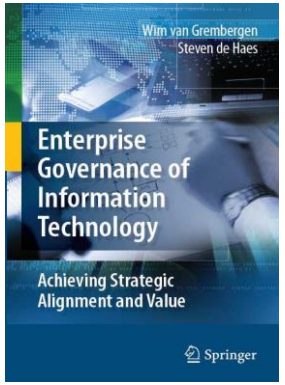
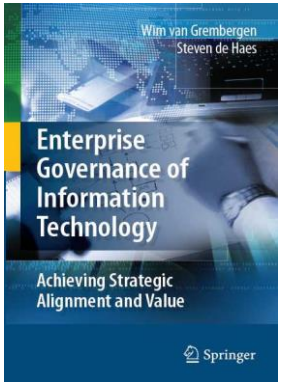


Enterprise Governance of IT

Prof. dr. Wim Van Grembergen

University of Antwerp (UA)
Antwerp Management School (AMS)
IT Alignment and Governance Research Institute (ITAG)

wim.vangrembergen@ua.ac.be



What is IT Governance?

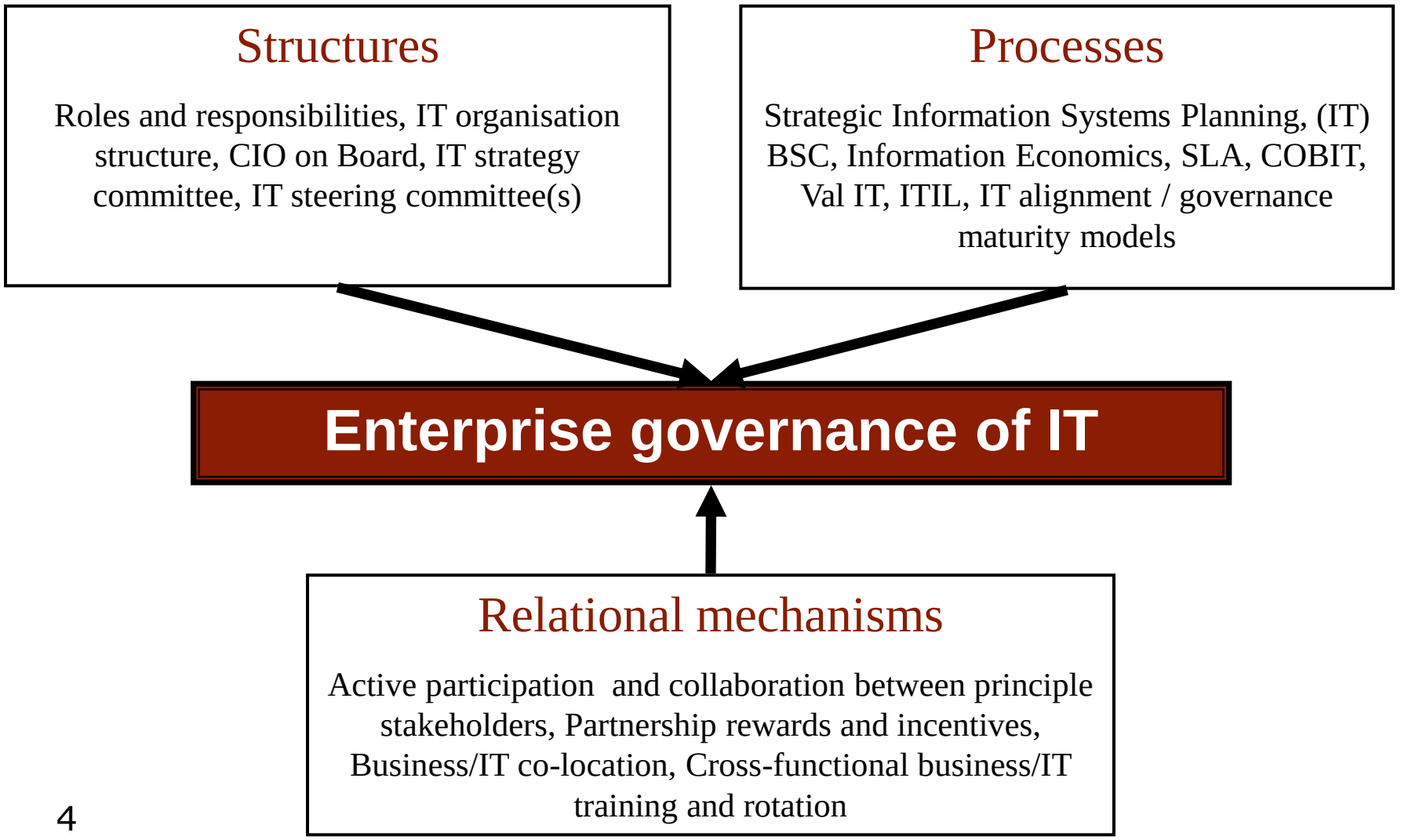
Definition of EGIT

Enterprise Governance of IT (EGIT) is an integral part of enterprise governance exercised by the Board overseeing the definition and implementation of processes, structures and relational mechanisms in the organisation enabling both business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT- enabled business investments.

(Van Grembergen & De Haes, 2009)

