

# How to audit Corporate Governance

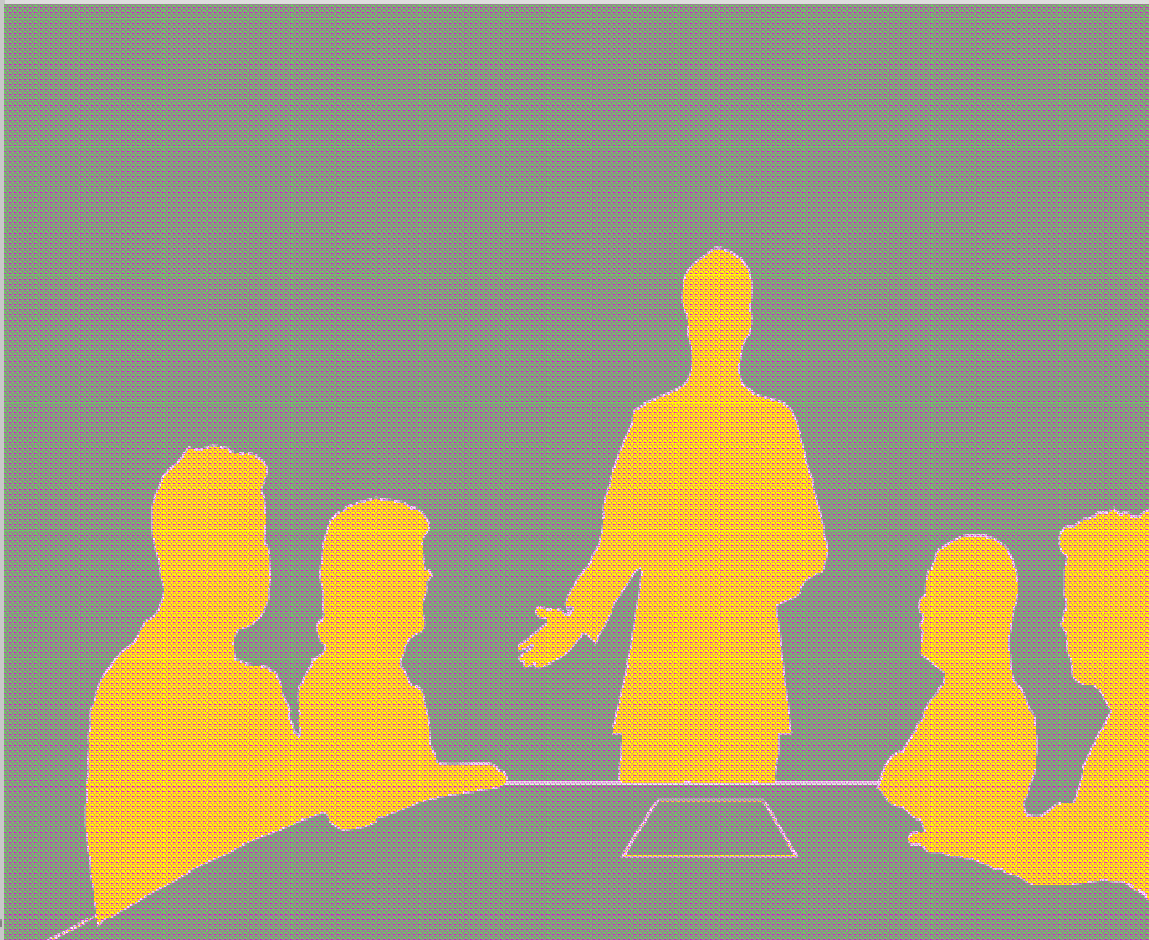


**Patrick Soenen**  
**20th Jan 2007**



- **Global Picture**  
**Why, What, When, Where, Who**
- **Evolution Regulatory Context**
- **Audit Universe**
- **Conducting CG Audit**
- **Knowledge**

# Corporate Governance Global Picture



**NEWS**

(13 December 2006 - Financial Times Deutschland)

**Former Siemens director Thomas Ganswindt detained**

Thomas Ganswindt, a former management board and central executive committee member of the German technologies group Siemens, is being held on remand, according to the Munich department of public prosecution.

....

According to a report in the daily *Süddeutsche Zeitung* newspaper, ... ex-Siemens manager Thomas Ganswindt knew of secret accounts outside Germany that were used to pay bribes for contracts.

Luc Blyaert, DataNews, **15 DECEMBER 2006**

Thomas Ganswindt, tot afgelopen zomer voorzitter van Siemens België, is door de politie opgepakt en blijft in de cel ....



Luc Blyaert, DataNews, **15 DÉCEMBRE 2006**

Thomas Ganswindt, jusqu'à l'été dernier président de Siemens Belgique et Luxembourg, a été arrêté par la police et emprisonné...

NEWS



**"Siemens has to be *cleaned up*. From top to bottom, we have to shed light on who knew about the affair and said nothing. And whoever did know about it has to go."**

**“Investors Concerned**

*Skies are hardly sunny for Siemens right now amidst a major corruption scandal.*

The news that top-level Siemens executives may have known about the slush funds has stockholders calling for big changes.“

"In the long term, this can have negative effects because the **firm's image** could suffer substantial damage. With future contracts, customers could ask themselves if they still want to work with Siemens."

**German engineering giant Siemens has said an **internal audit** had uncovered as much as 420 million euros in suspicious payments as part of the ongoing probe into an alleged bribery and embezzlement scandal.**

“The company is also set to tighten its **employee conduct guidelines**. "We have relentlessly to clarify and punish irregularities. Employees who violate our...regulations hurt Siemens in every respect,"

# Governance Threats

**Insider Trading**

**Self-Dealing**

**Conflict  
of interest**

**Misreporting**

**Theft**

**Fraud**

**Creative  
accounting**

**IT  
dysfunctions**

**Bribes**

...

# Governance Opportunities

**Good operating performance**

**Maximum shareholder value**

**Employee satisfaction**

**Customer Retention**

*Studies conducted by McKinsey & Cy showed that major investors and company owners are willing to pay an important premium for well governed companies.*

# Corporate Scandals



+ . . .

# External auditor



## *Analysis of European Business failures*

- **65** % : *no relation with the role of the audit process or the audit firm*
- **35** % : *role of the auditor or the audit firm was questioned*
- **0** % : *direct responsibility of the auditor*

# What ?

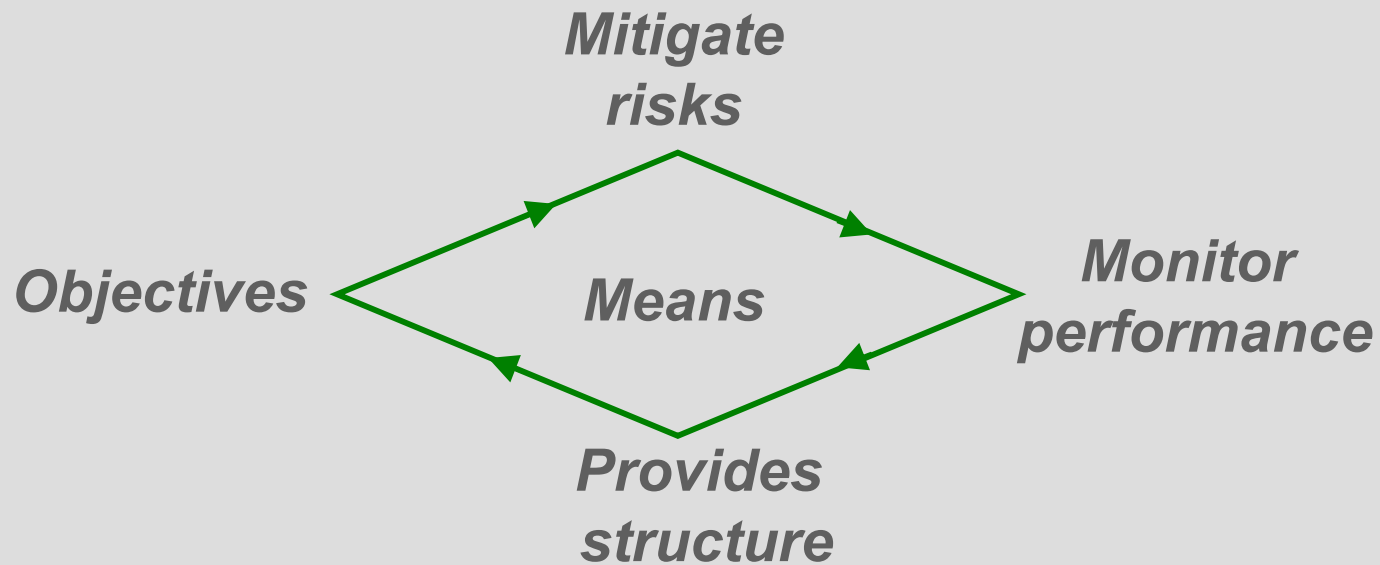
*Corporate Governance is the system by which business corporations are directed and controlled.*

*Its structure specifies the distribution of rights and responsibilities among different stakeholders in the corporation, such as,*

- the shareholders,*
- the managers,*
- the board and*
- other participants,*

*and spells out the rules and procedures for making decisions on corporate affairs.*

# What ?

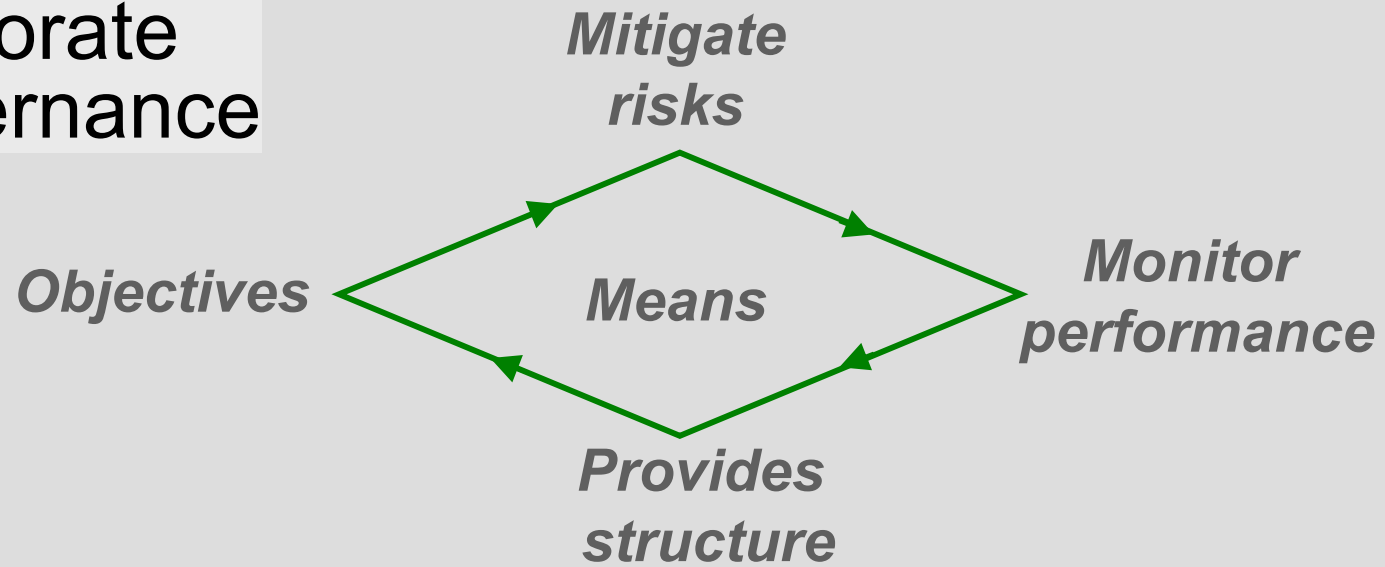


*Corporate Governance provides the structure through which*

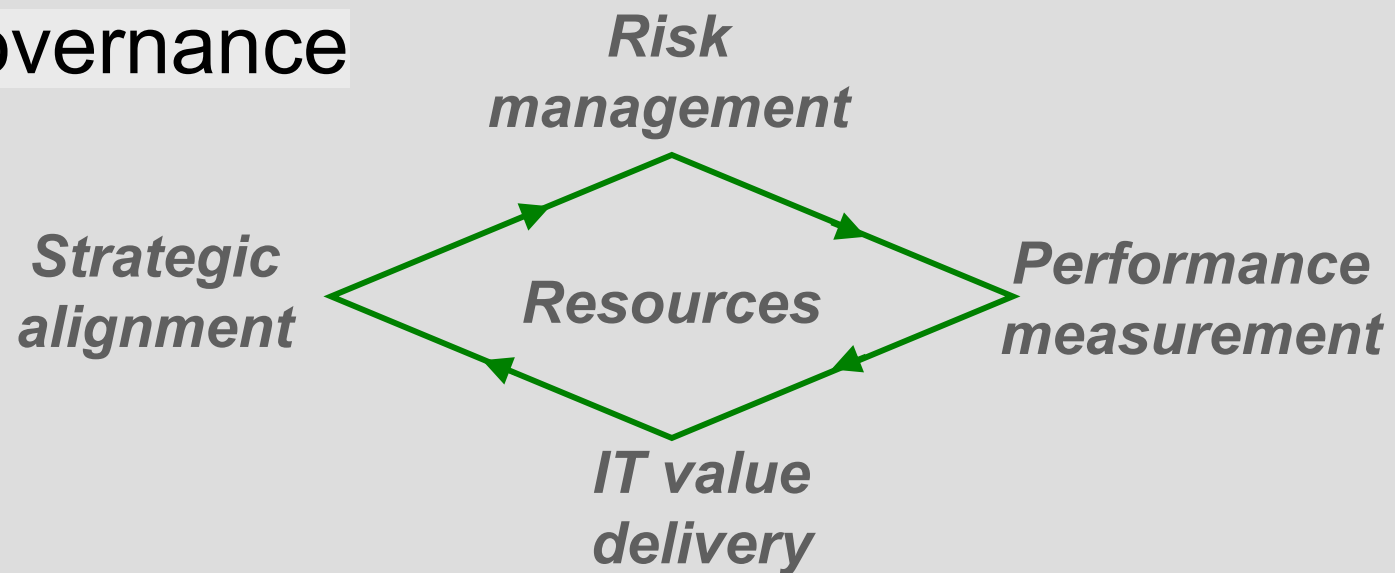
- the **objectives** of an organisation are set;
- the **means** of attaining those objectives are implemented;
- the **risks** are mitigated;
- and the monitoring **performance** guidelines are determined

