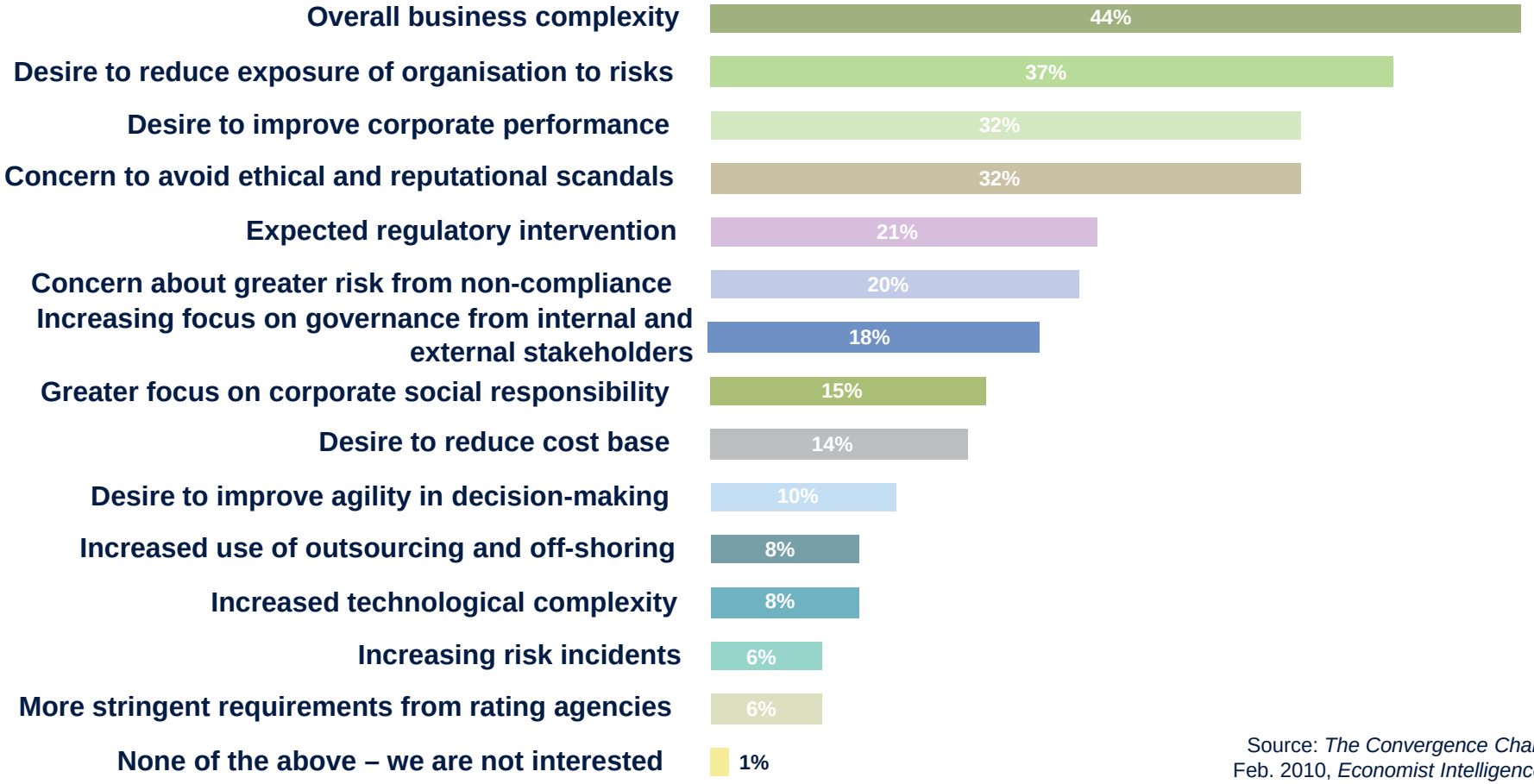
DRIVING FORCES - WHAT CLIENTS ARE SAYING



Rationalise information to drive business results

DRIVING FORCES - CHANGING LANDSCAPE

What is influencing your organisation's interest in GRC?