3

Structures, processes and relational mechanisms



Delphi research resulted in 33 EGIT practices

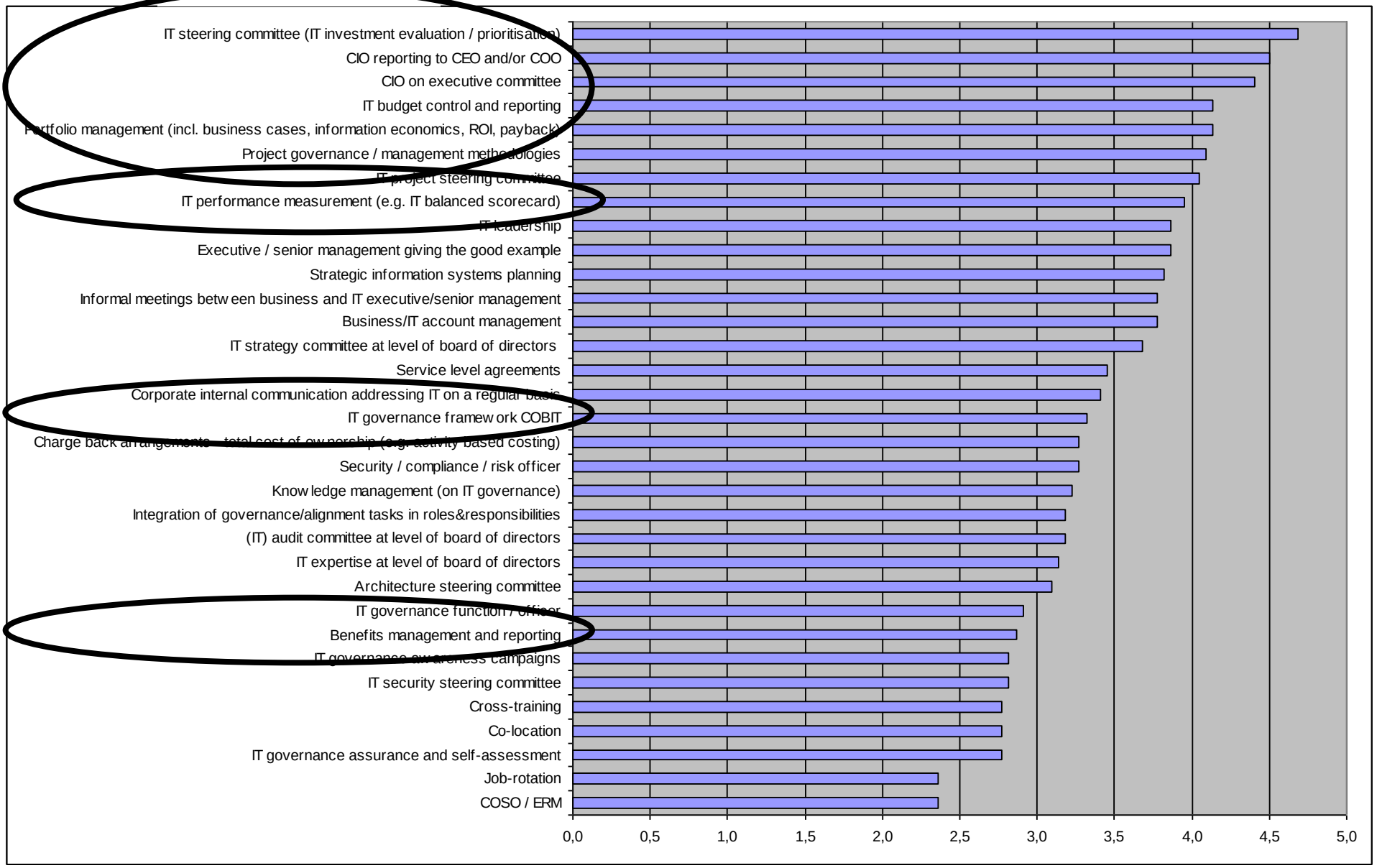
	Index	IT Governance Practice	Definition
IT governance structures	S1	IT strategy committee at level of board of directors	Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors
	S2	IT expertise at level of board of directors	Members of the board of directors have expertise and experience regarding the value and risk of IT
	S3	(IT) audit committee at level of board of directors	Indepent committee at level of board of directors overviewing (IT) assurance activities
	S4	CIO on executive committee	CIO is a full member of the executive committee
	S5	CIO (Chief Information Officer) reporting to CEO (Chief Executive Officer) and/or COO (Chief Operational Officer)	CIO has a direct reporting line to the CEO and/or COO
	S6	IT steering committee (IT investment evaluation / prioritisation at executive / senior management level)	Steering committee at executive or senior [illegible] responsible for determining business priorities in IT investments.
	S7	IT governance function / officer	Function in the organsation responsible for promoting, driving and managing IT governance processes
	S8	Security / compliance / risk officer	Function responsible for security, compliance and/or risk, which possibly impacts IT
	S9	IT project steering committee	Steering committee composed of business and IT people focusing on prioritising and managing IT projects
	S10	IT security steering committee	Steering committee composed of business and IT people focusing on IT related risks and security issues
	S11	Architecture steering committee	Committee composed of business and IT people providing architecture guidelines and advise on their applications.
	S12	Integration of governance/alignment tasks in roles&responsibilities	Documented roles&responsibilities include governance/alignment tasks for business and IT people (cf. Weill)
IT governance processes	P1	Strategic information systems planning	Formal process to define and update the IT strategy
	P2	IT performance measurement (e.g. IT balanced scorecard)	IT performance measurement in domains of corporate contribution, user orientation, operational excellence and future orientation
	P3	Portfolio management (incl. business cases, information economics, ROI, payback)	Prioritisation process for IT investements and projects in which business and IT is involved (incl. business cases)
	P4	Charge back arrangements - total cost of ownership (e.g. activity based costing)	Methodology to charge back IT costs to business units, to enable an understanding of the total cost of ownership
	P5	Service level agreements	Formal agreements between business and IT about IT development projects or IT operations
	P6	IT governance framework COBIT	[illegible] governance and control framework
	P7	IT governance assurance and self-assessment	Regular self-assessments or indepent assurance activities on the governance and control over IT
	P8	Project governance / management methodologies	Processes and methodologies to govern and manage IT projects
	P9	IT budget control and reporting	Processes to control and report upon budgets of IT investments and projects
	P10	Benefits management and reporting	Processes to monitor the planned business benefits during and after implementation of the IT investments / projects.
	P11	COSO / ERM	Framework for internal control
IT governance relational mechanisms	R1	Job-rotation	IT staff working in the business units and business people working in IT
	R2	Co-location	Physically locating business and IT people close to each other
	R3	Cross-training	Training business people about IT and/or training IT people about business
	R4	Knowledge management (on IT governance)	Systems (intranet, …) to share and distribute knowledge about IT governance framework, responsibilities, tasks, etc.
	R5	Business/IT account management	Bridging the gap between business and IT by means of account managers who act as in-between
	R6	Executive / senior management [illegible]	Se[illegible]artners"
	R7	Informal meetings between business and IT executive/senior management	Informal meetings, with no agenda, where business and IT senior management talk about general activities, directions, etc. (eg. during informal lunches)
	R8	IT leadership	Ability of CIO or similar role to articulate a vision for IT's role in the company and ensure that this vision is clearly understood by managers throughout the organisation
	R9	Corporate internal communication addressing IT on a regular basis	Internal corporate communication regularly addresses general IT issues.
	R10	IT governance awareness campaigns	Campaigns to explain to business and IT people the need for IT governance