# What ?

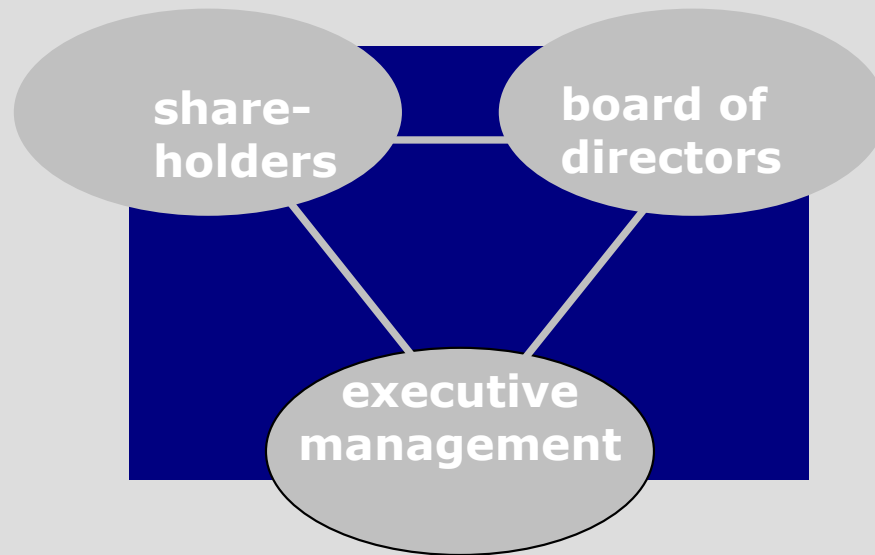
## Corporate Governance



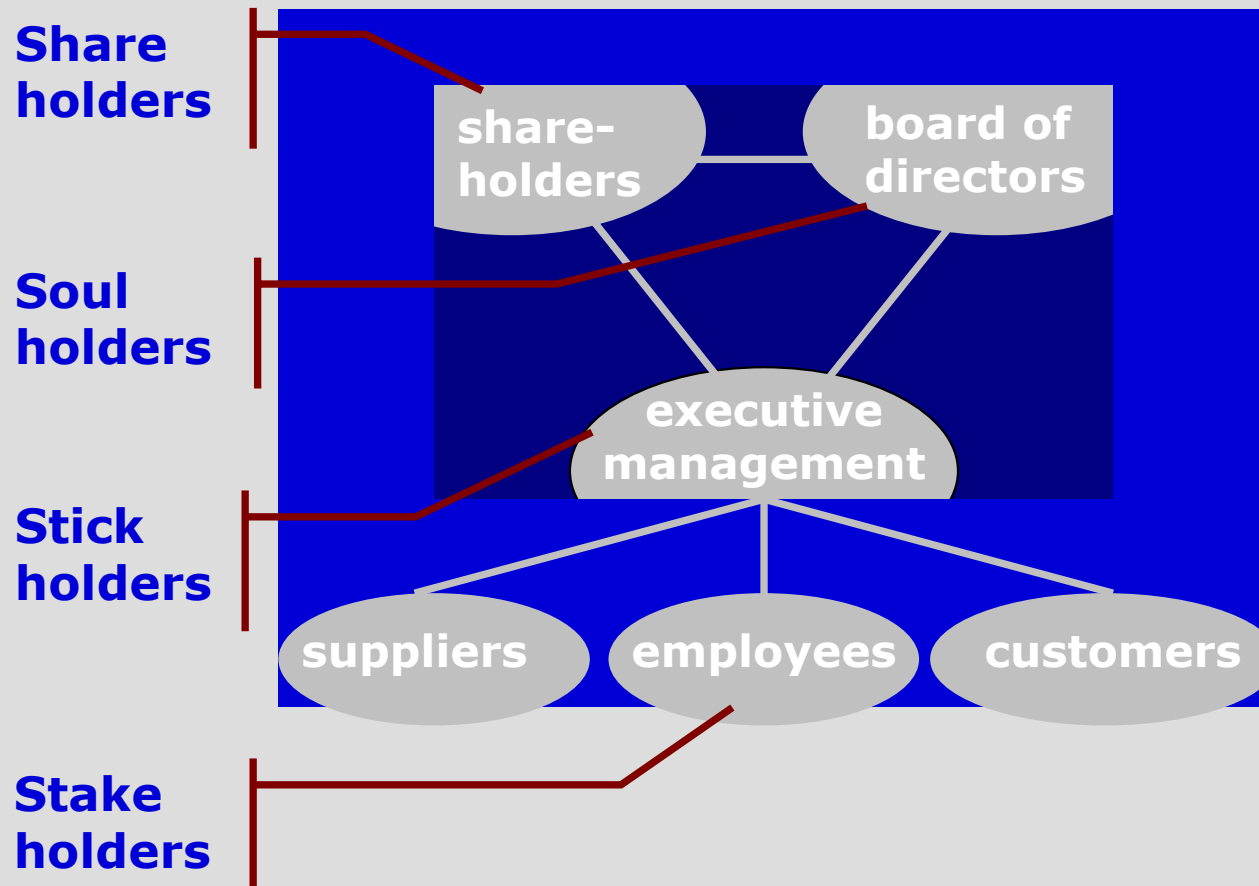
## IT Governance



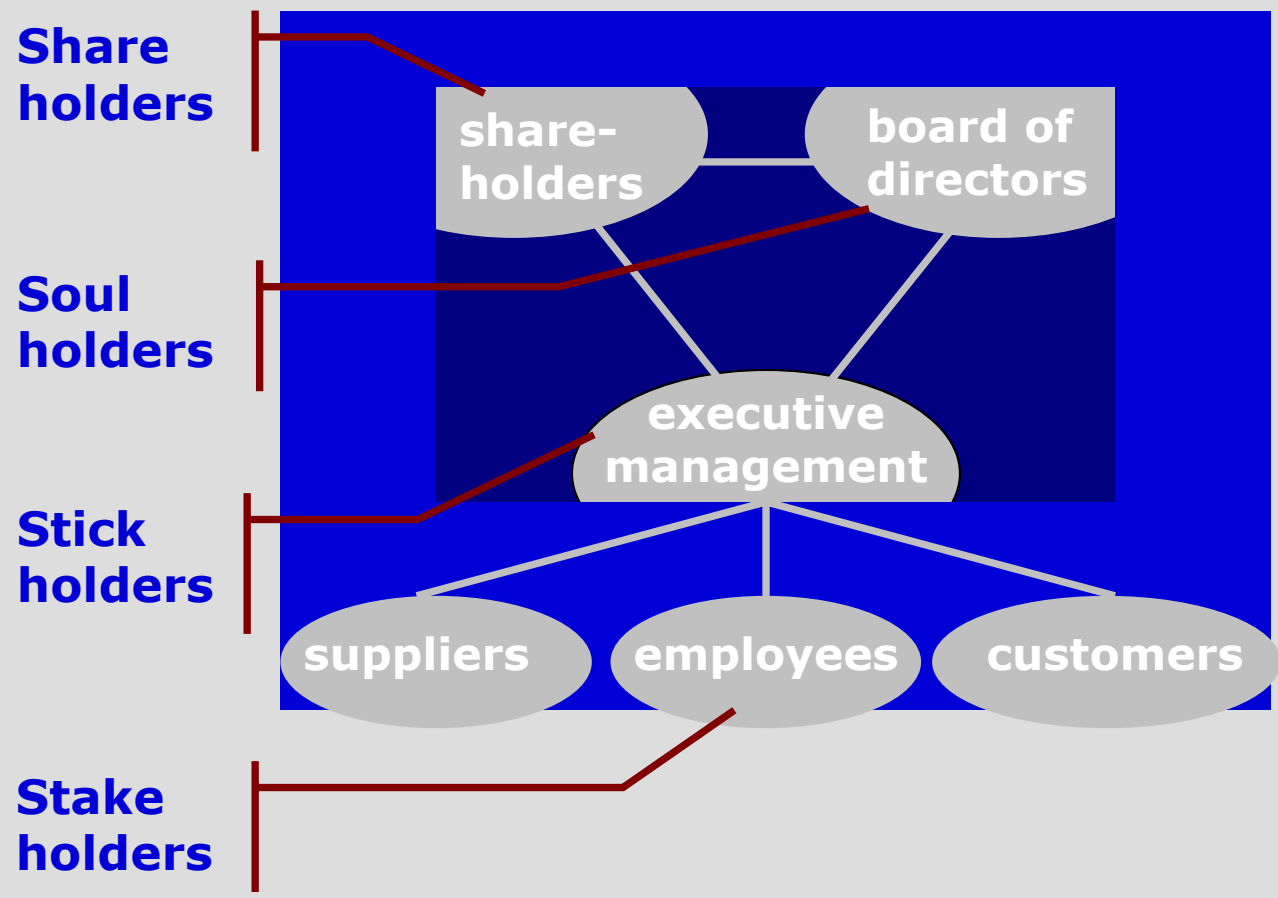
# Who ?



# Who ?

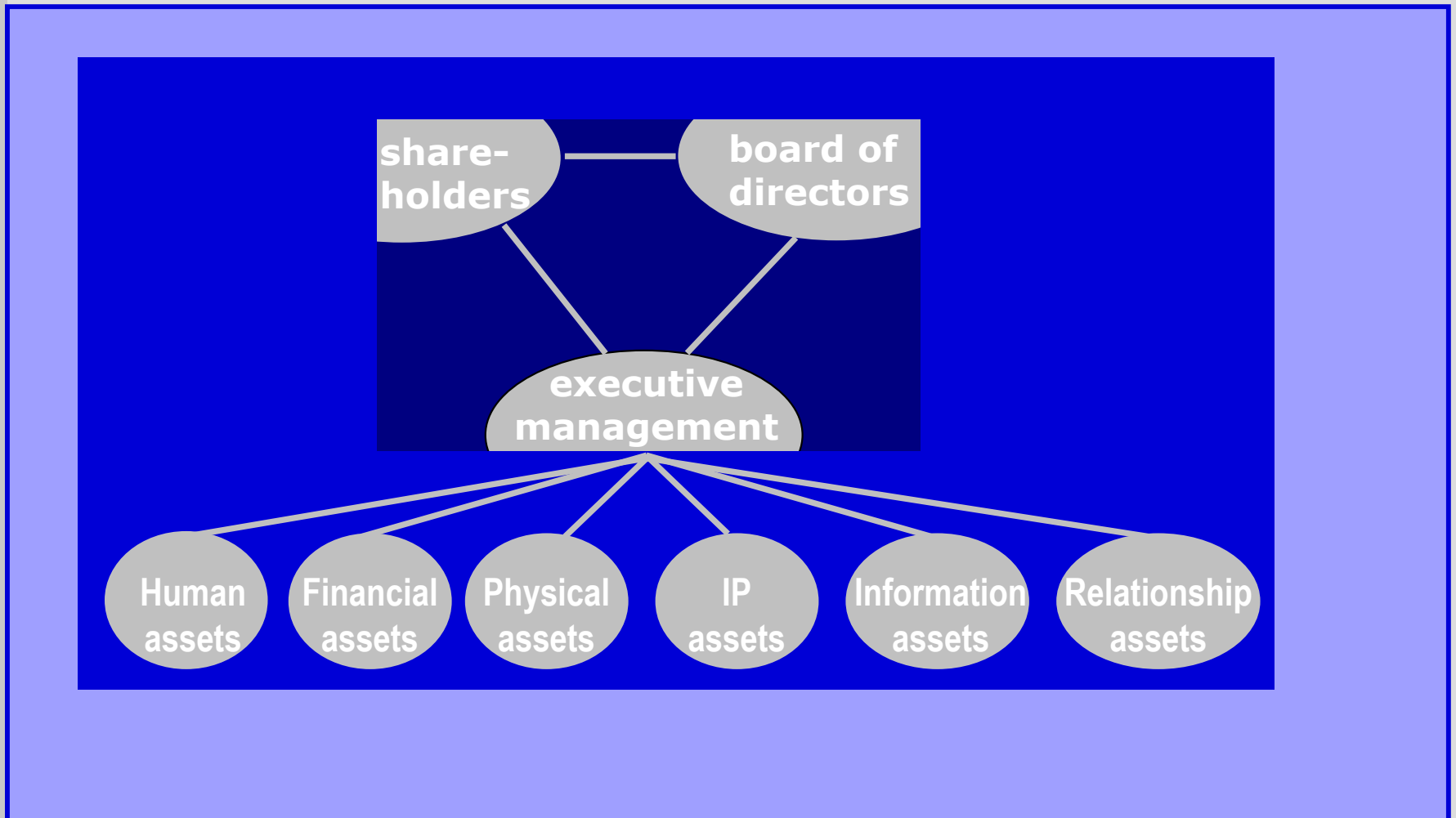


# Where ?

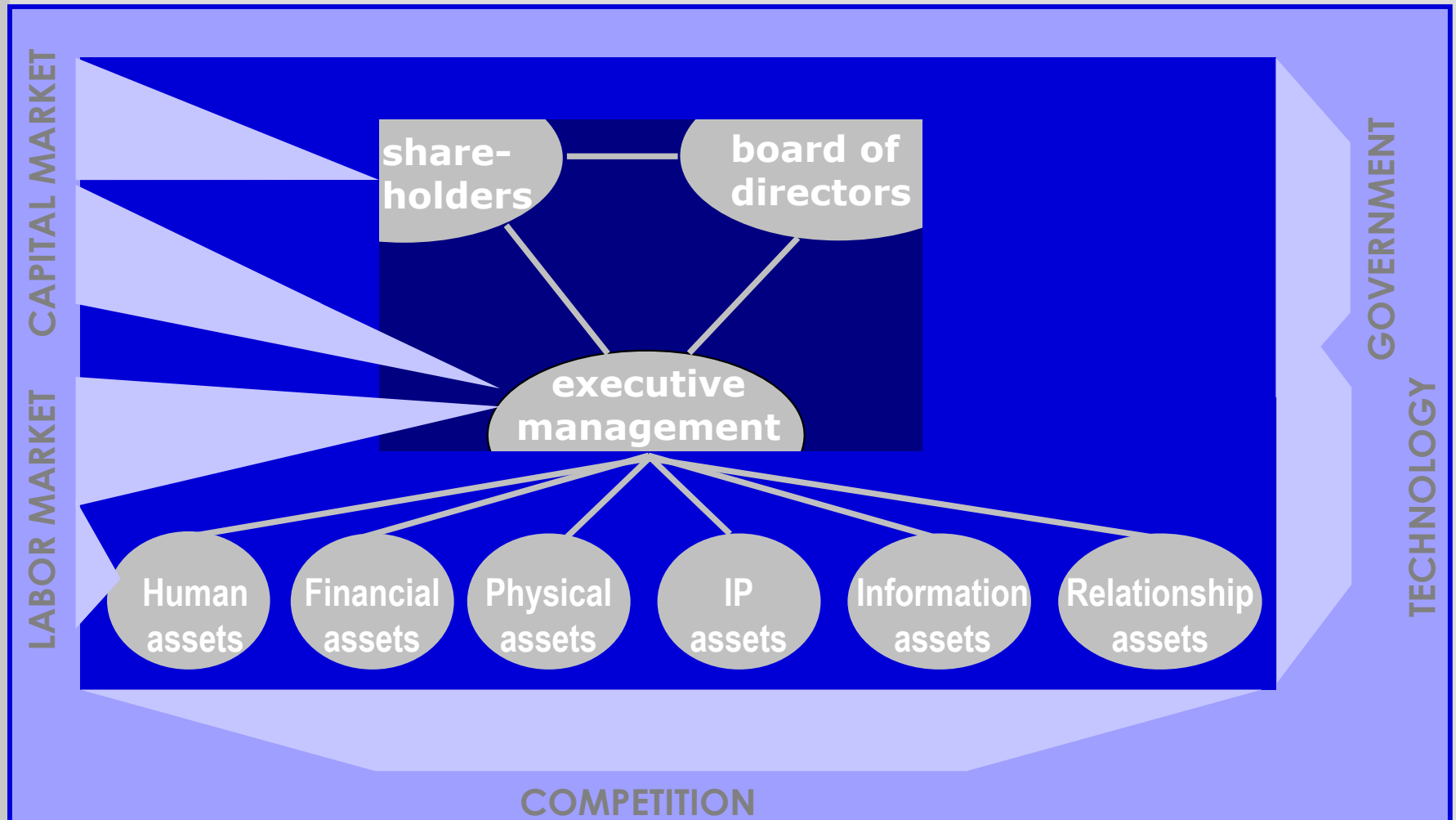


<b>Meetings</b>
<b>General assembly</b>
<b>Board of directors</b>
<b>Executive committee</b>
<b>Entreprise board</b>