Source: *The Convergence Challenge* Feb. 2010, *Economist Intelligence Unit*

DRIVING FORCES - DUPLICATION AND REDUNDANCY

73% of companies have seven or more separate risk functions

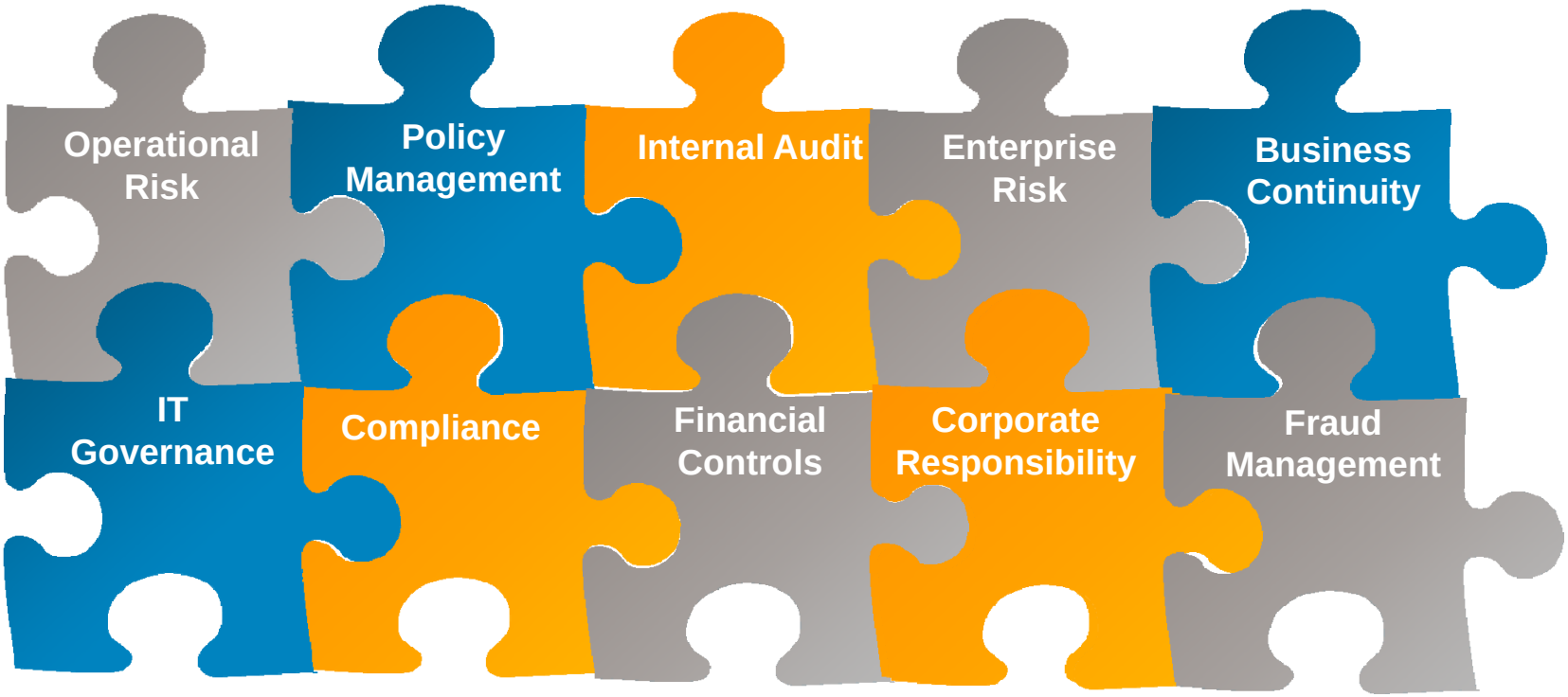
67% reported that they have overlapping risk coverage with two or more risk functions