12 structures

11 processes

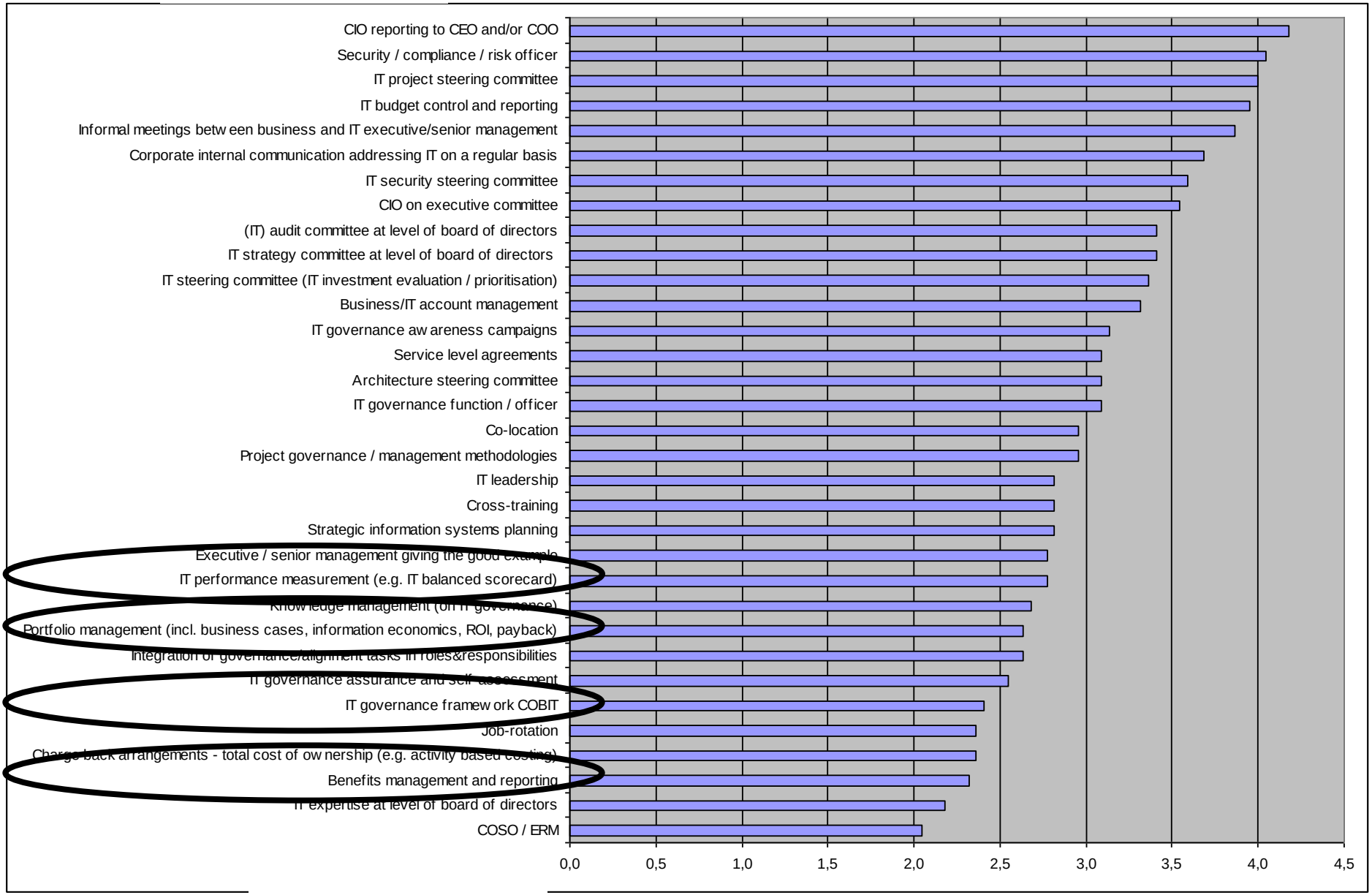
10 relational mechanisms

Perceived effectiveness of EGIT practices

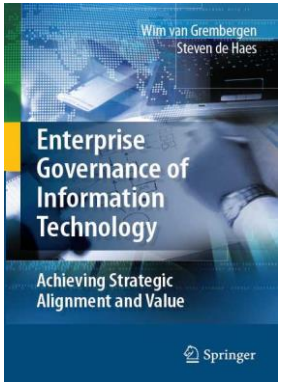


0 = not effective, 5 = very effective

Perceived ease of implementation of EGIT practices



0 = not easy to implement,,
5 = very easy to implement



Examples structures & processes

Example structure: IT Steering Committee

A group of senior executives appointed by the board to ensure that the board is involved in and kept informed of major IT-related matters and decisions. **The committee is accountable for managing the portfolio of IT-enabled investments**, IT services and IT assets, ensuring that value is delivered and risks are managed.

9

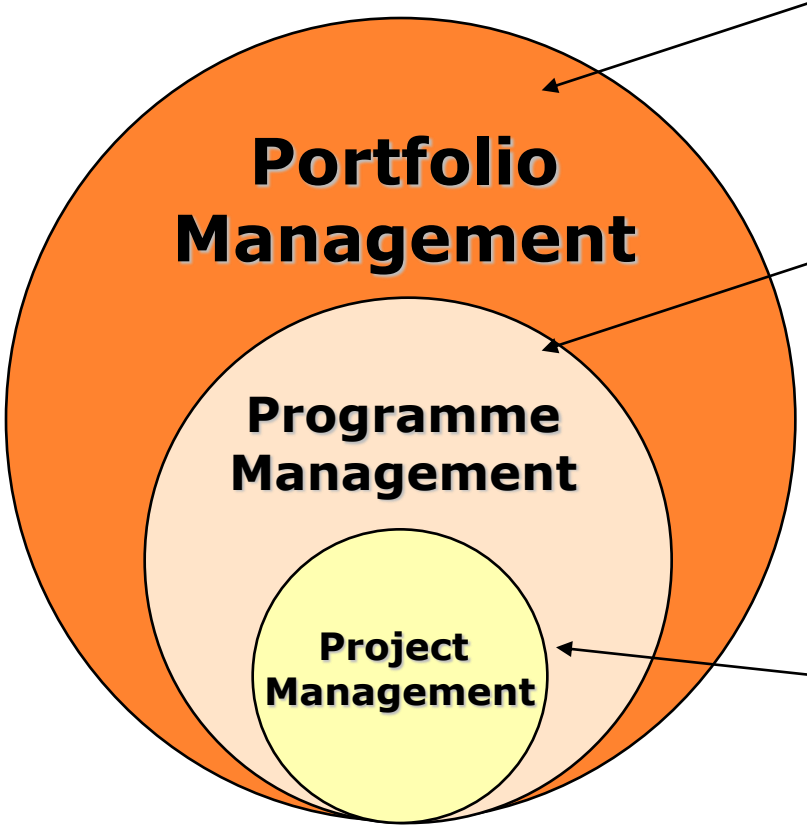
Example structure: IT Steering Committee

- **Mandate**: ensuring business value from IT-enabled investments
- **Span of Control**: servicing the entire business/IT entity for which the board is responsible
- **Delegation Rights**: delegating authority to executive management to carry out its decisions
- **Escalation Rights**: escalating all key issues and findings impacting the board
- **Authority Level/Decision Rights**: the Committee is responsible for the prioritisation and selecting the IT portfolio
- **Operating Principles**:
  - The Committee should meet at least quarterly. More frequent meetings may be scheduled depending on the need
  - Regular reporting to the board.
  - Minutes of meetings should be kept and approved in a timely manner

10

Example process: IT Portfolio Management

Value – the end business outcome expected from an IT-enabled business investment where such outcomes may be financial, non-financial or a combination of the two.