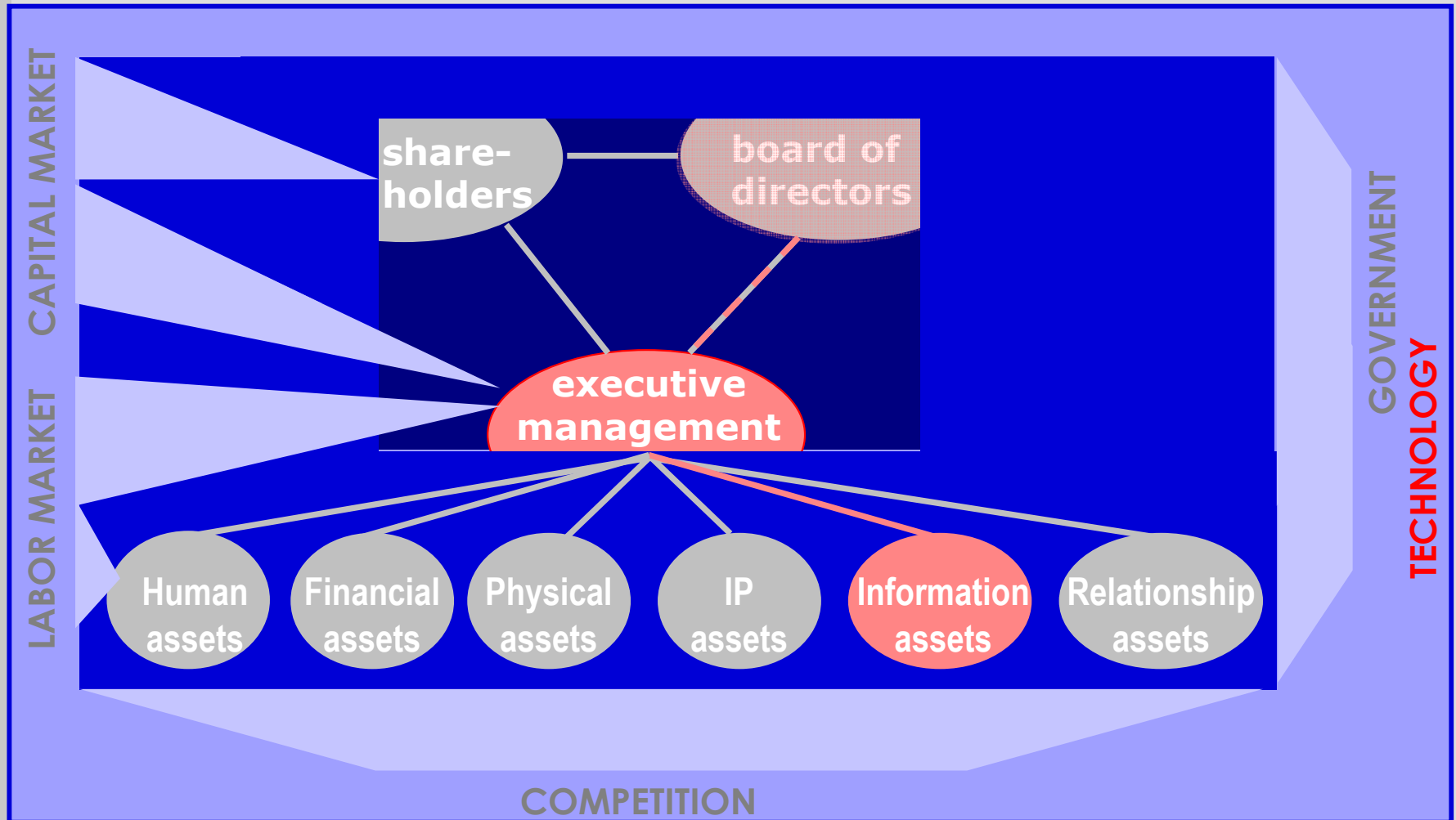
# Entreprise Governance structure



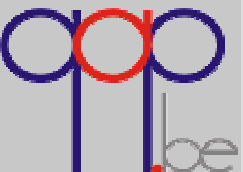
# Entreprise Governance structure



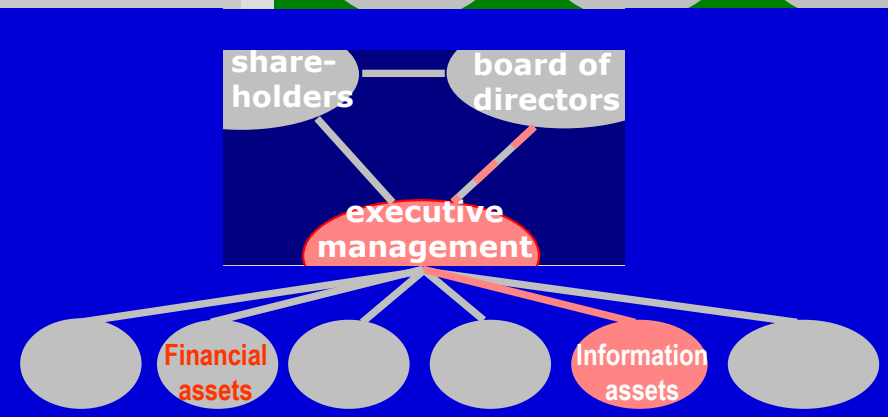
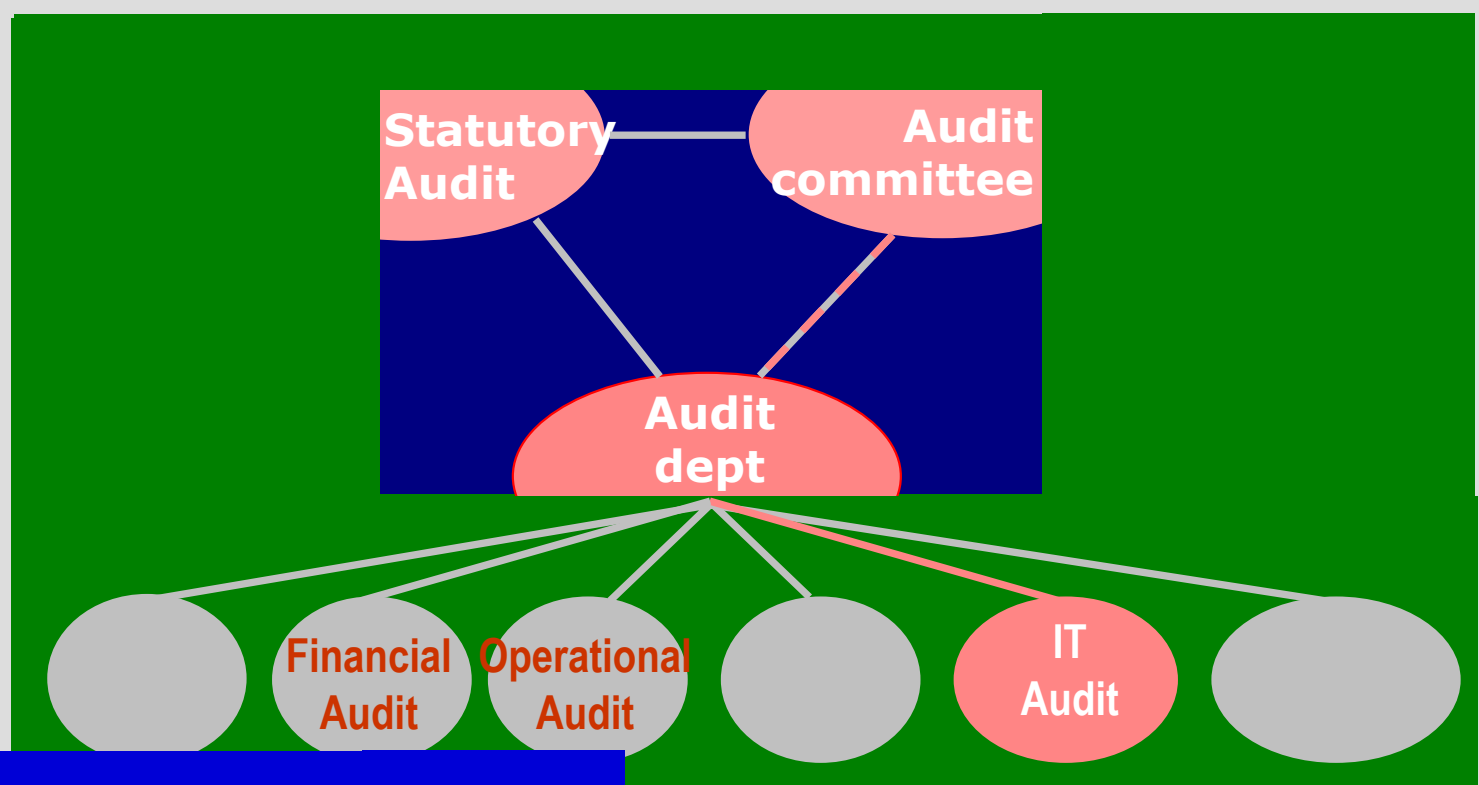
# IT Governance