50% of companies reported gaps in their coverage between risk functions

62% of companies believe they can get more risk coverage for less spend

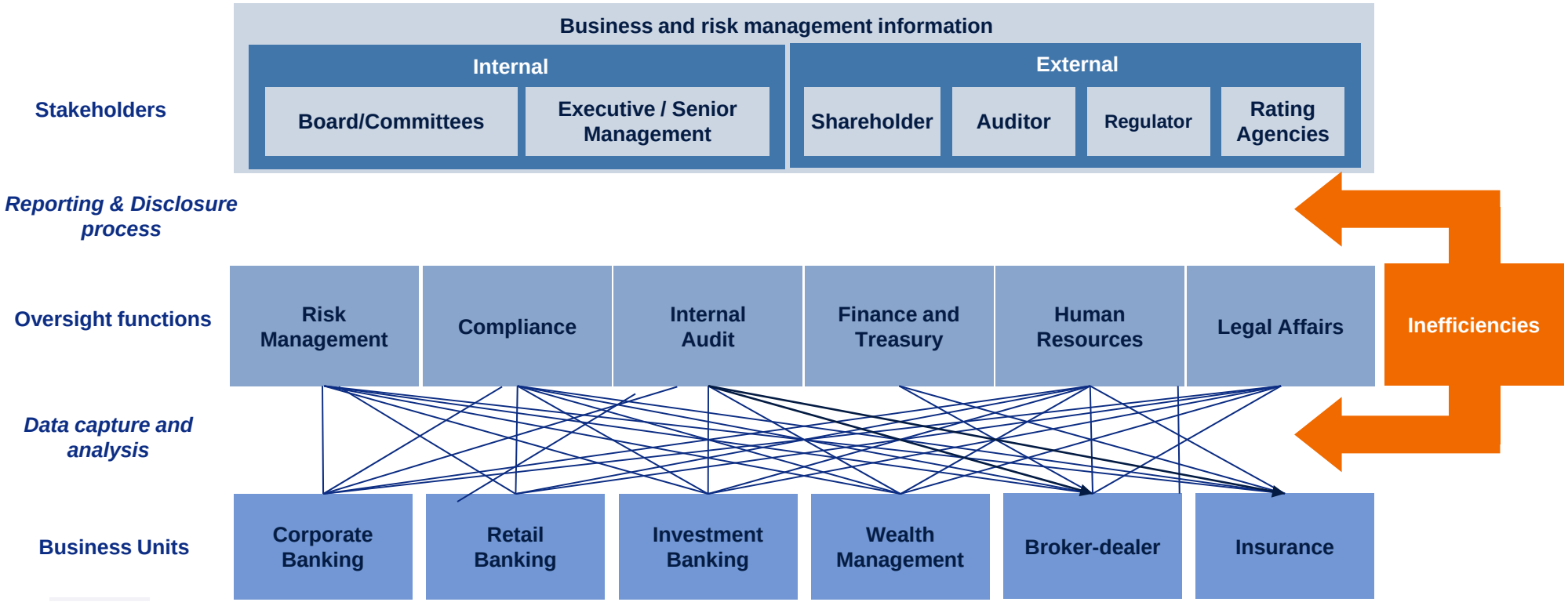
Source: *The future of risk, protecting and enabling performance Economist Intelligence Unit,* 2009