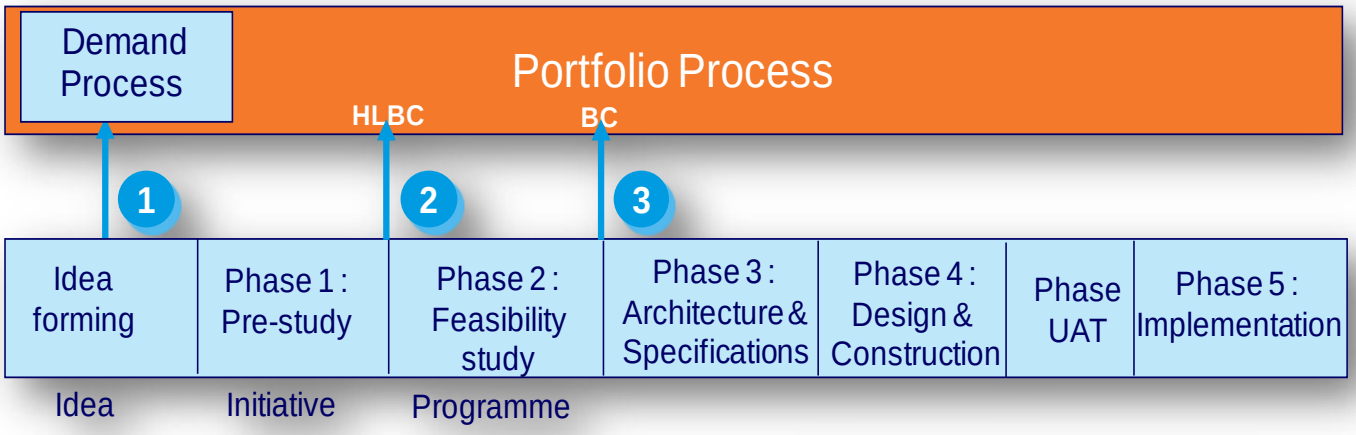


Portfolio – a suite of business programmes managed to optimise overall **enterprise value**

Programme – a structured grouping of projects that are both necessary and sufficient to achieve a business outcome and deliver value, including business change management, business processes, people, etc. (primary unit of investment within VALIT)

Project – a structured set of activities concerned with delivering a defined **capability** based on an agreed schedule and budget (that is necessary but not sufficient to achieve a required business outcome)

Portfolio Management



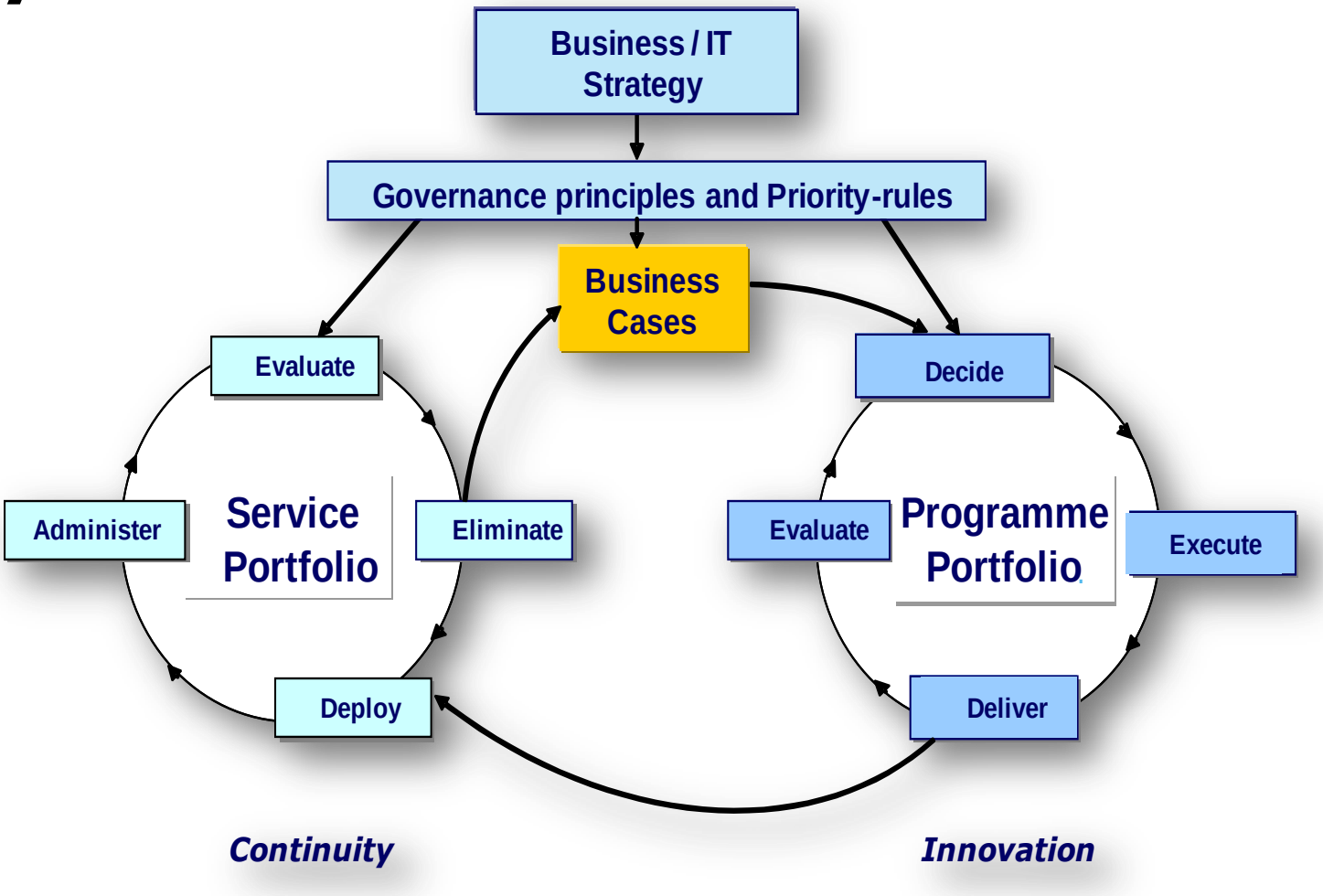
Three approval steps :