**IT governance part of enterprise governance**



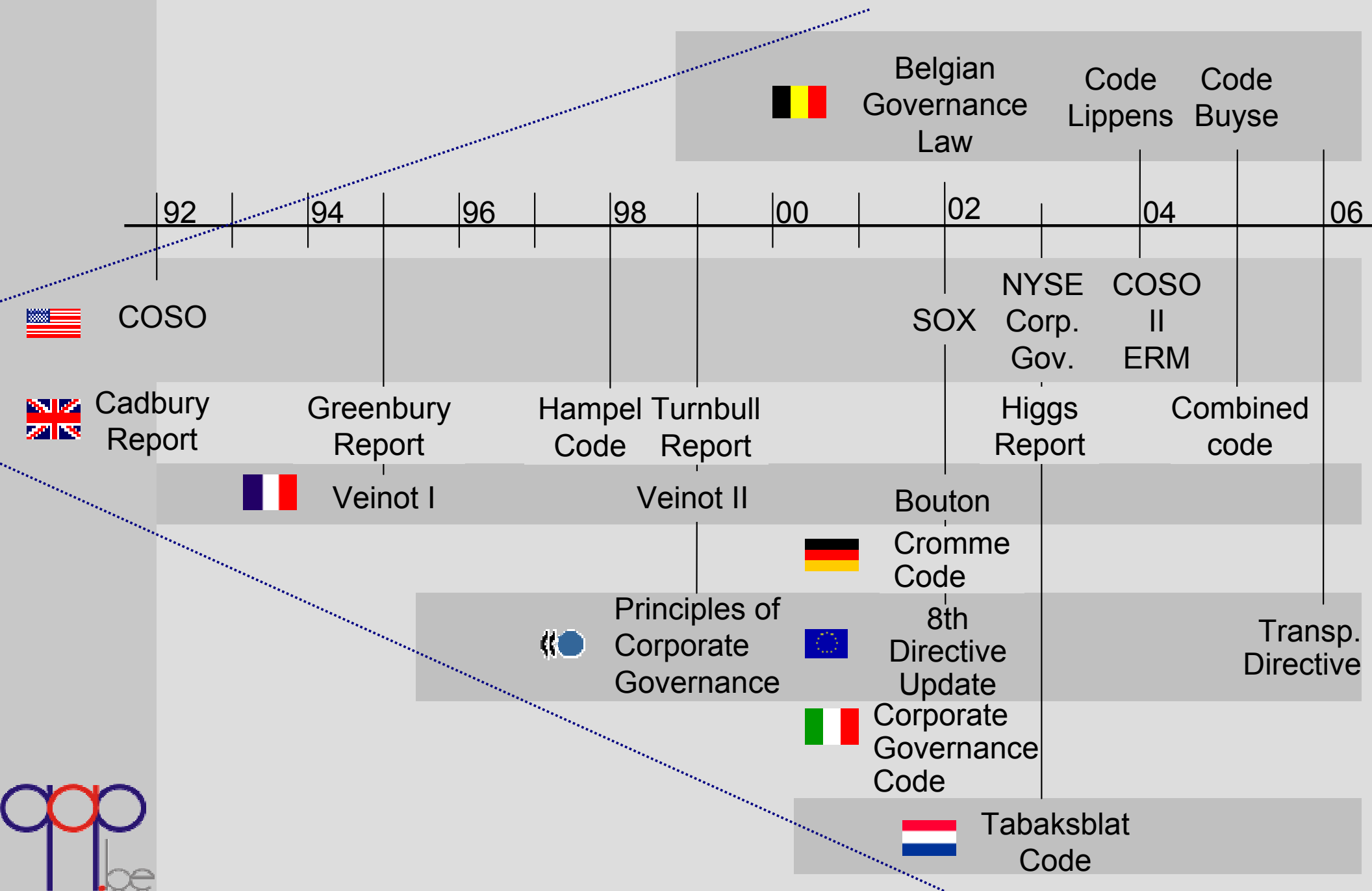
# The Audit structure



# Corporate Governance Evolution Regulatory Context

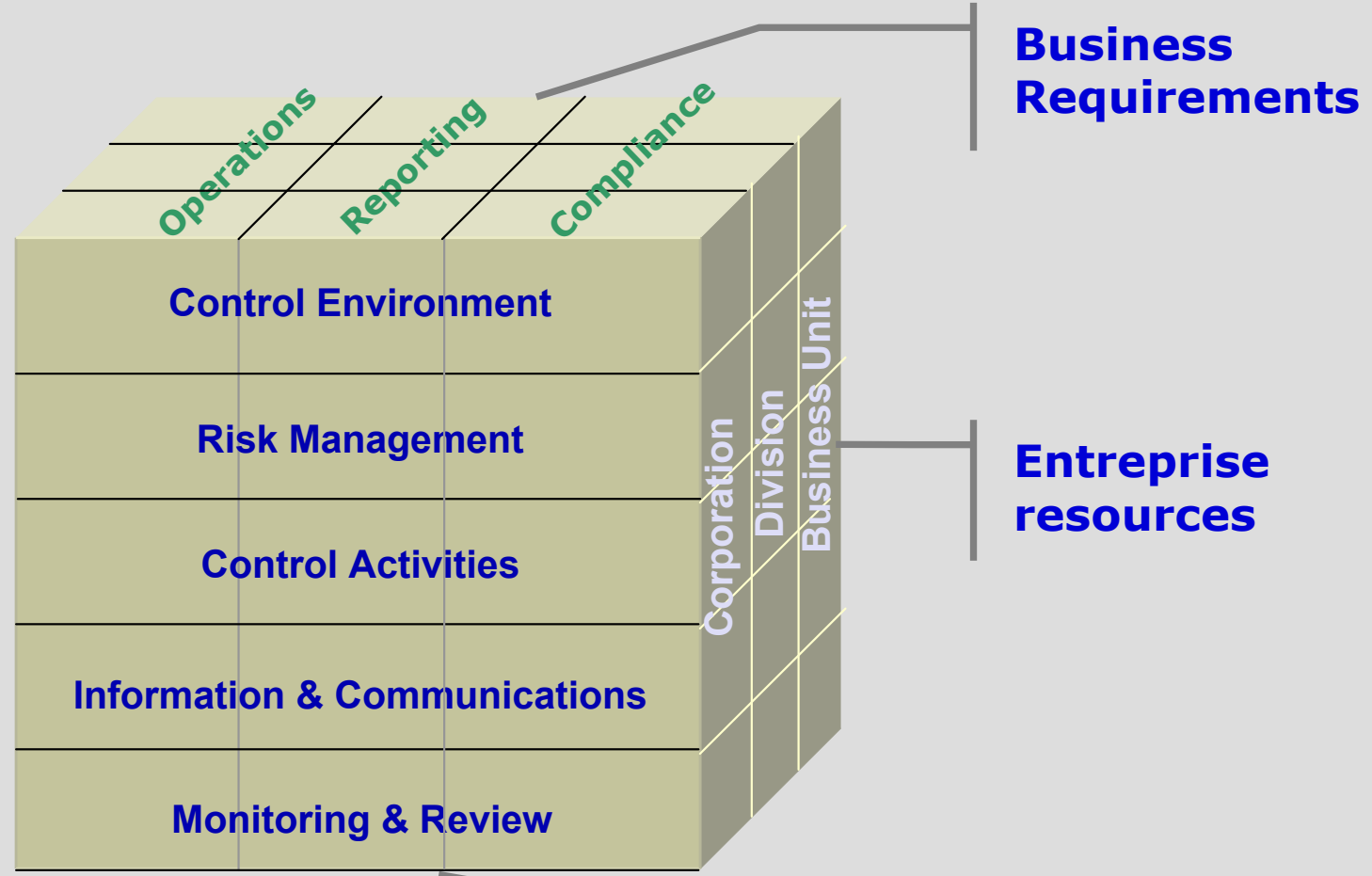


# Governance Timeline



# COSO framework

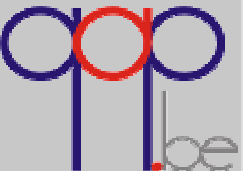
*COSO was formed in 1985 in the US to sponsor the National Commission on Fraudulent Financial Reporting*



WWW.COSO.ORG

2004: COSO II – Enterprise Risk Management

COSO – 2004 ©



# Sarbanes Oxley (SOX)



- SOX - key sections
  - 301 Accounting and Auditing *Complaints Hotline*
  - 302 Disclosure Procedures and Controls
    - *quarterly CEO/CFO certification*
  - **404** Internal Control over Financial Reporting certification and attestation (management responsibility)
  - 409 *Rapid Disclosure* of material events
  - Audit Committee *independence and expertise* and external auditor relationship
  - Establishment of the Public Company Accounting Oversight Board (PCAOB)
- Main focus is on internal control  
<-> management ethics, board provisions...

# Belgian Governance code Code Lippens



- Set up of Corporate Governance Committee in 2004
- Created at the initiative of the
  - Banking, Finance and Insurance Commission,
  - the Federation of Enterprises in Belgium, and
  - Euronext Brussels (stock exchange)
- Aim : single reference code for listed companies to set out principles of good governance and transparency
- Principles
  - Complementary to law
  - Recommendations on how to apply principles
  - Comply or explain
  - One-tier model

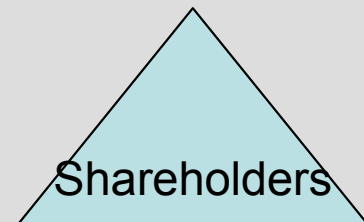
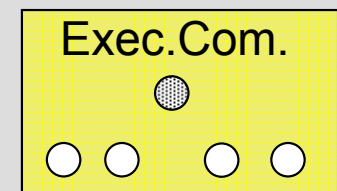
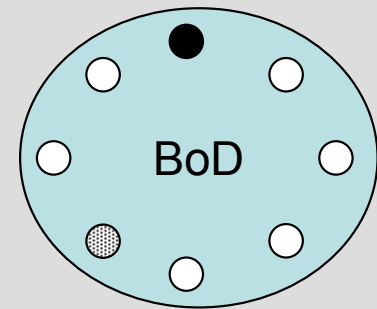


# Belgian Governance code



## PRINCIPLES of the LIPPENS CODE

1. THE COMPANY SHALL ADOPT A **CLEAR GOVERNANCE STRUCTURE**
2. THE COMPANY SHALL HAVE AN **EFFECTIVE AND EFFICIENT BOARD** TAKING DECISIONS IN THE CORPORATE INTEREST
3. ALL DIRECTORS SHALL DEMONSTRATE **INTEGRITY AND COMMITMENT**
4. THE COMPANY SHALL HAVE A RIGOROUS AND TRANSPARENT **PROCEDURE** FOR THE **APPOINTMENT AND EVALUATION** OF THE BOARD AND ITS MEMBERS
5. THE BOARD SHALL SET UP **SPECIALISED COMMITTEES**
6. THE COMPANY SHALL DEFINE A CLEAR **EXECUTIVE MANAGEMENT STRUCTURE**
7. THE COMPANY SHALL **REMUNERATE** DIRECTORS AND EXECUTIVE MANAGERS **FAIRLY AND RESPONSIBLY**
8. THE COMPANY SHALL RESPECT THE **RIGHTS** OF ALL **SHAREHOLDERS** AND ENCOURAGE THEIR PARTICIPATION
9. THE COMPANY SHALL ENSURE **ADEQUATE DISCLOSURE** OF ITS CORPORATE GOVERNANCE



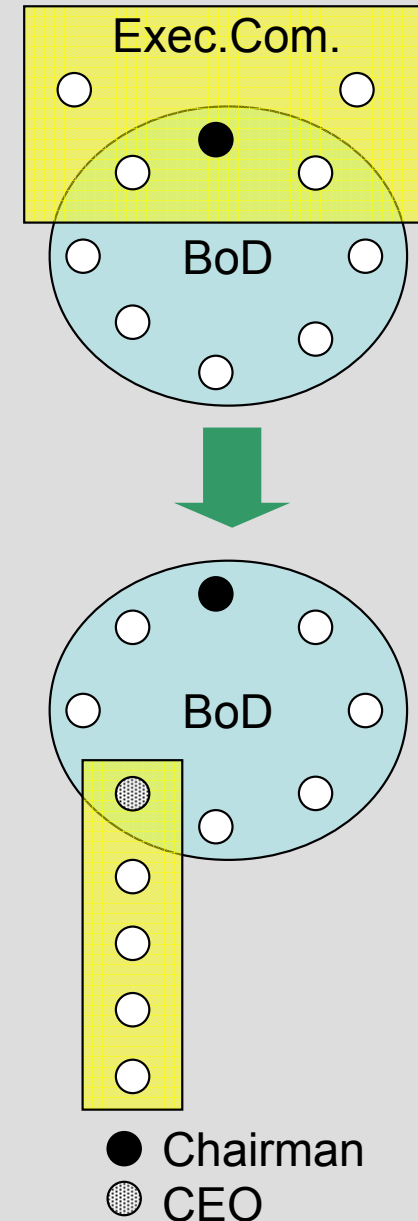
- Chairman
- CEO

# Belgian Governance code



## PRINCIPLE 1. THE COMPANY SHALL ADOPT A CLEAR GOVERNANCE STRUCTURE

- a collegial board,
- decide on the company's values and strategy, its risk appetite and key policies,
- monitoring responsibilities,
- decide on the executive management structure and determine its powers and duties,
- division of responsibilities between the chairman of the board and the CEO,
- account to shareholders.



# Belgian Governance code



## PRINC. 5. THE BOARD SHALL SET UP SPECIALISED COMMITTEES

- set up of committees giving advice to board,
- set up of an audit committee,
- set up of a nomination committee,
- set up of a remuneration committee,
- ensure 3 members including chairman per committee,
- board committees entitled to use external advice,
- committee findings and recommendations to board.

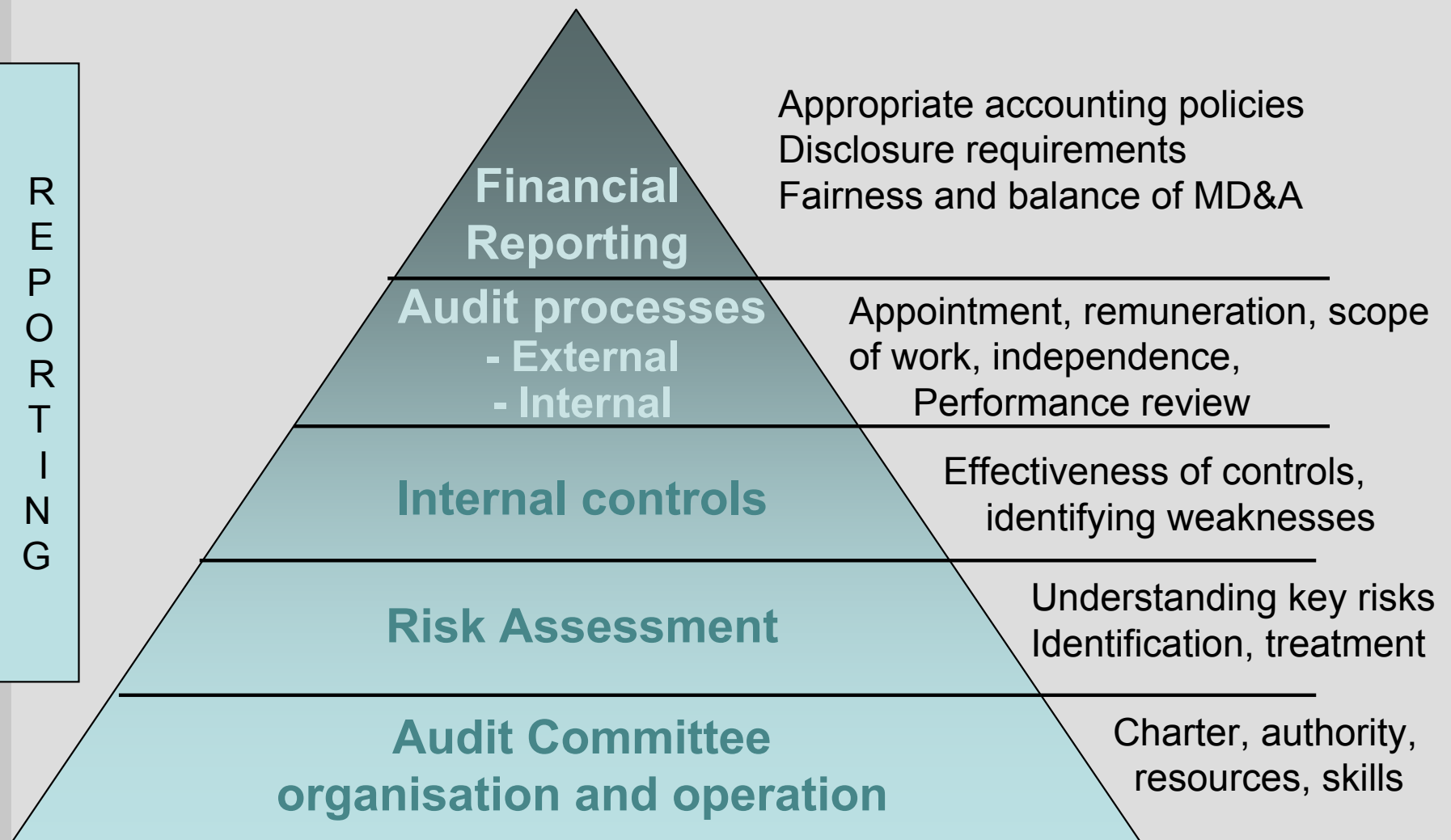
# Audit Committee

- **Composition**
  - **Non executive directors** exclusively, with a majority of independent directors.
  - The **chairman** should **not** be the chairman of the board.
  - Should have sufficient relevant **expertise** (e.g., financial expertise, risk management).
- **Functioning**
  - should meet at least **three times** a year.
  - should decide **who attends** its meetings (i.e., the CEO, CFO, internal and external auditors, etc.)
  - should be entitled to meet with **any relevant person** without any executive manager present.
  - **Auditors** should be guaranteed **free access** to the audit committee (Internal and external). Audit committee = the principal contact point.
  - should discuss **terms of reference** and any **issues** arising from the audit process, at least twice a year (with internal and external auditors)

# Audit committee oversight

C  
O  
M  
M  
U  
N  
I  
C  
A  
T  
I  
O  
N

R  
E  
P  
O  
R  
T  
I  
N  
G



# Code Buysse



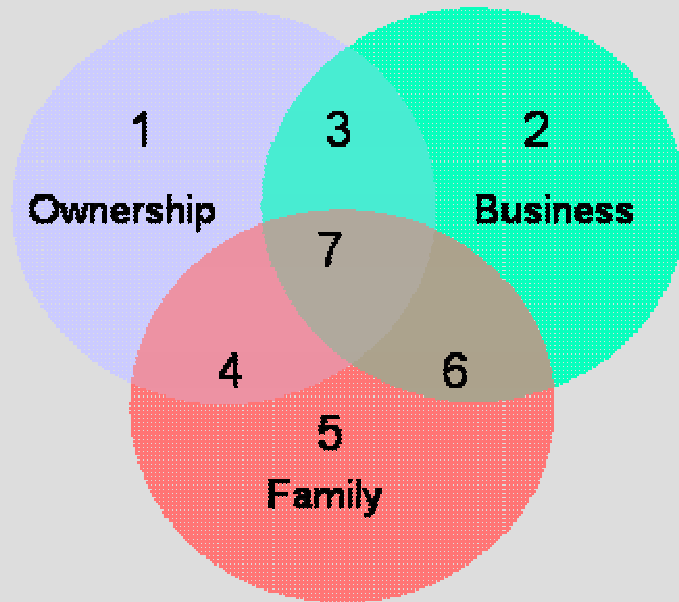
- Recommendation for non listed companies
  - Establishment of a vision and a mission
  - Active Board : balanced and independent composition
  - Efficient (senior) management
  - Involved shareholders
  - External control
  - Shareholders agreement : rights and obligations
  - Corporate Governance declaration



# Code Buysse



- Recommendations for family companies



1. External investors
2. Management & employees
3. Manager owners
4. Inactive family owners
5. Family (not owning, not active)
6. Family employees
7. Controlling family owner

- Family Forum
- Family Charter (vision, objectives, ownership, careers, governance, communication....)
- Succession
- Management of conflicts

# Code Buysse



- Relationships
  - Banks and financial institutions
  - Suppliers
  - Customers
  - Employees
  - External advisors
  - Shareholders agreement : rights and obligations
  - Public institutions

# 8th European Directives

- Major changes
  - Public oversight
  - Auditor independence
  - International Standards on Auditing (ISA)
- For public interest companies
  - Audit Committee requirement
  - A cooling-off period of two years (for statutory auditors)
  - Mandatory audit partner rotation  
(7 years - no audit cy rotation)
  - Annual transparency report (audit firms)