DRIVING FORCES - FRAGMENTATION PUZZLE



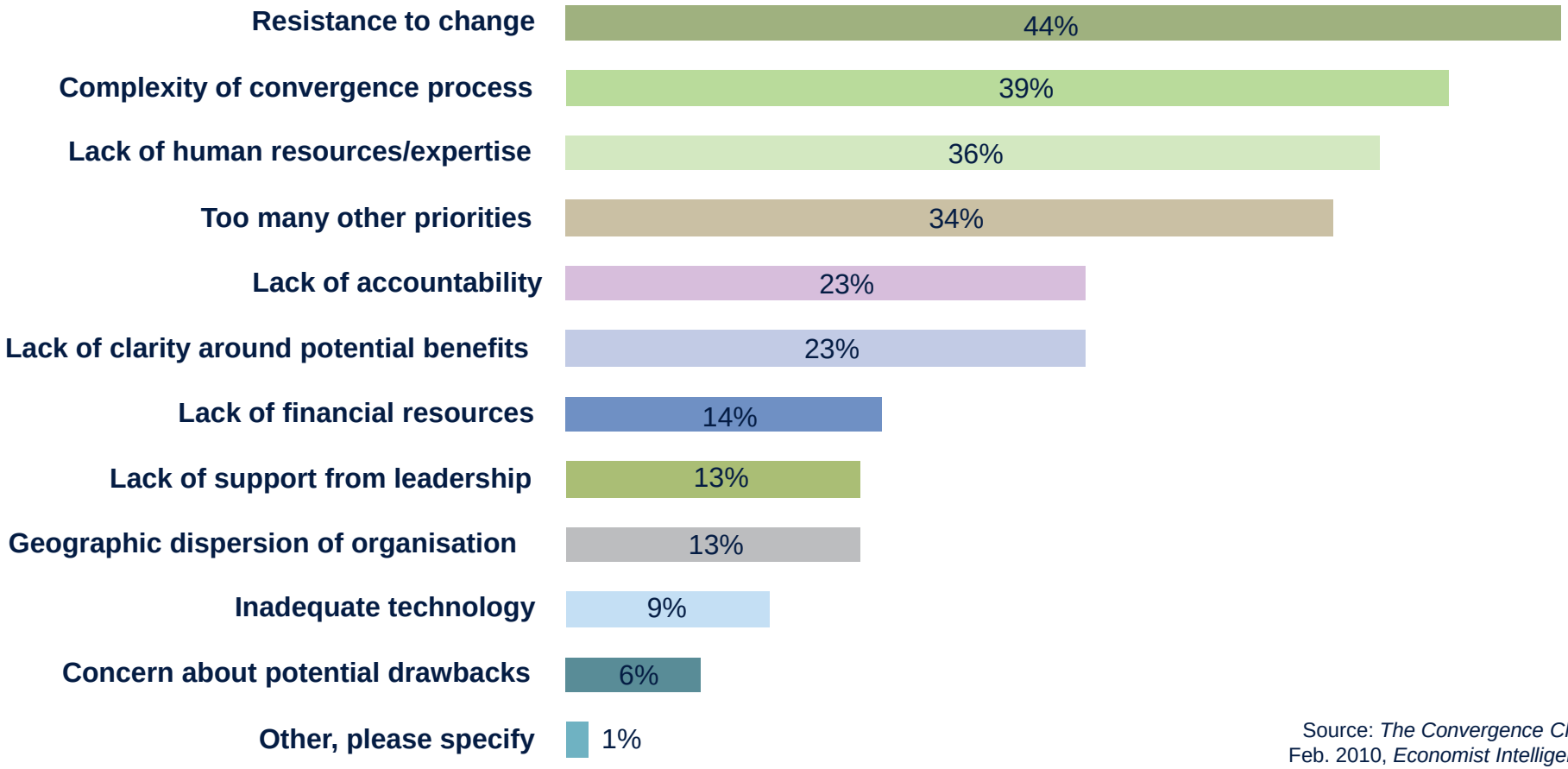
Increasing (legal) requirements result in increasingly complex financial sector structures

- Business and risk management processes have multiples connections with the business and supporting departments
- Business is often asked to provide ad hoc information in different formats and different intervals
- Insufficient consistency and reliability between information derived from different silos in the organisation



BARRIERS TO ENTRY

Significant barriers to greater GRC acceptance

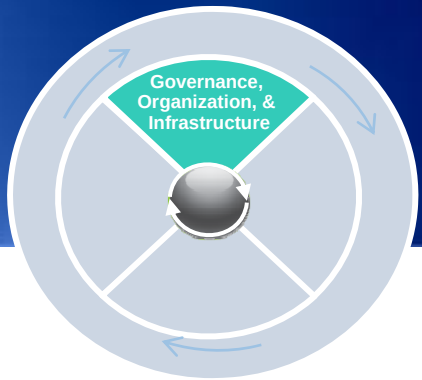


Source: *The Convergence Challenge* Feb. 2010, *Economist Intelligence Unit*

WHAT WE ARE SEEING IN THE MARKET
A GRC HOLISTIC MODEL

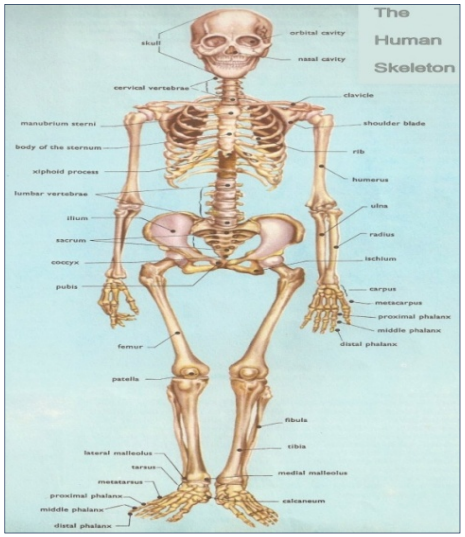
Source: KMPG LLP 2009
KPMG's GRC Holistic Model©