1. Approval 1: **Business ideas selection**
2. Approval 2: **Programme Go**
3. Approval 3: **Investment approval**

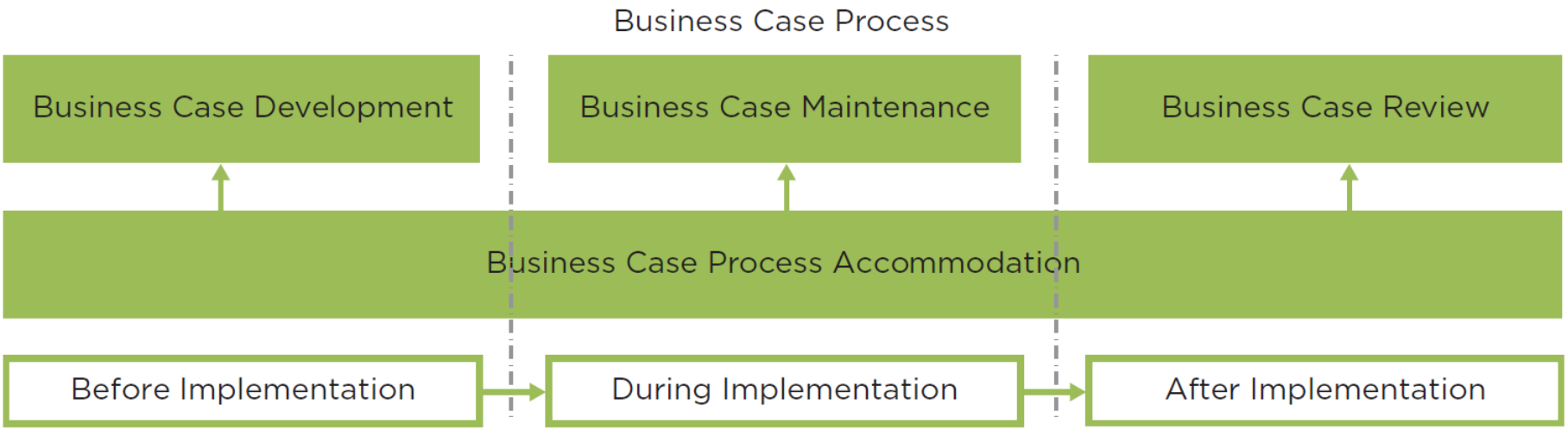
Three decision thresholds:

	Business	BIC	EC
> 5M€	1 2 3	2 3	3
> 500 k€	1 2 3	2 3	
> 150 k€	1 2 3		

Example: KLM - Innovation Continuity Bicycle



Example:
Business Case Process



A BUSINESS CASE is a formal investment document with a structured overview of relevant information that provides a rationale and justification of an investment with the intent to enable well-founded investment decision-making.

A BUSINESS CASE PROCES is a set of logically related tasks that affect a business case and supports continuous business case usage with the intent to enable well-founded investment decision-making and to ultimately increase investment success.

Example process: IT Balanced Scorecard (BSC)

USER ORIENTATION

How do users view the IT department?

Mission

To be the preferred supplier of information systems.

Objectives

- Preferred supplier of applications
- Preferred supplier of operations vs. proposer of best solution, from whatever source
- Partnership with users
- User satisfaction

The *Business Contribution* perspective captures the business value created from the IT investments.

BUSINESS CONTRIBUTION

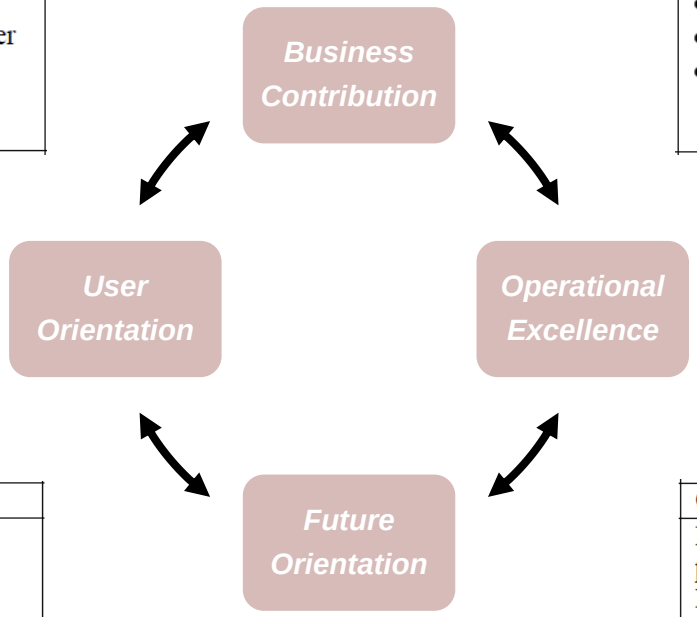
How does management view the IT department?

Mission

To obtain a reasonable business contribution from IT investments.

Objectives

- Control of IT expenses
- Business value of IT projects
- Provision of new business capabilities



The *User Orientation* perspective represents the user evaluation of IT.

The *Operational Excellence* perspective represents the IT processes employed to develop and deliver the applications.

FUTURE ORIENTATION

How well is IT positioned to meet future needs?

Mission

To develop opportunities to answer future challenges.

Objectives

- Training and education of IT staff
- Expertise of IT staff
- Research into emerging technologies
- Age of application portfolio

The *Future Orientation* perspective represents the human and technology resources needed by IT to deliver its services over time.

OPERATIONAL EXCELLENCE

How effective and efficient are the IT processes?

Mission

To deliver effective and efficient IT applications and services.

Objectives

- Efficient and effective developments
- Efficient and effective operations

16

IT Balanced scorecard

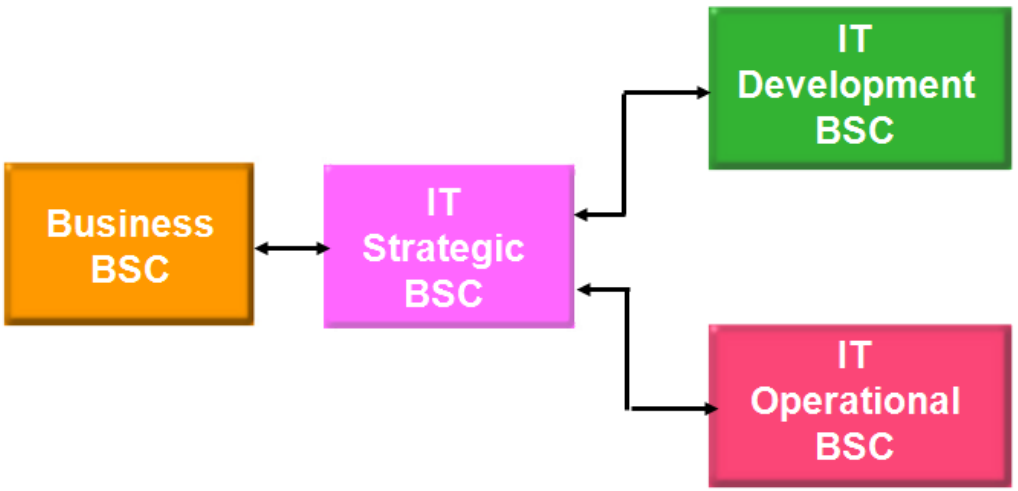
- **Key Goal Indicator** (KGI) - is defined as a measure of *what* has to be accomplished.
- **Key Performance Indicator** (KPI) - measures of *how well* the process is performing.