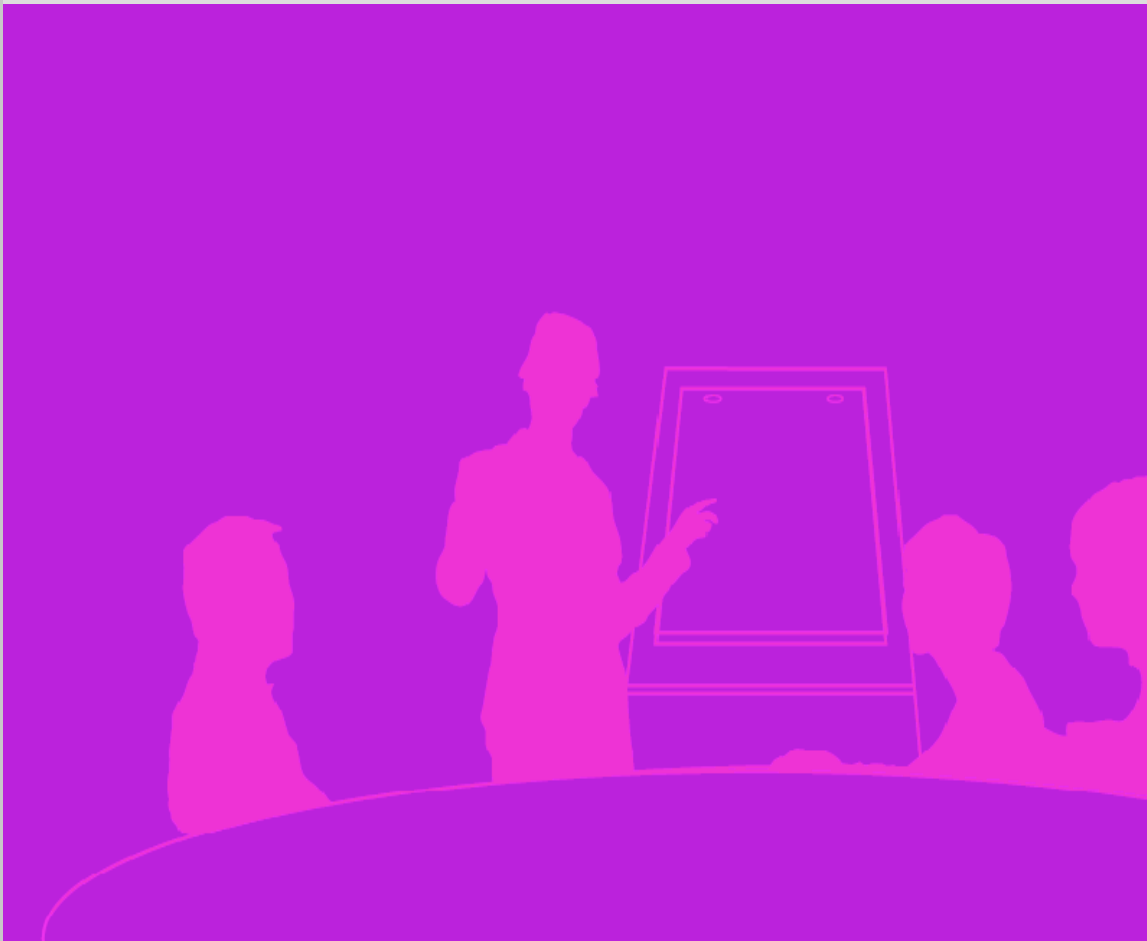
# European Transparency Directive

- Significant change to **timing** and **extent of publication** requirements for listed companies. (2007 in Be?)
- Annual financial info :
  - *4 months* after year end & available for 5 years
  - Contents : Financial statements (IFRS), Annual report of the Board, *Management true & fair view statements*
  - Full Audit report on Financial statements
- Half year financial information
  - Within *2 months* & available for 5 years
  - Contents : *Condensed financial statements, interim management report, True & fair view statements*
  - Full Audit report on Financial statements

# European Transparency Directive (2)

- Interim management statements
  - Every 6 months period
  - Between 10 weeks after start & 6 weeks before end period
  - Contents : explanation of material events and transactions, their impact on the financial position, and a general description of the financial position and performance
- Ongoing information
  - Changes in participation
  - Vote by means of proxy (already in B)
  - Information by electronic means (already in B)
- Directors and members of the Audit Committee will have to **ensure** that these changes are **implemented**.

# Corporate Governance Audit Universe & plan



# Risk evolution

Financial Reporting & Compliance	<ul style="list-style-type: none"><li>• Inaccurate financial statements</li><li>• Compliance with laws</li><li>• Integrity</li></ul>	

80s

# Risk evolution

Operational		<ul style="list-style-type: none"><li>• Ineffective and inefficient use of resources</li><li>• Systems integration</li></ul>
Financial Reporting & Compliance	<ul style="list-style-type: none"><li>• Inaccurate financial statements</li><li>• Compliance with laws</li><li>• Integrity</li></ul>	
	80s	90s

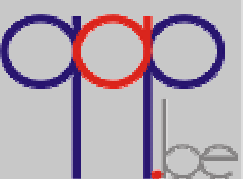
# Risk evolution

Strategic			<ul style="list-style-type: none"> <li>• Expansion / Acquisitions / ...</li> <li>• External conditions</li> <li>• Cy reputation</li> </ul>
Operational		<ul style="list-style-type: none"> <li>• Ineffective and inefficient use of resources</li> <li>• Systems integration</li> </ul>	<ul style="list-style-type: none"> <li>• Ineffective risk management</li> <li>• IT risks</li> <li>• Outsourcing</li> <li>• Supply chain</li> <li>• Customer relations</li> </ul>
Financial Reporting & Compliance	<ul style="list-style-type: none"> <li>• Inaccurate financial statements</li> <li>• Compliance with laws</li> <li>• Integrity</li> </ul>		
	80s	90s	00s

# Expanding audit responsibilities

Financial Reporting & Compliance	<ul style="list-style-type: none"><li>• Reactive control based financial statement review</li></ul>	

80s



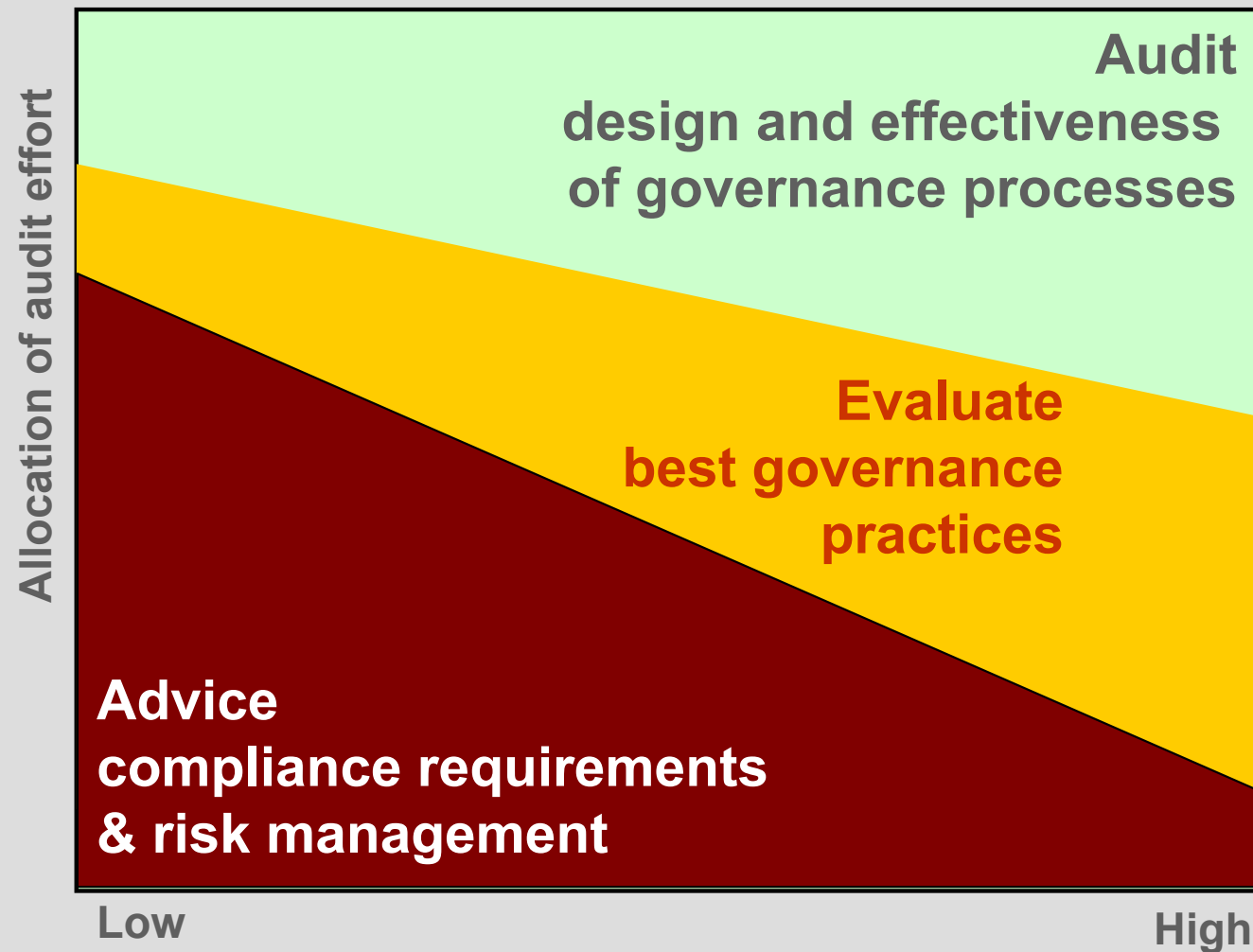
# Expanding audit responsibilities

	80s	90s	
Operational		<ul style="list-style-type: none"> <li>• Evaluate operational controls</li> <li>• Assist in control &amp; process design</li> </ul>	
Financial Reporting & Compliance	<ul style="list-style-type: none"> <li>• Reactive control based financial statement review</li> </ul>	<ul style="list-style-type: none"> <li>• Review control objectives &amp; efficiency</li> <li>• Assist in drafting company policy</li> </ul>	

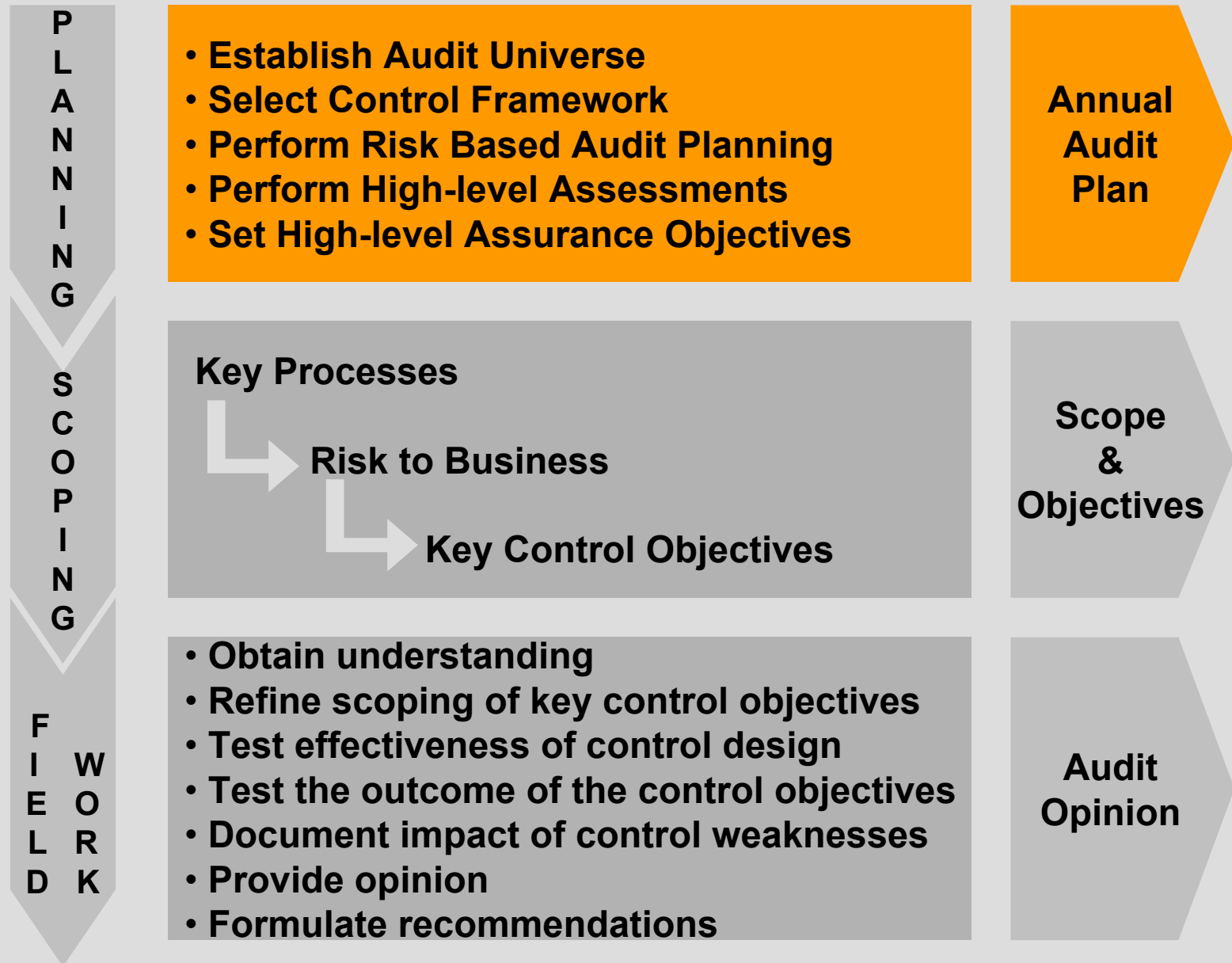
# Expanding audit responsibilities

Strategic			<ul style="list-style-type: none"> <li>• Strategic risk assurance</li> <li>• Review of risk management</li> </ul>
Operational		<ul style="list-style-type: none"> <li>• Evaluate operational controls</li> <li>• Assist in control &amp; process design</li> </ul>	<ul style="list-style-type: none"> <li>• Identify risk trends</li> <li>• Recommendations on risk processes</li> <li>• Identify gaps</li> </ul>
Financial Reporting & Compliance	<ul style="list-style-type: none"> <li>• Reactive control based financial statement review</li> </ul>	<ul style="list-style-type: none"> <li>• Review control objectives &amp; efficiency</li> <li>• Assist in drafting company policy</li> </ul>	<ul style="list-style-type: none"> <li>• Proactive risk based audit of mgt processes</li> <li>• Evaluate controls' effectiveness</li> </ul>
	80s	90s	00s

