S5: Enterprise Governance of IT COBIT 5

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

Reseña curricular del autor:

- Wim Van Grembergen is professor at the Economics and Management Faculty of the University of Antwerp (UA)
- Executive professor at the Antwerp Management School (AMS)
- Teaches information systems at master and executive level
- Researches in IT governance within his *IT Alignment and Governance (ITAG) Research Institute*
- Most recent book *"Enterprise governance of IT. Achieving strategic alignment and value"* (Springer, New York)
- Has been involved in the development of COBIT 4, VAL IT and COBIT 5
- Frequent speaker speaker at academic, professional meetings and conferences
- Has served in a consulting capacity to a number of organisations

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Índice

1. **Enterprise Governance of IT**
2. Enterprise Governance of IT practices
3. Enterprise Governance of IT as enabler for business / IT alignment
4. Enterprise Governance of IT as enabler for business value
5. COBIT 5

Setting the scene

"Firms with superior IT governance have at least 20% higher profits...than firms with poor governance given the same strategic objectives."

(Louis Boyle, VP Gartner EXP, 2006)

IT governance definitions

IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensuring the fusion of business and IT.
(Van Grembergen, 2002)

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.
(IT Governance Institute, 2001)

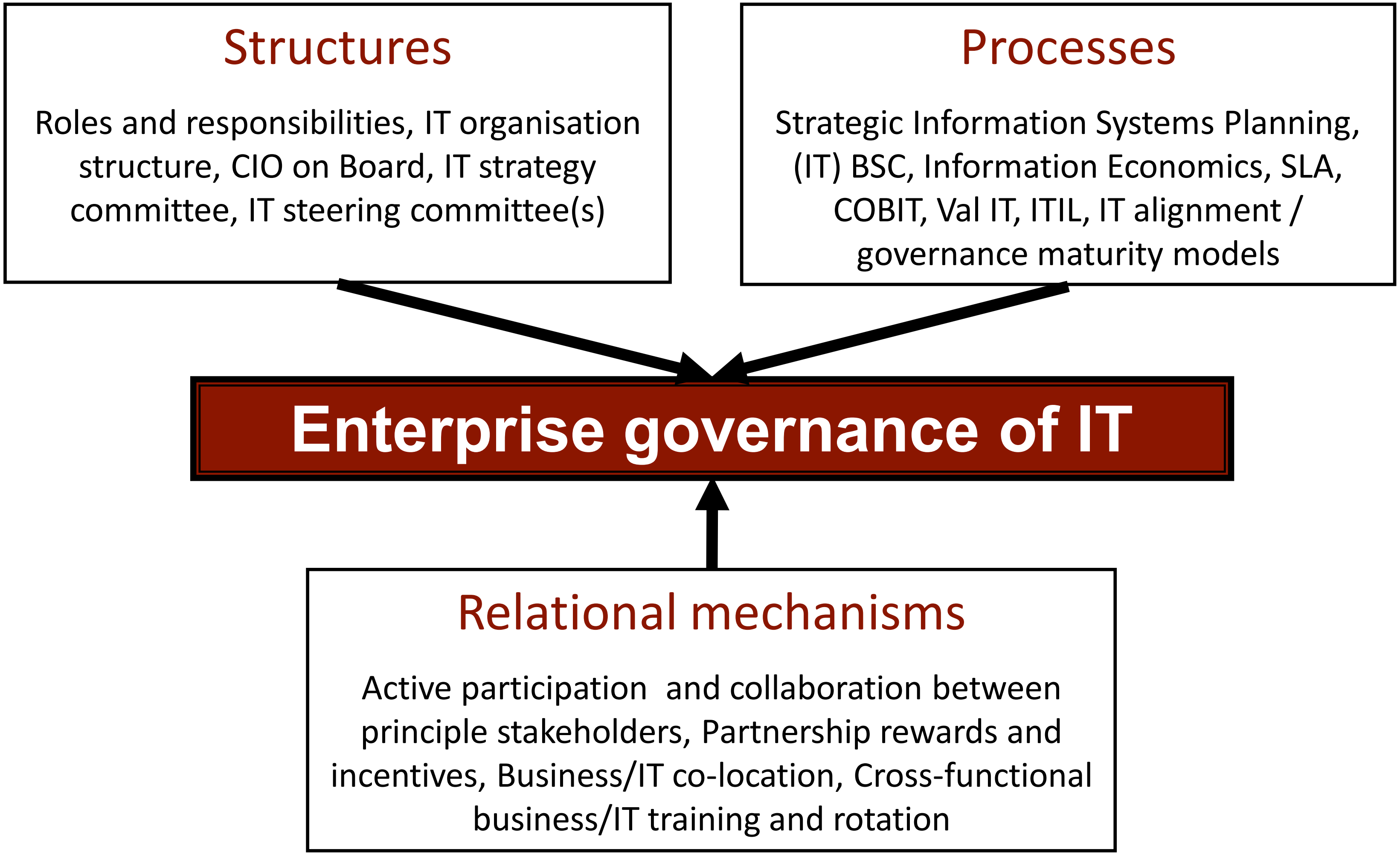
Moving to Enterprise Governance of IT

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)

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Structures, processes and relational mechanisms



Structures

Roles and responsibilities, IT organisation structure, CIO on Board, IT strategy committee, IT steering committee(s)

Processes

Strategic Information Systems Planning, (IT) BSC, Information Economics, SLA, COBIT, Val IT, ITIL, IT alignment / governance maturity models

Enterprise governance of IT

Relational mechanisms

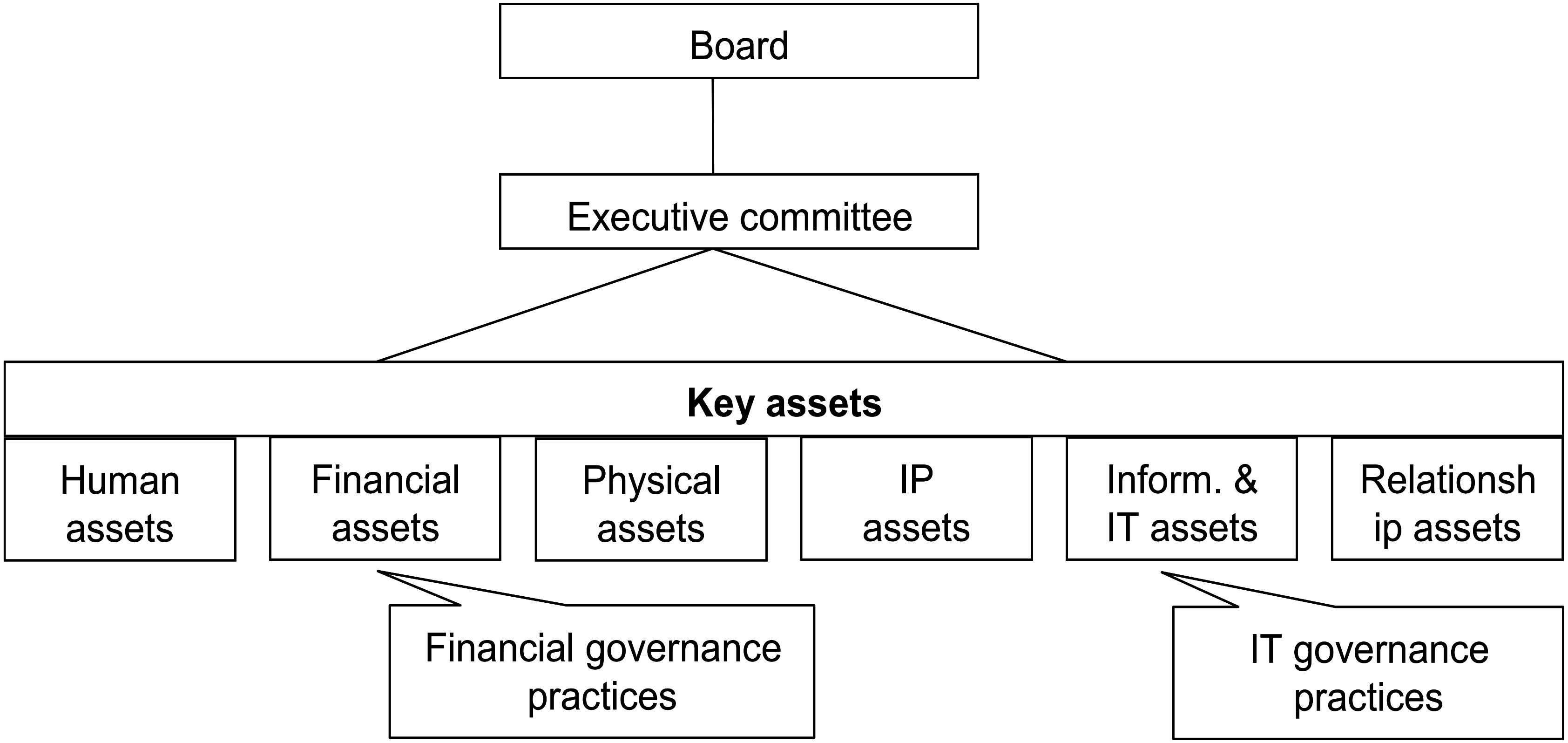
Active participation and collaboration between principle stakeholders, Partnership rewards and incentives, Business/IT co-location, Cross-functional business/IT training and rotation