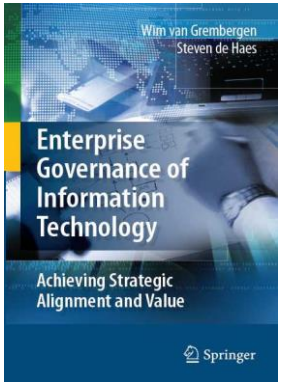
KGI	*KPI*
E:G: Lines of code per Person index of user satisfaction	E.g. Number of educational days response time of help desk

---

Balanced Scorecards Cascade:

The IT Development BSC and the IT Operational BSC both are enablers of the IT Strategic BSC that in turn is the enabler of the Business BSC.





Relationship EGIT – Business/IT alignment

IT Governance assessment

	Organisation						
	Maturity						Rationale
IT strategy committee at level of board of directors	0	1	2	3	4	5	
IT expertise at level of board of directors	0	1	2	3	4	5	
(IT) audit committee at level of board of directors	0	1	2	3	4	5	
CIO on executive committee	0	1	2	3	4	5	
CIO reporting to CEO and/or COO	0	1	2	3	4	5	
IT steering committee (IT investment evaluation / prioritisation at executive / senior management level)	0	1	2	3	4	5	
IT governance function / officer	0	1	2	3	4	5	
Security / compliance / risk officer	0	1	2	3	4	5	
IT project steering committee	0	1	2	3	4	5	
IT security steering committee	0	1	2	3	4	5	
Architecture steering committee	0	1	2	3	4	5	
Integration of governance/alignment tasks in roles&responsibilities	0	1	2	3	4	5	
Strategic information systems planning	0	1	2	3	4	5	
IT performance measurement (e.g. IT balanced scorecard)	0	1	2	3	4	5	
Portfolio management (incl. business cases, information economics, ROI, payback)	0	1	2	3	4	5	
Charge back arrangements - total cost of ownership (e.g. activity based costing)	0	1	2	3	4	5	
Service level agreements	0	1	2	3	4	5	
IT governance framework COBIT	0	1	2	3	4	5	
IT governance assurance and self-assessment	0	1	2	3	4	5	
Project governance / management methodologies	0	1	2	3	4	5	
IT budget control and reporting	0	1	2	3	4	5	
Benefits management and reporting	0	1	2	3	4	5	
COSO / ERM	0	1	2	3	4	5	
Job-rotation	0	1	2	3	4	5	
Co-location	0	1	2	3	4	5	
Cross-training	0	1	2	3	4	5	
Knowledge management (on IT governance)	0	1	2	3	4	5	
Business/IT account management	0	1	2	3	4	5	
Executive / senior management giving the good example	0	1	2	3	4	5	
Informal meetings between business and IT executive/senior management	0	1	2	3	4	5	
IT leadership	0	1	2	3	4	5	
Corporate internal communication addressing IT on a regular basis	0	1	2	3	4	5	
IT governance awareness campaigns	0	1	2	3	4	5	
Other practices							
General remarks							

Business/IT alignment

Business/IT alignment refers to applying IT in an appropriate and timely way in harmony with business strategies. It addresses how:

1. IT is aligned with the business
2. The business should or could be aligned with IT.

Jerry Luftman's assessment of business/IT alignment maturity.

Business/IT maturity assessment (Jerry Luftman)

IT is perceived by the business as:

1. A cost of doing business
2. Emerging as an asset
3. A fundamental enabler of future business activity
4. A fundamental driver of future business activity
5. A partner for the business that co-adapts/improvises in bringing value to the firm
6. N/A or don't know

The following statements are about the IT and business relationship and trust.

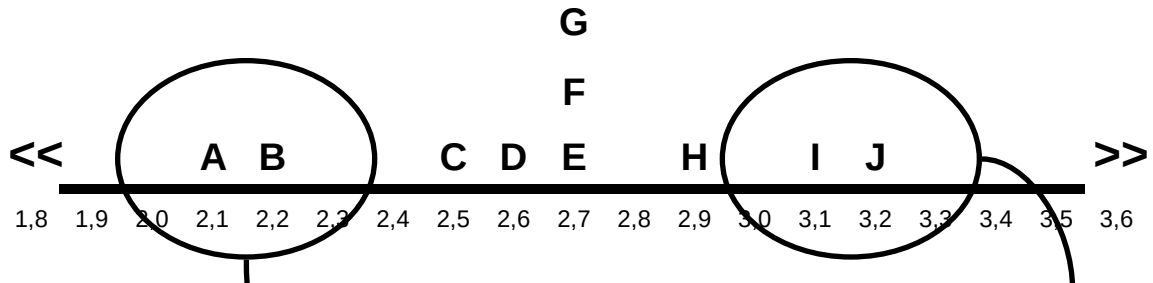
1. There is a sense of conflict and mistrust between IT and the business.
2. The association is primarily an "arm's length" transactional style of relationship.
3. IT is emerging as a valued service provider.
4. The association is primarily a long-term partnership style of relationship.
5. The association is a long-term partnership and valued service provider.
6. N/A or don't know

The following statements are about the cultural locus of power in making IT-based decisions. Our important IT decisions are made by:

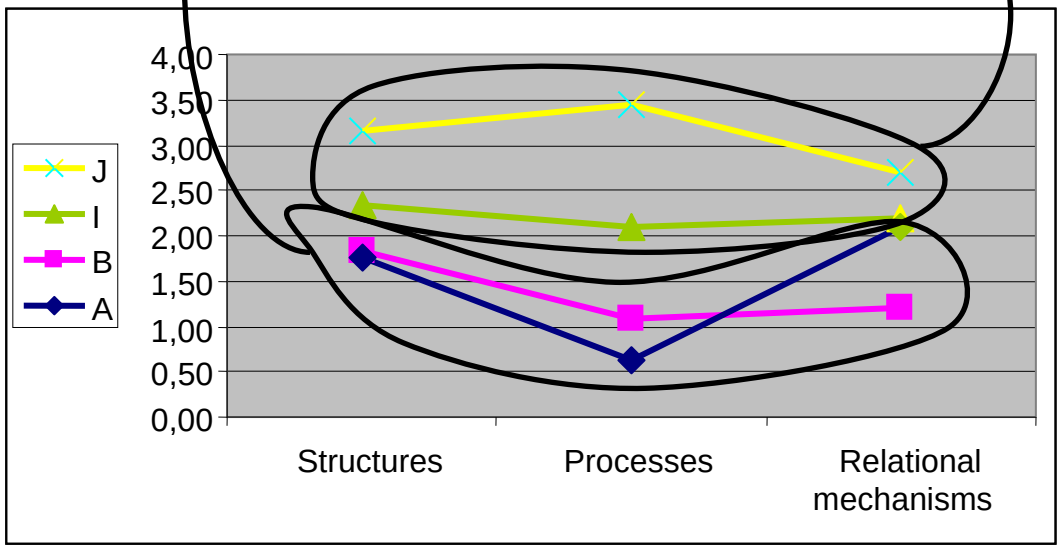
1. Top business management or IT management at the corporate level only
2. Top business or IT management at corporate level with emerging functional unit level influence
3. Top business management at corporate and functional unit levels, with emerging shared influence from IT management
4. Top management (business and IT) across the organization and emerging influence from our business partners/alliances.
5. Top management across the organization with equal influence from our business partners/alliances.
6. N/A or don't know