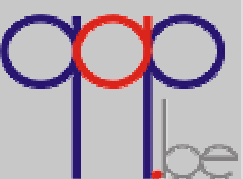
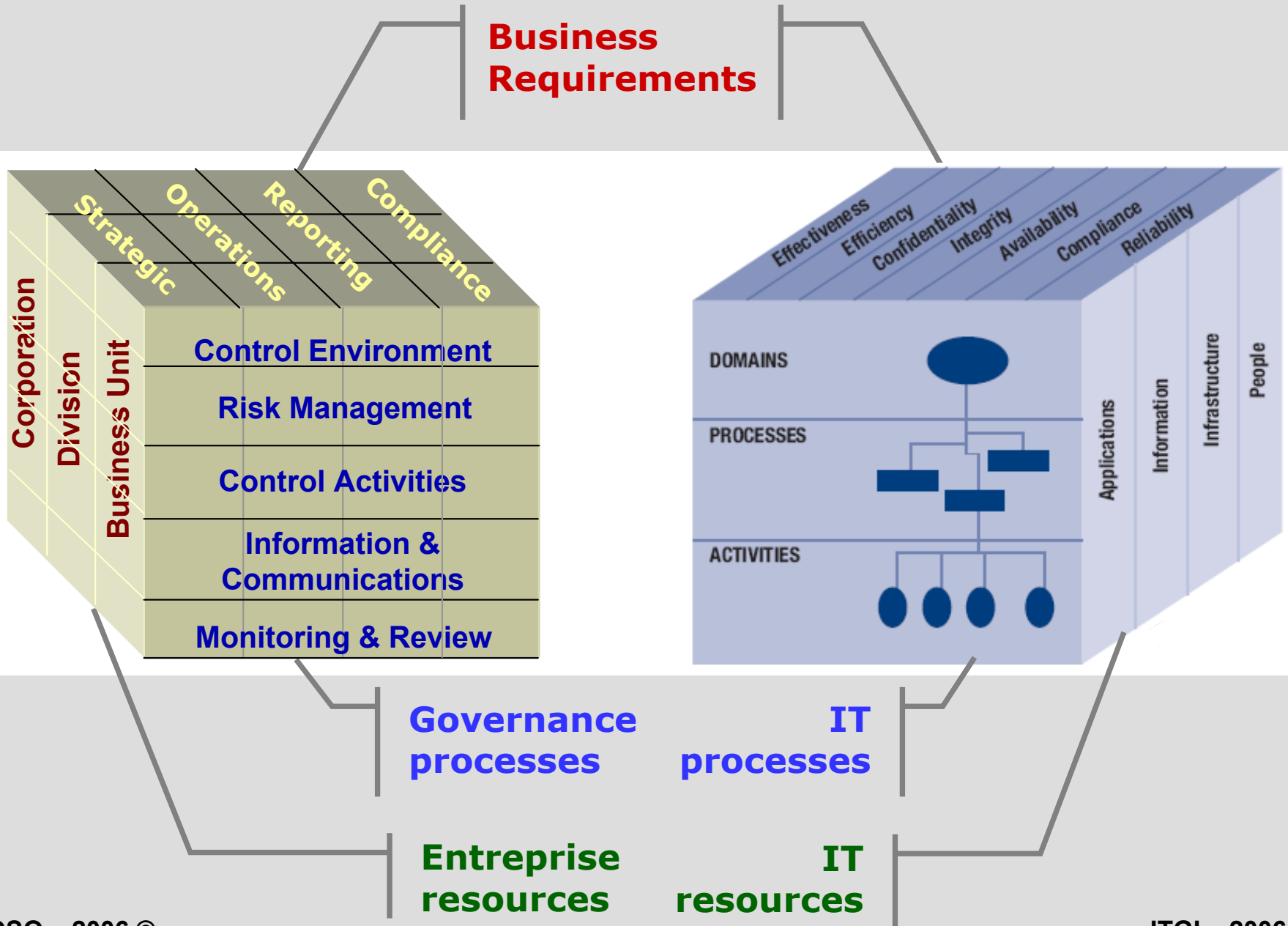
# Governance Audit maturity model



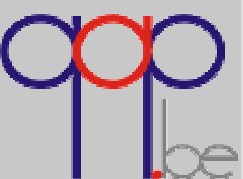
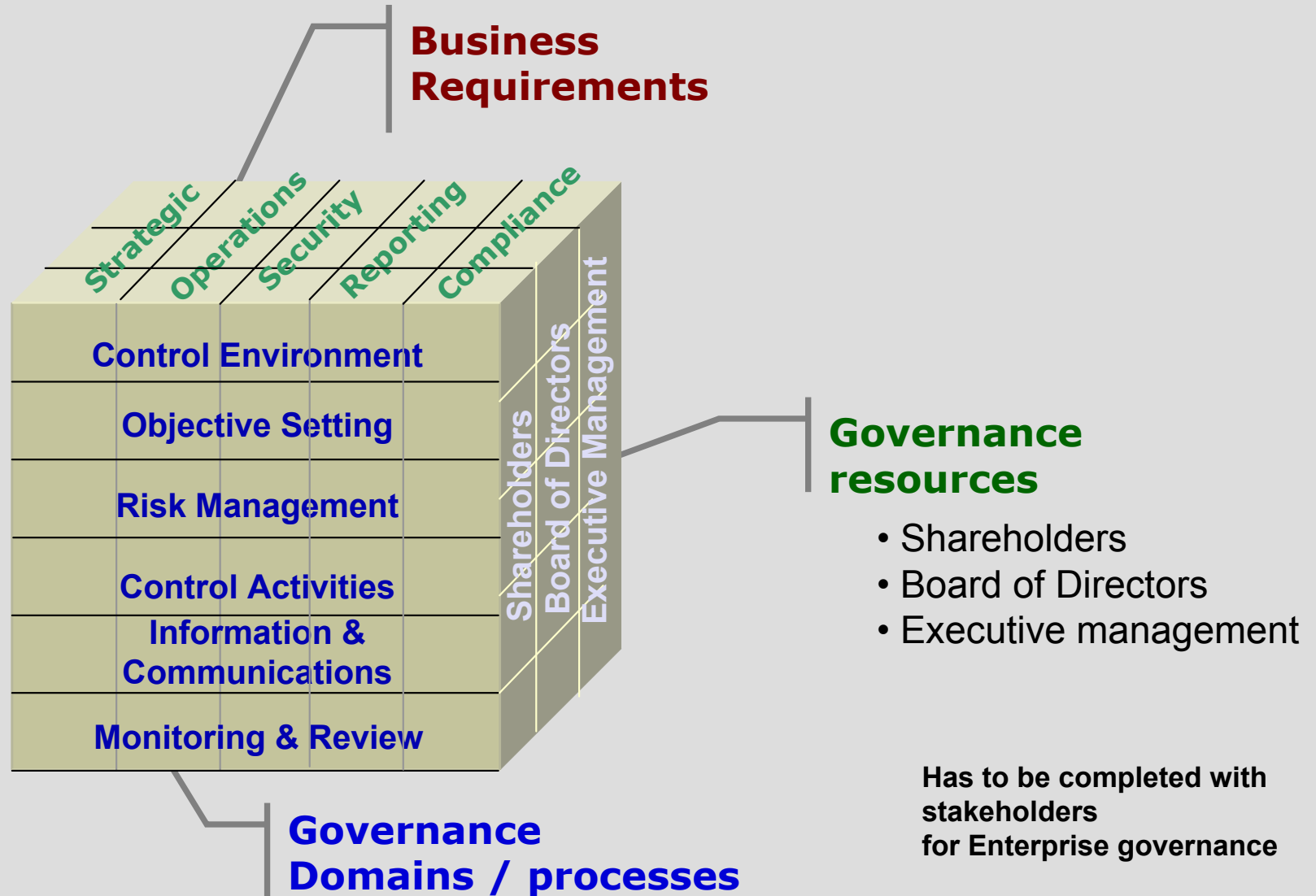
# From Audit plan to Audit Assignment



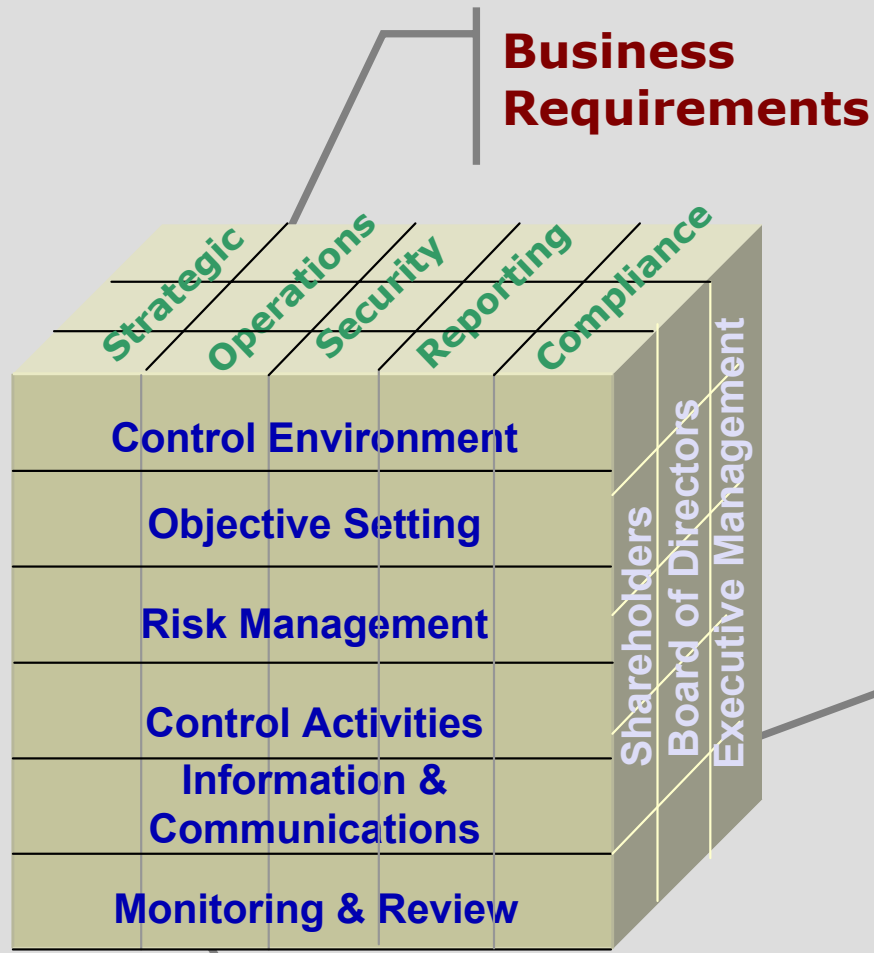
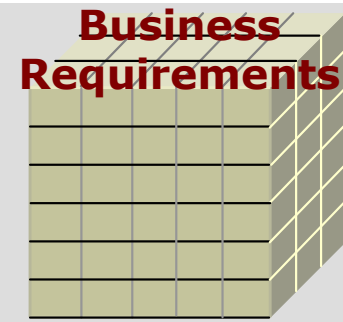
# COSO & CobiT frameworks



# Governance Framework



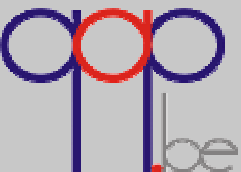
# Business requirements



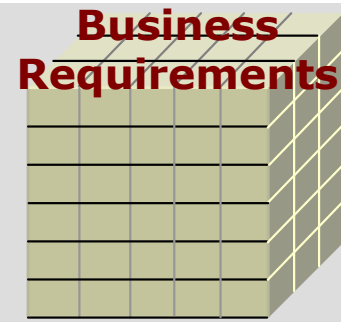
- Strategic
- Operations
  - Efficiency
  - Effectiveness
- Security
  - Confidentiality
  - Integrity
  - Availability
- Reporting (see next slide)
  - Completeness
  - Existence
  - Commitments
  - Reliability (Valuation)
  - Presentation & disclosure
- Compliance (with laws and regulations)

**Governance resources**

**Governance Domains / processes**

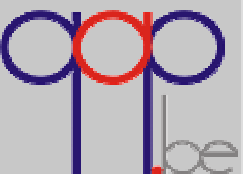


# Reporting requirements

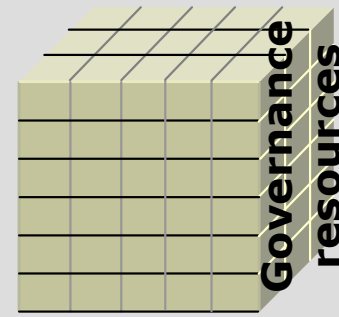


Express an opinion on [*financial*] statements:

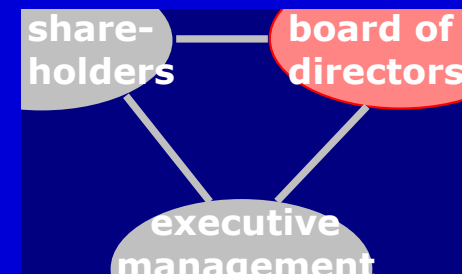
- **Existence** or occurrence of the assets / liabilities / transactions reflected in the [*financial*] statements
- **Completeness** of all [*financial*] information presented
- **Rights and obligations** to appropriately present relevant commitments in the [*financial*] statements
- **Reliability**(valuation) or allocation of the value of [*financial*] statement captions, on a fair and consistent basis
- **Presentation and disclosure** of values in the appropriate captions of the [*financial*] statements and relevant accounting principles or additional information to help ensure correct interpretation



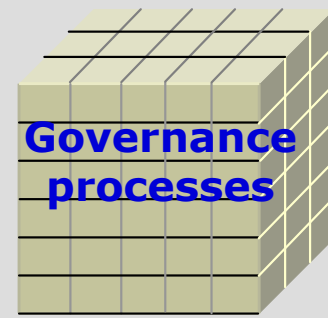
# Governance resources



- Board of Directors
  - President
  - Secretary
  - Executive Directors
  - Independent Directors
- Board Committees
- Shareholders
  - Majority shareholder
  - Minority shareholders
- Executive Management
  - CEO
  - Executive Committee
  - Compliance Officer
  - Risk Manager