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).

Key assets governance



ISO/IEC 38500 (2008): Corporate governance of information technology

Scope

- This standard provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.

- This standard applies to the governance of management processes (and decisions) relating to the information and communication services used by an organization. These processes could be controlled by IT specialists within the organization or external service providers, or by business units within the organization

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

ISO/IEC 38500 (2008): Principles for Enterprise Governance of IT

Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy

The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.

Principle 3: Acquisition

IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Principle 4: Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Principle 5: Conformance

IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behaviour

IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

ISO/IEC 38500 (2008): Corporate governance of information technology

Model

Directors should govern IT through three main tasks:

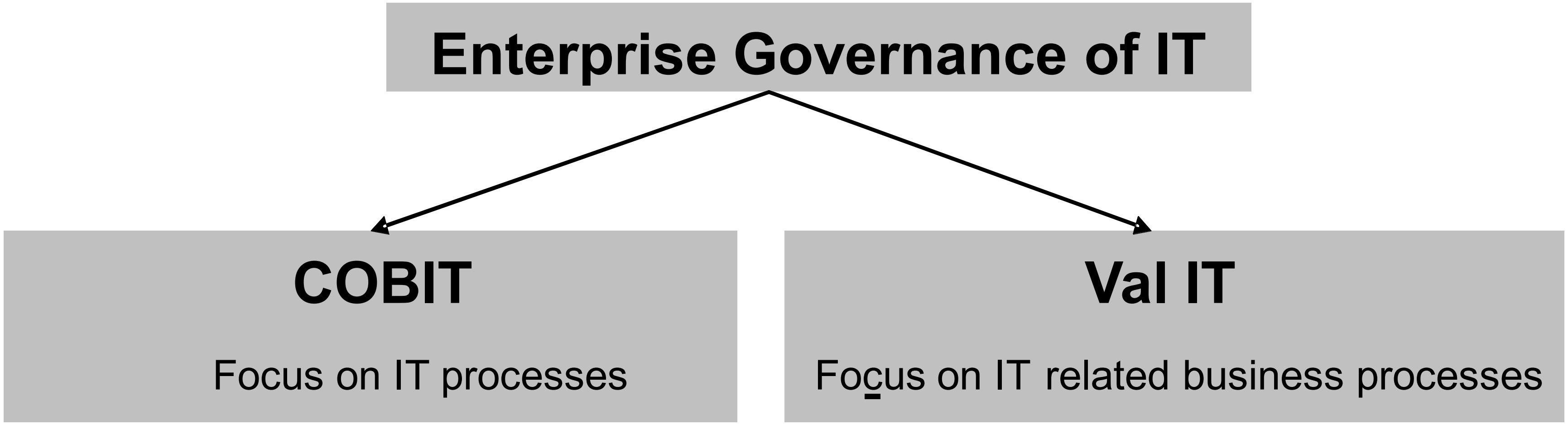
a) Evaluate the current and future use of IT.

b) Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.

c) Monitor conformance to policies, and performance against the plans.