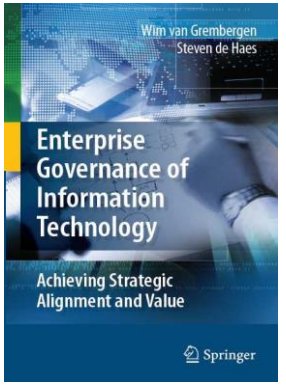
The relationship between EGIT and business/IT alignment

Business/IT alignment maturity



Maturity of IT governance practices





COBIT 5 framework for EGIT

Synopsis:

COBIT 5 brings together **five principles** that allow the enterprise to build an effective **governance and management** framework based on a holistic set of **seven enablers** that optimises information and technology investment and use for the benefit of stakeholders.

24

1. Meet Stakeholder Needs

Synopsis:

- Stakeholder needs have to be transformed into an enterprise's actionable strategy.
- The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals.

25

2. Covering the Enterprise End-to-end RACI

EDM02 RACI Chart

Key Governance Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
EDM02.01 Evaluate value optimisation.	A	R	R	C	R		R			C	C		C	C	C	C	C	R	C	C	C					
EDM02.02 Direct value optimisation.	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM02.03 Monitor value optimisation.	A	R	R	C	R		R			R	C	C	C	C	C	C	C	R	C	C	C					

3. Applying a Single Integrated Framework

COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:

- Enterprise: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
- IT-related: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI, etc.

- This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
- ISACA plans a capability to facilitate COBIT user mapping of practices and activities to third-party references.

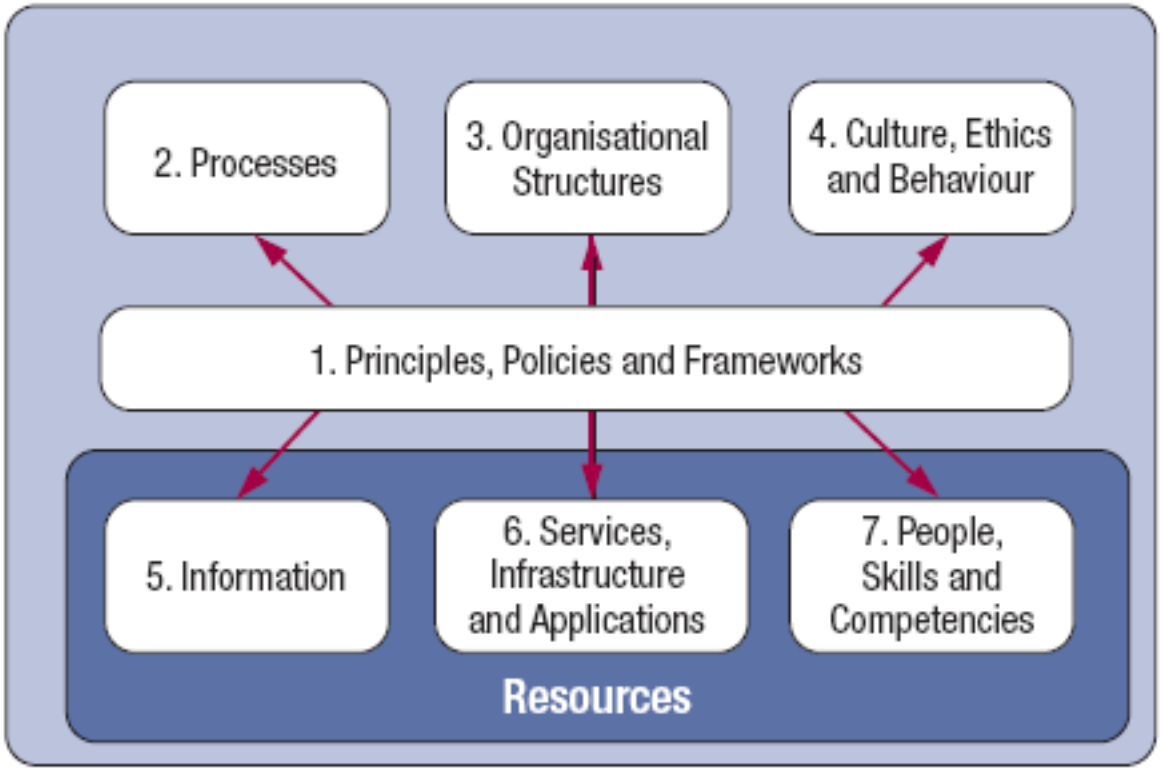
27

4. Enabling a Holistic Approach (Enablers)

Synopsis:

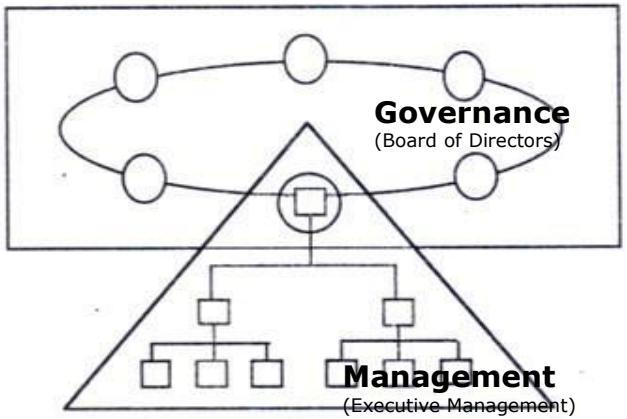
COBIT 5 has 7 enablers:

- Factors that, individually and collectively, influence whether something will work - in the case of COBIT, governance and management over enterprise IT
- Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve
- Described by the COBIT 5 framework in seven categories



5. Separating Governance From Management

- The COBIT 5 framework makes a clear distinction between Governance and Management.
- These two disciplines:
  - Encompass different types of activities.
  - Require different organisational structures.