WHAT WE SEE IN THE MARKET
COMMON SHARED CONTEXT

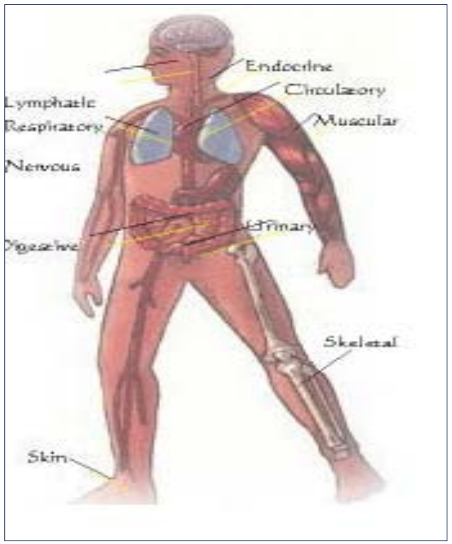


- **Setting the organisation structure and legal environment**
- **Knowledge is organised into contexts**
- **Specialists usually organise GRC in a similar way**

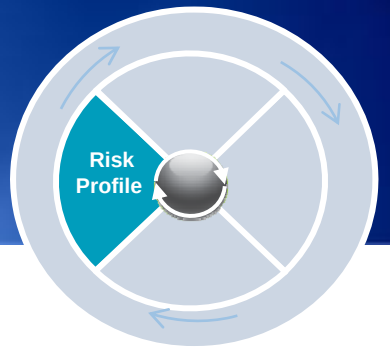
ORGANISATION STRUCTURE



PROCESS STRUCTURE



WHAT WE SEE IN THE MARKET
A COMMON GRAMMAR FOR RISK AND CONTROL



- Taxonomies for risk, control, and consequence

COSO CONTROL

Control Environment

Monitoring

Info and Communication

Risk Management

Control Activity

COSO RISK EVENTS

Economic

Natural Environment

Political

Infrastructure

Personnel

COSO OBJECTIVES

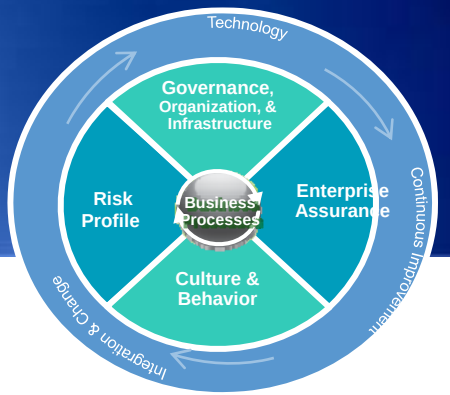
Strategic

Operational

Financial

Compliance

WHAT WE SEE IN THE MARKET
CALIBRATED APPROACH



1. Identify/ Assess Context

2. Assign Business Processes

2. Identify critical processes in high risk orgs/accounts. Identify KPI's.

7. Assess KPI/KRI Results

3. Assess Process Risks

3. Discover and rate process risks. Identify high risk issues. Identify KRI's for high risks.

7. If KPI's or KRI's are outside range, update risks, controls and issues to explain gaps.

4. Manage Process Risks

4. Identify and assess controls where high risks are mitigated. Create issues to remediate.

5. Identify Issues

5. Do issues explain process performance gaps? If not, reassess risks and controls.

6. Create Action Plans

8. Organisation/ Process Certification

8. Management certifies to conformance with methodology and reliability of information.

WHAT WE SEE IN THE MARKET
BEST PRACTICES

Change management requires an executive sponsor and individual champions

A phased in approach works best

- Start with 2-3 groups (e.g., audit, SOX ORM)
- Don't try to forcefully win over skeptics but keep them informed or involved

Plan for quick wins (e.g., common issue tracking or calibrated risk assessment)

Consider entity-wide reporting requirements vs. siloed

- Board and senior management requirement

Don't start with a technology solution

- Consider options throughout planning and scoping
- Enable processes with technology – keep it simple