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

COBIT and VAL IT as frameworks for Enterprise Governance of IT



Enterprise Governance of IT

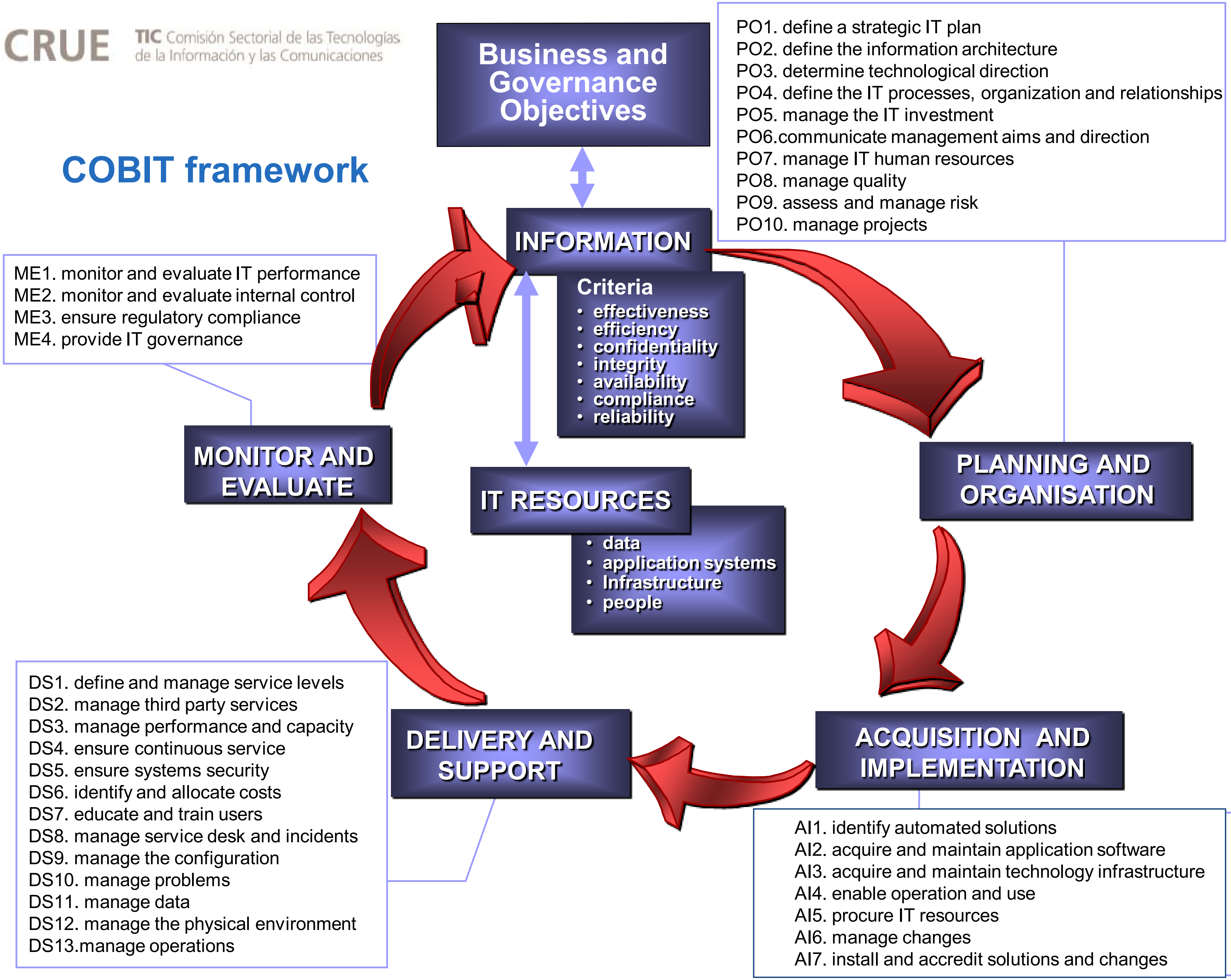
COBIT

Focus on IT processes

Val IT

Focus on IT related business processes

COBIT framework



Business and Governance Objectives

INFORMATION

Criteria
- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

IT RESOURCES
- data
- application systems
- Infrastructure
- people

PLANNING AND ORGANISATION

PO1. define a strategic IT plan
PO2. define the information architecture
PO3. determine technological direction
PO4. define the IT processes, organization and relationships
PO5. manage the IT investment
PO6.communicate management aims and direction
PO7. manage IT human resources
PO8. manage quality
PO9. assess and manage risk
PO10. manage projects