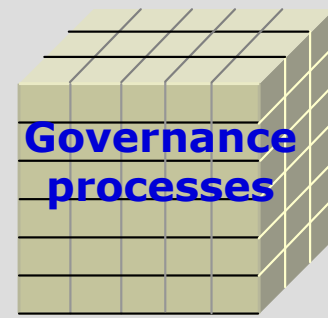


# Control Environment

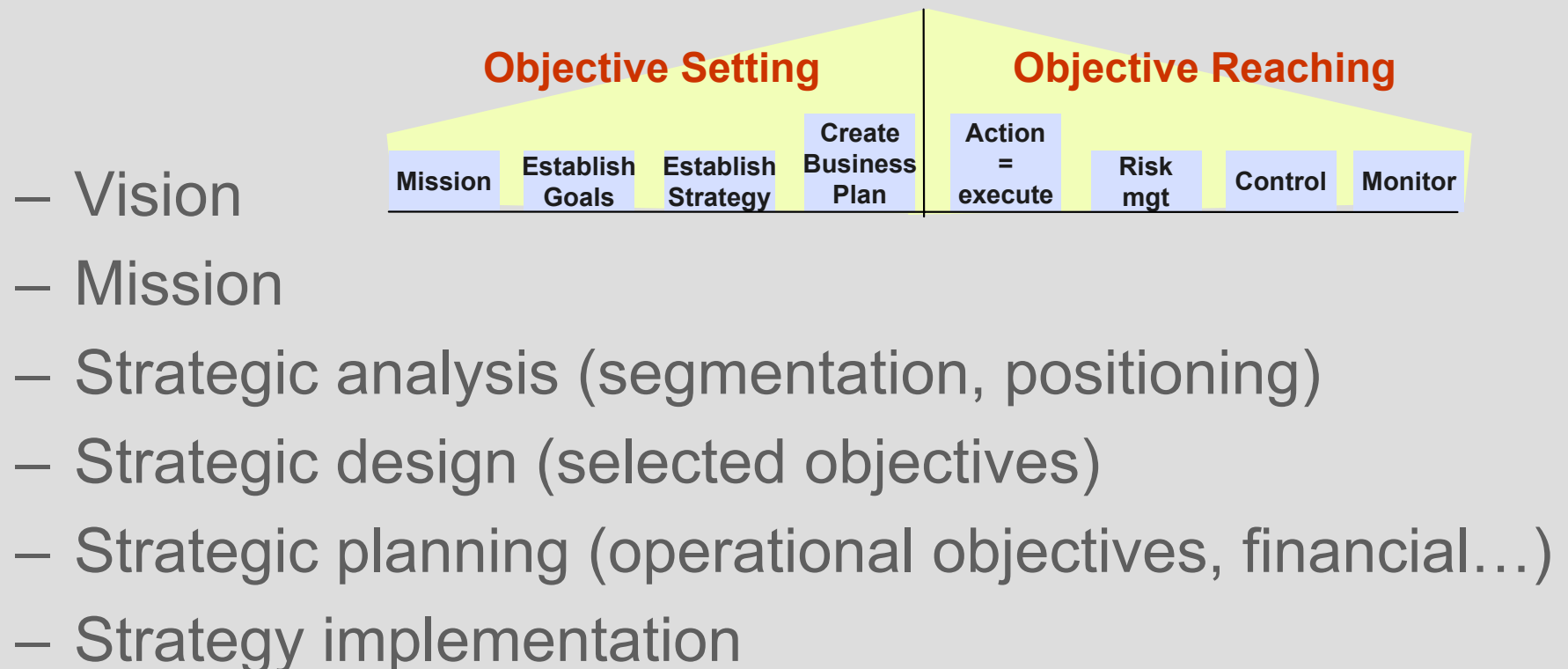


- *The Tone at the Top reflects the organisation's culture*
  - Integrity and Ethical Values (Behaviour, code of conduct, ...)
  - Management's Philosophy
  - Operating Style (Management styles, Risk appetite ...)
  - Risk Management Philosophy (Value, Communication)
  - Risk Culture & Risk Appetite (Strategy link)
  - Organizational Structure (Matrix, Reporting lines...)
  - Assignment of Authority and Responsibility (Empowerment, Accountability, Competence...)
  - Human Resource Management (Policies/Practices, recruitment, qualification, remuneration, training...)
  - Commitment to Competence (Knowledge, skills...)

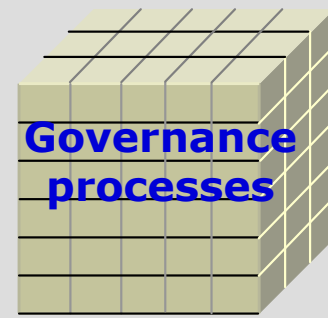
# Objective Setting



- The mission and vision set by management should be translated into a comprehensive set of objectives, communicated at all enterprise levels.



# Risk management

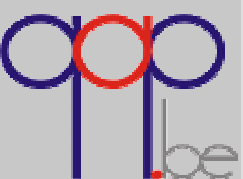


- Risk management aimed at

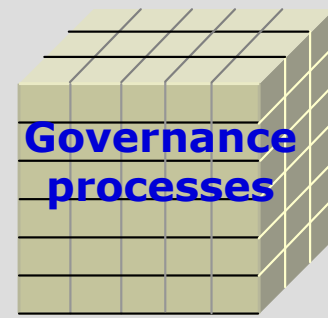


- o identifying potential events,
- o mitigating their impact on business objectives,
- o providing management reasonable assurance they will be reached.

- Event identification
- Risk assessment
- Risk treatment : mitigate
- Change management (new staff, new systems....)
- Communication and information



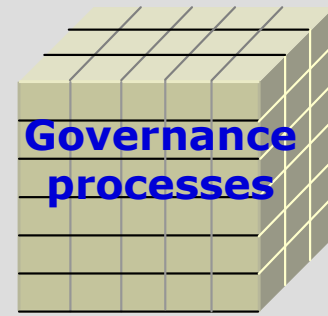
# Control activities



The comprehensive set of measures taken to ensure management directives and risk degree are suitably taken into account in the day-to-day operations to achieve the organisation's objectives.

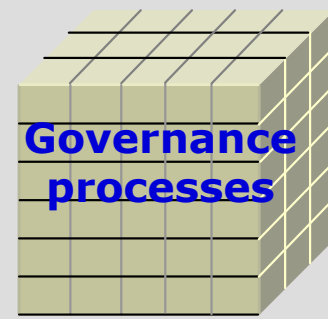
This includes approvals, verifications, reconciliations, performance reviews and security of assets.

# Control activities



- Control processes
  - General control activities
    - Policies and procedures
    - Management supervision
  - Financial reporting control activities
    - Accounting controls
    - Administrative controls
  - Operational controls
    - Process controls
    - Physical controls (e.g. inventory)
    - Segregation of duties
  - IT controls
    - General controls
    - Application controls
    - Data centre operations controls
  - Compliance controls
    - Laws, regulations

# Communication & Information



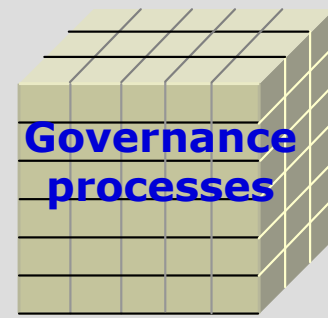
To carry out management and personnel responsibilities pertinent information should be

- identified,
- captured and
- communicated

in

- an adequate form and
- timeframe.

# Communication & Information



- Processes

- Information (Quality of the message)

- Information content

- Internal information to management, to staff

- External information to shareholders, to suppliers, to customers

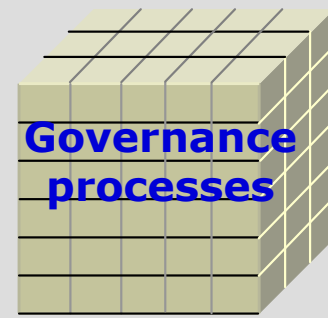
- Communication (Effectiveness)

- Form : Presentation of the message

- Communication channel : Press, internet, brochure...

- Timeframe : Adequate timing

# Monitoring & Review



- Monitoring is a process that assesses the quality of the company's performance over time.

It is accomplished

through ongoing monitoring activities and by separate evaluations.

Processes:

- Internal evaluations (integrated in mgt processes)
- External assessments (audits)
- Reporting deficiencies
- Balanced scorecards (KPIs)

# IT Governance integration

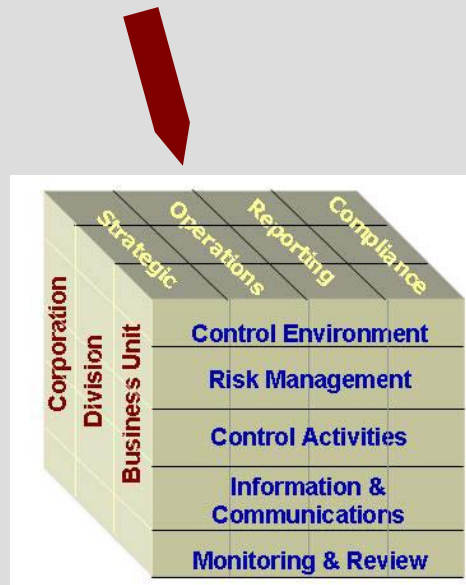
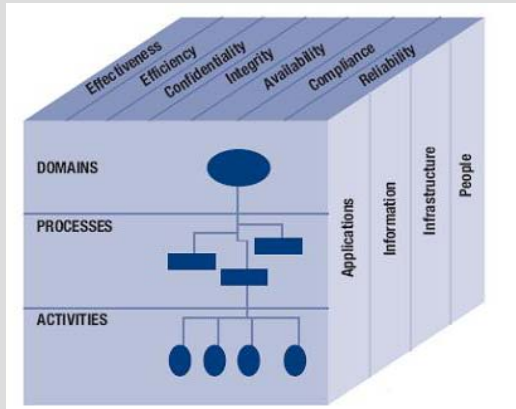
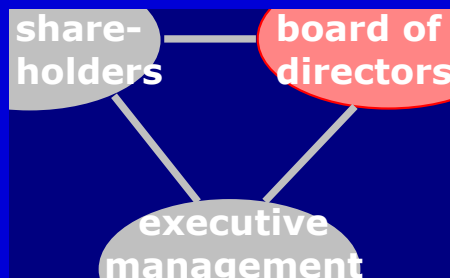


Figure 8—COBIT Relationship to COSO

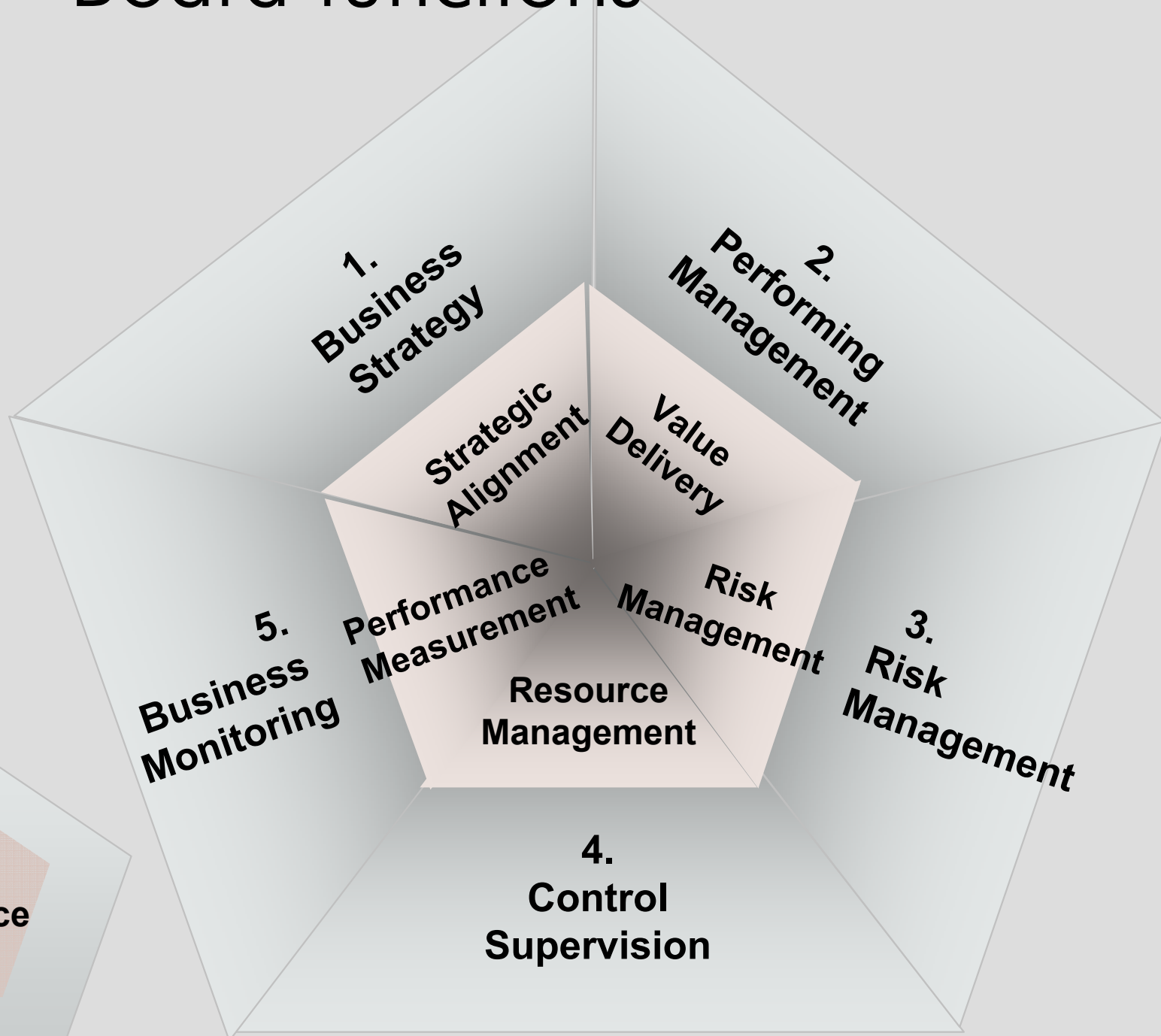
COBIT Control Objectives	COSO Component				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
<b>Plan and Organize</b>					
Define a strategic IT plan.		•		•	•
Define the information architecture.			•	•	
Determine technological direction.					
Define the IT organization and relationships.	•			•	
Manage the IT investment.					
Communicate management aims and direction.	•			•	•
Manage human resources.	•			•	
Ensure compliance with external requirements.			•	•	•
Assess risks.		•			
Manage projects.					
Manage quality.	•		•	•	•
<b>Acquire and Implement</b>					
Identify automated solutions.					
Acquire and maintain application software.			•		
Acquire and maintain technology infrastructure.			•		
Develop and maintain procedures.			•	•	
Install and accredit systems.			•		
Manage changes.			•		•
<b>Deliver and Support</b>					
Define and manage service levels.	•		•		•
Manage third-party services.	•	•	•		•
Manage performance and capacity.	•		•		
Ensure continuous service.	•		•		•
Ensure systems security.	•		•	•	•
Identify and allocate costs.				•	
Educate and train users.	•			•	
Assist and advise customers.				•	
Manage the configuration.	•		•	•	
Manage problems and incidents.			•	•	•
Manage data.			•	•	
Manage facilities.			•		
Manage operations.			•	•	
<b>Monitor and Evaluate</b>					
Monitor the processes.				•	•
Assess internal control adequacy.					•
Obtain independent assurance.	•				
Provide for independent audit.					