Link to business performance

- Understand key performance indicators from a business perspective

Redefine GRC performance indicators and mission

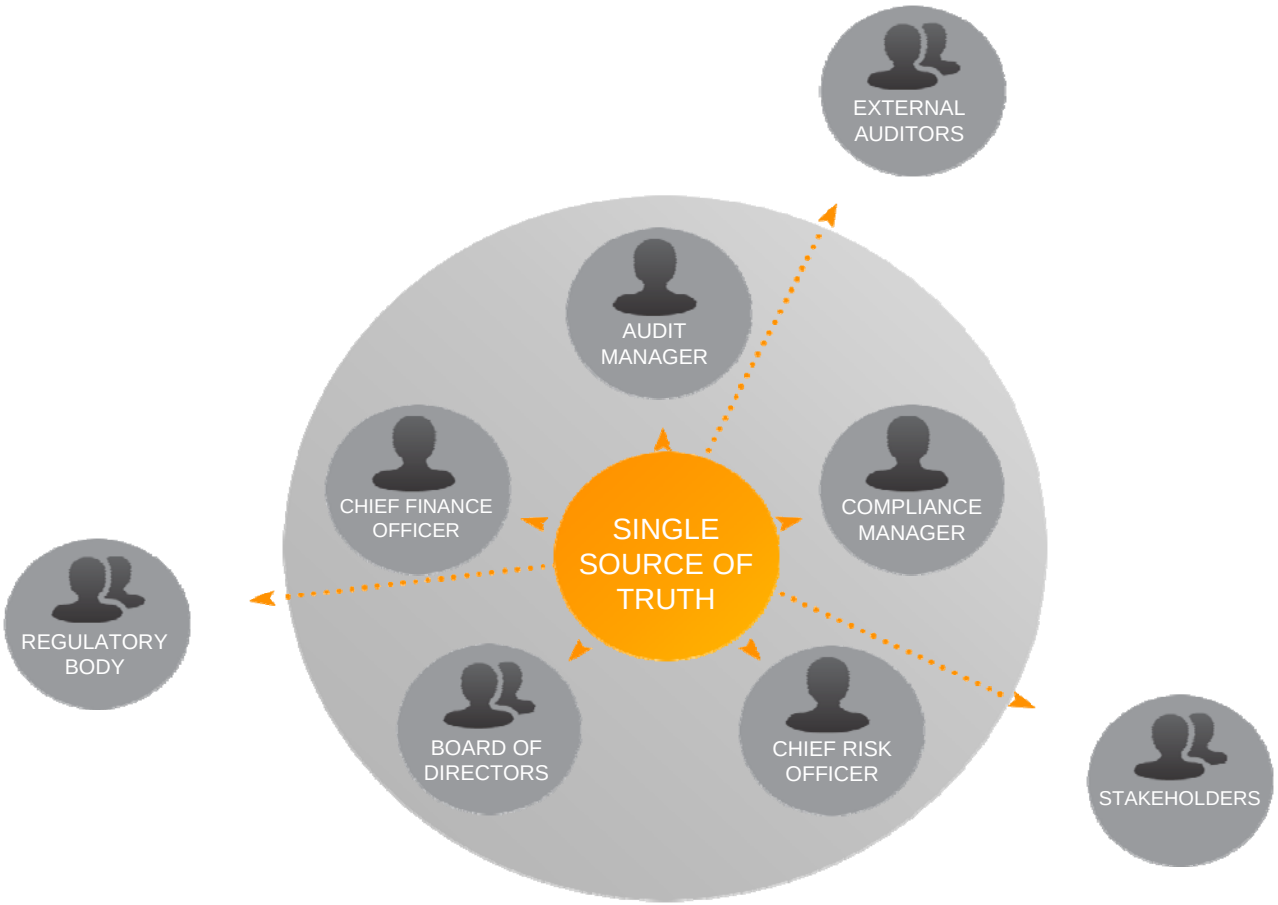
- Measure the creation of knowledge and quantify benefits from collaboration

BENEFITS
MEASURING TACTICAL SUCCESS

- All reporting from a single data source – no inconsistencies or reconciliations
- Common grammar of risk and control makes knowledge searchable
- Common calibrated methodology allows professionals to collaborate and rely on each others work
- Reduced footprint on business
- Control testing is efficient – one test for multiple needs
- Control design efficiency – reduce redundant controls, better link to risk

BENEFITS
MEASURING STRATEGIC SUCCESS

- Transparent
- Reliable
- Timely
- Relevant



KEY TAKEAWAYS

Compelling reasons to drive towards an integrated GRC approach

- Reducing complexities, leveraging results, reducing duplication / redundancy, and improved reporting

- **Proven tools and methodologies are available**
- Common risk and control models
- Standardised workflows showing integration opportunities
- Flexible and proven technologies (e.g., Paisley GRC)

- **Major internal obstacles to overcome**
- Reluctance to change
- Time and financial investment
- Multi-year initiative

- **Early benefits are easy to realize**
- Quick wins are available
- Longer term value

Prof. Dr. Peter Diekman RA

Partner
KPMG Risk & Compliance

Diekman.Peter@kpmg.nl
Tel +31 20 656 7958
Cell +31 651 52 7383