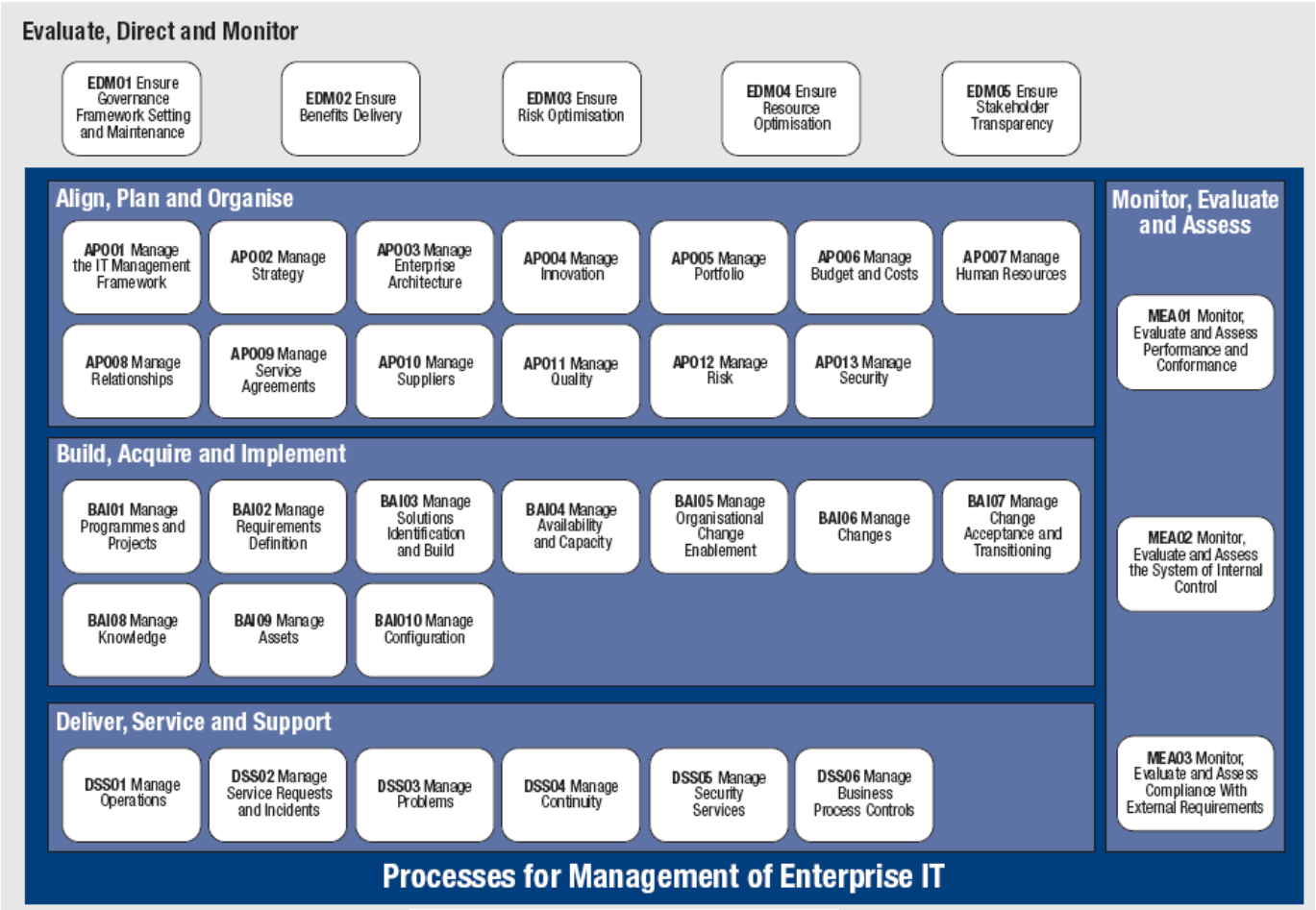


- **Governance:** In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
- **Management:** In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.

Synopsis:

37 Processes:

- EDM – Governance Processes
- APO, BAI & DSS – Management Processes



Source: COBIT® 5, figure 16. © 2012 ISACA®

30

Governance versus Management

antwerp management school

Example Governance Process

EDM01	Set and Maintain the Governance Framework	Area: Governance
		Domain: Evaluate, Direct and Monitor

Process Description

Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Process Purpose Statement

The process purpose is to embed an effective governance system for IT in the enterprise.

Governance versus Management

Example Governance Process + key management practices

Ref	Governance Practice
EDM01.01	**Evaluate design of enterprise governance of IT** Continually identify and engage with the enterprise's stakeholders and document an understanding of the requirements and make judgement on the current and future design of governance of enterprise IT.
EDM01.02	**Direct the Governance System** Establish informed leadership and obtain their support, buy-in and commitment. Establishment the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision-making.
EDM01.03	**Monitor the Governance System** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

Governance versus Management

antwerp management school

Ref	Governance Practice
EDM01.01	**Evaluate design of enterprise governance of IT** Continually identify and engage with the enterprise's stakeholders and document an understanding of the requirements and make judgement on the current and future design of governance of enterprise IT.

Activities

1 Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.

2 Determine the significance of IT and its role with respect to the business.

3 Consider external regulations, laws and contractual obligations and determine how they should apply within the enterprise governance of IT.

4 Determine the implications of the overall enterprise control environment with regards to IT.

5 Articulate principles that will guide the design of governance and decision making of IT.

6 Understand the enterprise's decision making culture and determine the optimal decision making model for IT.

7 Determine the right levels of authority delegation, including threshold rules, for IT decisions.

Governance versus Management

antwerp management school

Governance Practice

EDM01.02 Direct the governance system.

Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making.

Activities

1 Communicate governance of IT principles and agree with executive management on the way forward to establish informed and committed leadership.

2 Establish or delegate the establishment of governance structures, processes and practices in line with agreed-upon design principles.

3 Allocate responsibility, authority and accountability in line with agreed-upon governance design principles, decision-making models and delegation.

4 Ensure that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information.

5 Direct that staff follow relevant guidelines for ethical and professional behaviour and ensure that consequences of non-compliance are known and enforced.

6 Direct the establishment of a reward system to promote desirable cultural change.

Governance versus Management

antwerp management school

Governance Practice

EDM01.03 Monitor the governance system.

Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

Activities

1 Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT.

2 Periodically assess whether agreed governance of IT mechanisms (structures, principles, processes, etc.) are established and operating effectively.

3 Assess the effectiveness of the governance design and identify actions to rectify any deviations found.

4 Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.

5 Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.

6 Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.

The knowing-doing gap

- While organisations do recognise EGIT's importance, they are still struggling with getting such governance practices implemented and embedded into their organisations ('knowing-doing gap')
- Need for an organizational system, i.e. "the way a firm gets its people to work together to carry out the business". (De Wit and Meyer, 2005).

More information

- IT Alignment and Governance Research Institute
  - www.antwerpmanagementschool.be/ITAG
- Email
  - wim.vangrembergen@ua.ac.be
- Books & Publications
  - Van Grembergen W., De Haes S., Implementing Information Technology Governance: models, practices and cases, 255p., IGI Publishing, 2008
  - Van Grembergen W., De Haes S., Enterprise Governance of IT: achieving strategic alignment and value, 360p., Springer, 2009
  - International Journal on IT/Business Alignment and Governance (IJITBAG)
    www.igi-global.com/IJITBAG
- Executive education
  - Executive Master in IT Governance & Assurance
  - Executive Master in Enterprise IT Architecture