# Board functions

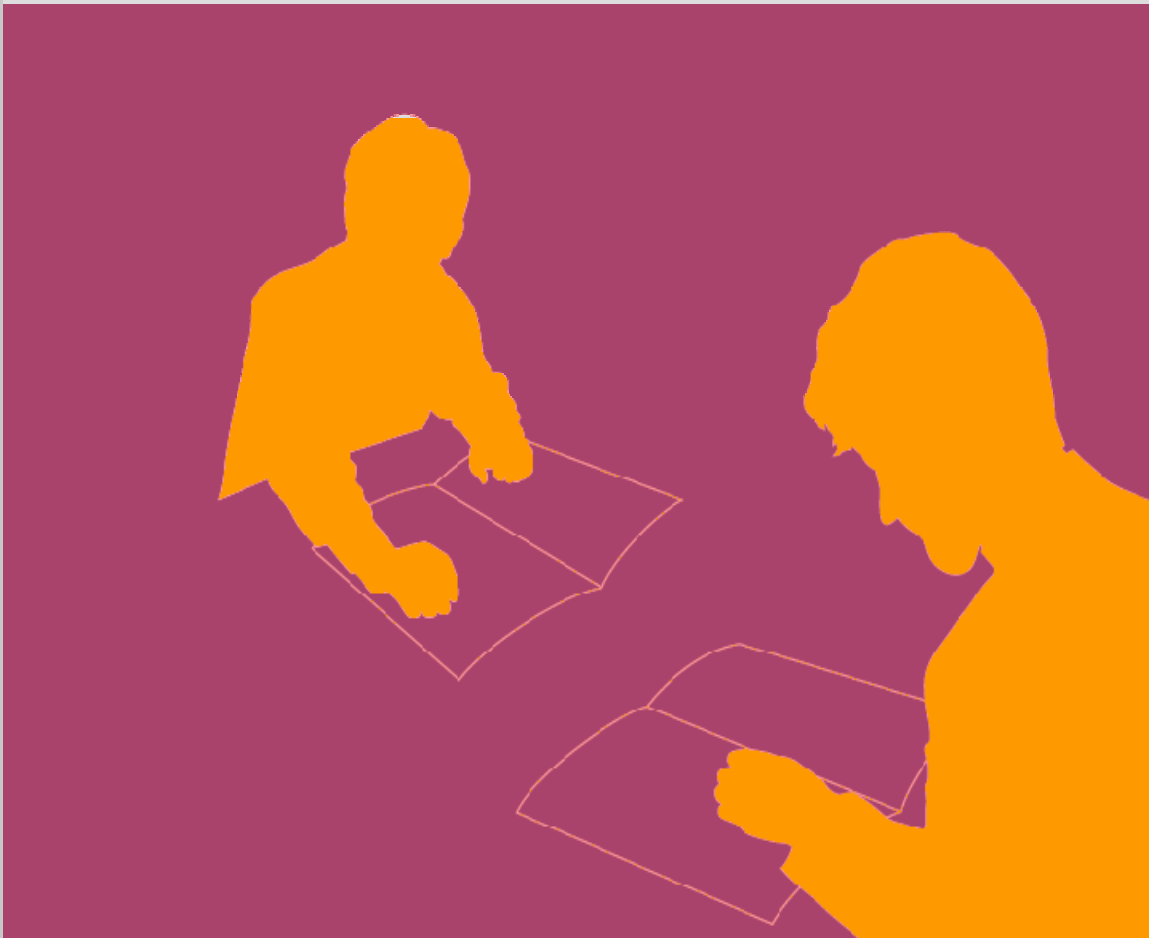
- Strategic : approve major strategies, financial objectives and strategic plans
- Performing management : CEO, mgt compensation, succession planning, advice
- Risk management : risk mitigation
- Internal control : review systems adequacy
- Monitoring : business, mgt, and board itself (processes and performance)



# Board functions

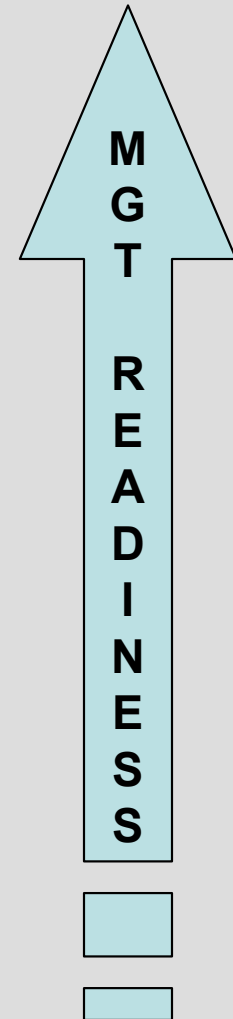


# Conducting Corporate Governance Audit



# Audit Decision

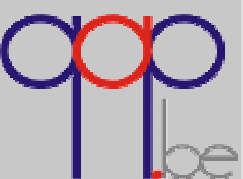
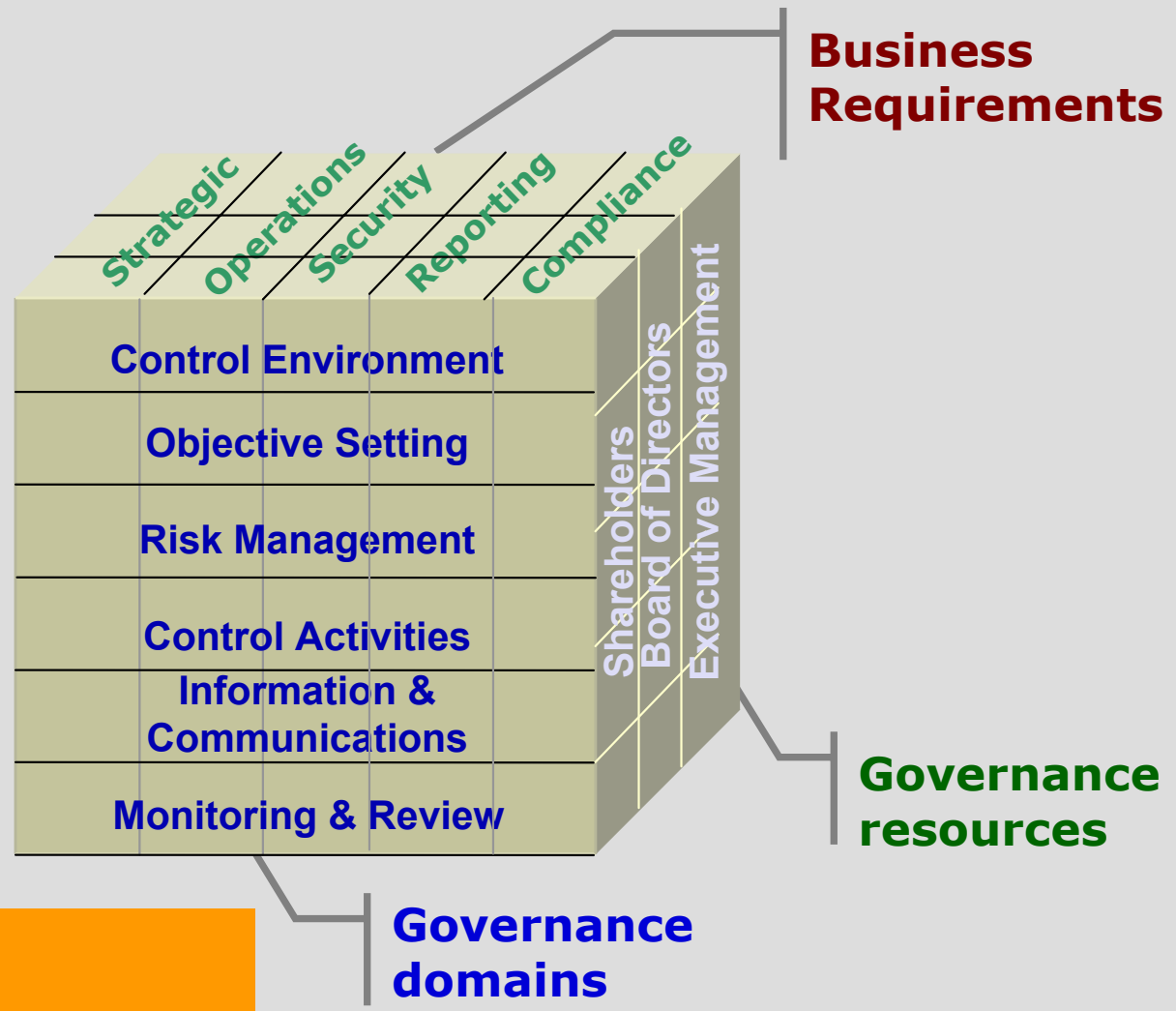
- Audit plan (audit cycle)
- Management demand
  - Business strategy or restructuring
  - Acquisition/merger
  - Management scandal
  - Negative press
  - .....



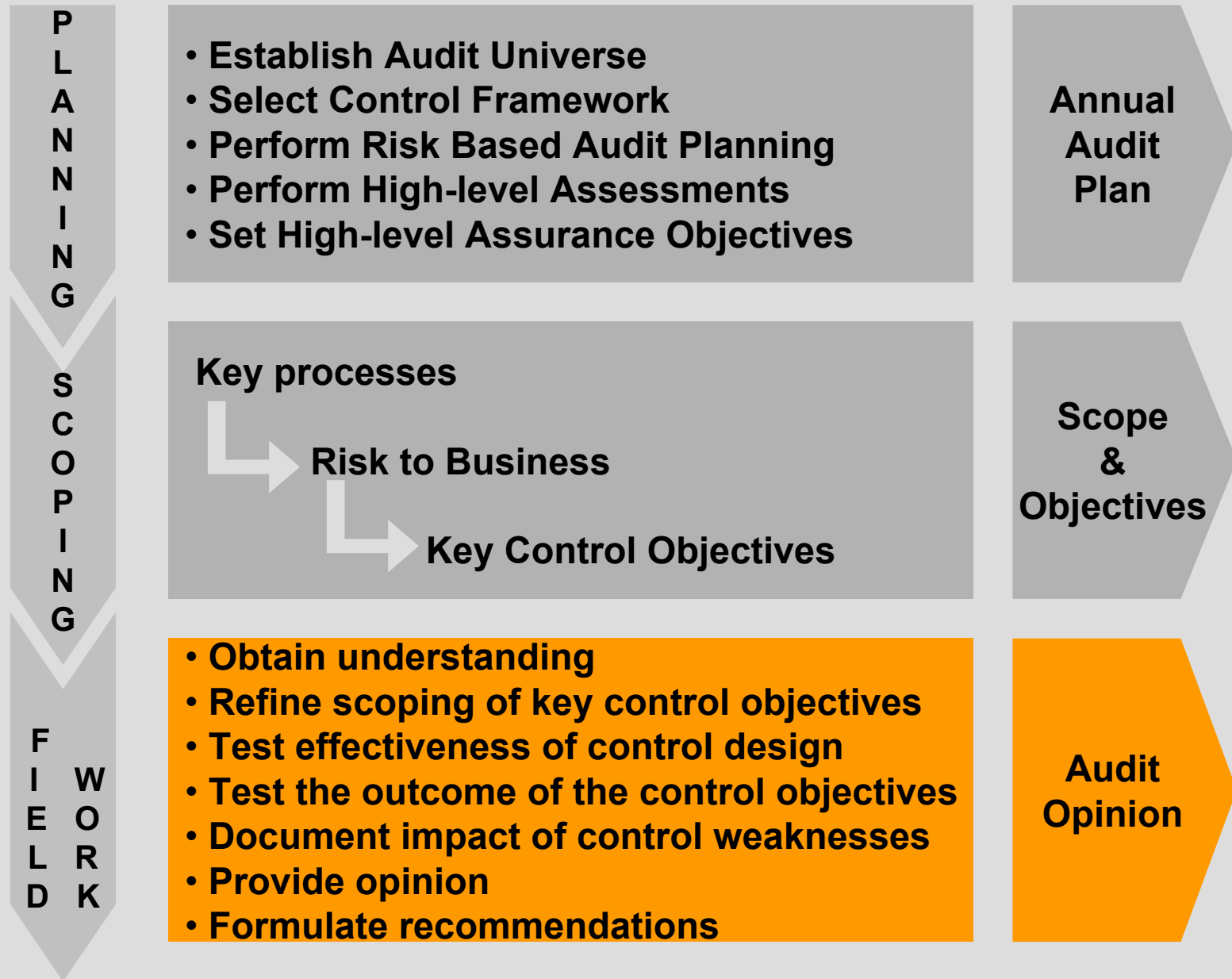
# From Audit plan to Audit Assignment



# Audit program



# From Audit plan to Audit Assignment



# The audit program - sample

- Annual General Meeting
  - Control Environment
    - Rights and duties of shareholders (\*)
    - Appointment of directors and external auditors
    - Remuneration of directors and external auditors .....
  - Control activities
    - Relieve board members responsibilities
  - Information & Communication
    - Financial information
    - Business status / Management information
    - Regulatory disclosures (statutory audit, governance, compensation...)
  - Monitoring
    - Shareholder participation

# The audit program - sample

- Annual General Meeting
  - Control Environment
    - Definition of shareholders' rights and duties

## Risks :

- ✓ No opportunity to exercise rights
- ✓ Lack of prior information
- ✓ Lack of opportunity to voice an opinion
- ✓ Unequal information (vs equal rights concept)

## Control Objective :

Shareholders should have the right to exercise their rights on the basis of the principle « one share – one vote ».

# The audit program - sample

- Annual General Meeting
  - Control Environment
    - Definition of shareholders' rights and duties

Risks	Control Measures	Field work
No opportunity to exercise rights	Annual General Meeting	Check agenda, invitation, minutes
Lack of prior information	Schedule of matters for decision	Check official documents, minutes
Lack of opportunity to voice an opinion	Able to vote in person or by proxy	Check in internal regulations
Inequal information (vs equal rights concept)	Structures or arrangements ensuring disproportionate control	Check regulations & shareholder agreements

# Audit activities

- Review documents
  - Annual reports
  - Governance charter
  - Organisation chart
  - Bylaws
  - Ethical code
  - Minutes of AGM, Board meetings, Executive meetings
  - Minutes and charter of the Audit Committee
  - Internal regulations of Board & Ex. meetings
  - Strategy documents, strategic analysis, plans
  - General policy documents
  - ...

# Audit activities

- Interviews
  - With Board of Directors (president & members)
  - With Executive Committee (CEO & managers)
  - With Corporate Secretary
  - With staff personnel (legal, compliance, reporting, HR)
  - With secretaries of Board Committees
  - With statutory auditor
  - ...
- Field work
  - Meeting notes
  - Corporate documents : bylaws, registrations...
  - Authorities
  - Decision signatures
  - ...

# Corporate Governance knowledge



# Association of Board members in Belgium (**AB**)



[www.boardmembers.org](http://www.boardmembers.org)

- Objectives
  - Help directors to execute their functions with maximum efficiency
    - in enterprises and associations
    - in the private and the public sector
  - Favour the growth of the enterprises and associations through
    - Professionalism
    - Increased productivity of their Board of Directors



- Creation of an European Confederation of Directors' Association
- Members :
  - IOD – Institute Of Director (UK)
  - AB – Association of Board Members (BE)
  - IFA – Institut Français des Administrateurs (FR)
  - ILA – Institut Luxembourgeois des Administrateurs (LU)
  - Finnish Association of Professional Board Members (FI)
  - Instituto de Consejeros – Administradores (SP)
  - Czech Institute of Directors (CZ)
- influence policies and informing European decision-makers on corporate governance

} Founders



# European Corporate Governance Institute

[www.ecgi.org](http://www.ecgi.org)

- international scientific non-profit association
- undertake, commission and disseminate research on corporate governance
- advise on the formulation of corporate governance policy
- focal point for academics working on corporate governance in Europe



# References

- [www.coso.org](http://www.coso.org)
- [www.sarbanes-oxley.com](http://www.sarbanes-oxley.com)
- [www.corporategovernancecommittee.be](http://www.corporategovernancecommittee.be)
- [www.codebuysse.be](http://www.codebuysse.be)
- [www.itgi.org](http://www.itgi.org)
- [www.theiia.org](http://www.theiia.org)
- [www.ecgi.org](http://www.ecgi.org)
- [www.ecoda.org](http://www.ecoda.org)
- [www.boardmembers.org](http://www.boardmembers.org)

# Corporate Governance under control ?



Patrick Soenen  
qualified audit partners  
Champ des Pétrales, 6  
1332 Genval  
[www.qap.be](http://www.qap.be)  
[p.soenen@qap.be](mailto:p.soenen@qap.be)  
+32.477.75.78.61