ACQUISITION AND IMPLEMENTATION

AI1. identify automated solutions
AI2. acquire and maintain application software
AI3. acquire and maintain technology infrastructure
AI4. enable operation and use
AI5. procure IT resources
AI6. manage changes
AI7. install and accredit solutions and changes

DELIVERY AND SUPPORT

DS1. define and manage service levels
DS2. manage third party services
DS3. manage performance and capacity
DS4. ensure continuous service
DS5. ensure systems security
DS6. identify and allocate costs
DS7. educate and train users
DS8. manage service desk and incidents
DS9. manage the configuration
DS10. manage problems
DS11. manage data
DS12. manage the physical environment
DS13.manage operations

MONITOR AND EVALUATE

ME1. monitor and evaluate IT performance
ME2. monitor and evaluate internal control
ME3. ensure regulatory compliance
ME4. provide IT governance

Example: Detailed Control Objectives for Manage Changes (AI6)

AI6.1 Change Standards and Procedures
Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 Impact Assessment, Prioritisation and Authorisation
Ensure that all requests for change are assessed in a structured way for impacts on the operational system and its functionality. This assessment should include categorisation and prioritisation of changes. Prior to migration to production, changes are authorized by the appropriate stakeholder.

AI6.3 Emergency Changes
Establish a process for defining, raising, assessing and authorising emergency changes that do not follow the established change process. Documentation and testing should be performed, possibly after implementation of the emergency change.

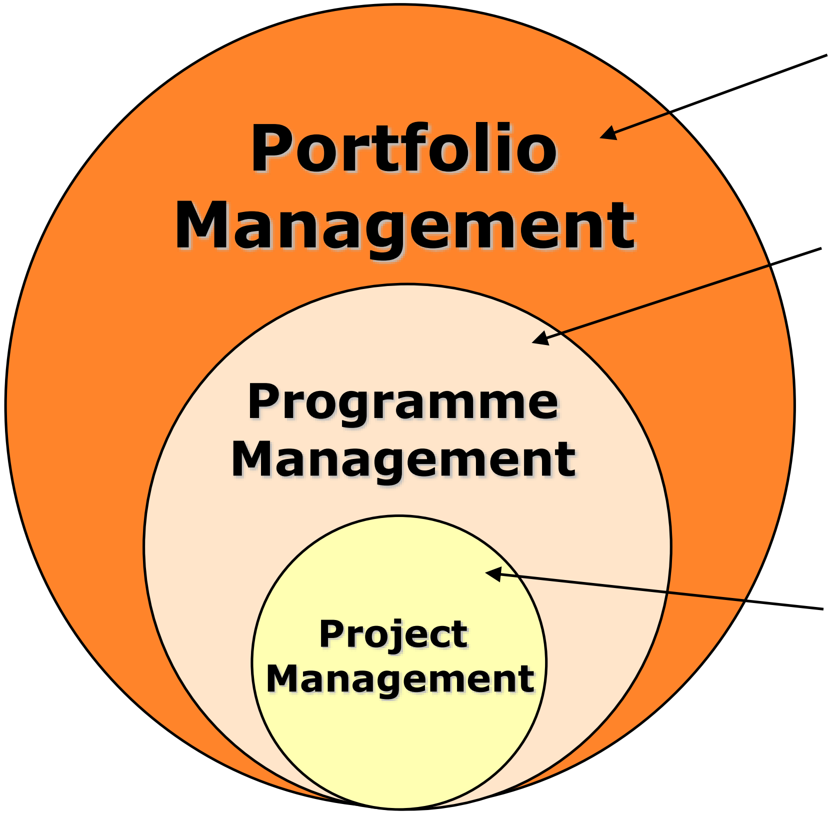
AI6.4 Change Status Tracking and Reporting
Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.5 Change Closure and Documentation
Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Val IT: Projects, Programmes, Portfolios and Value

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.



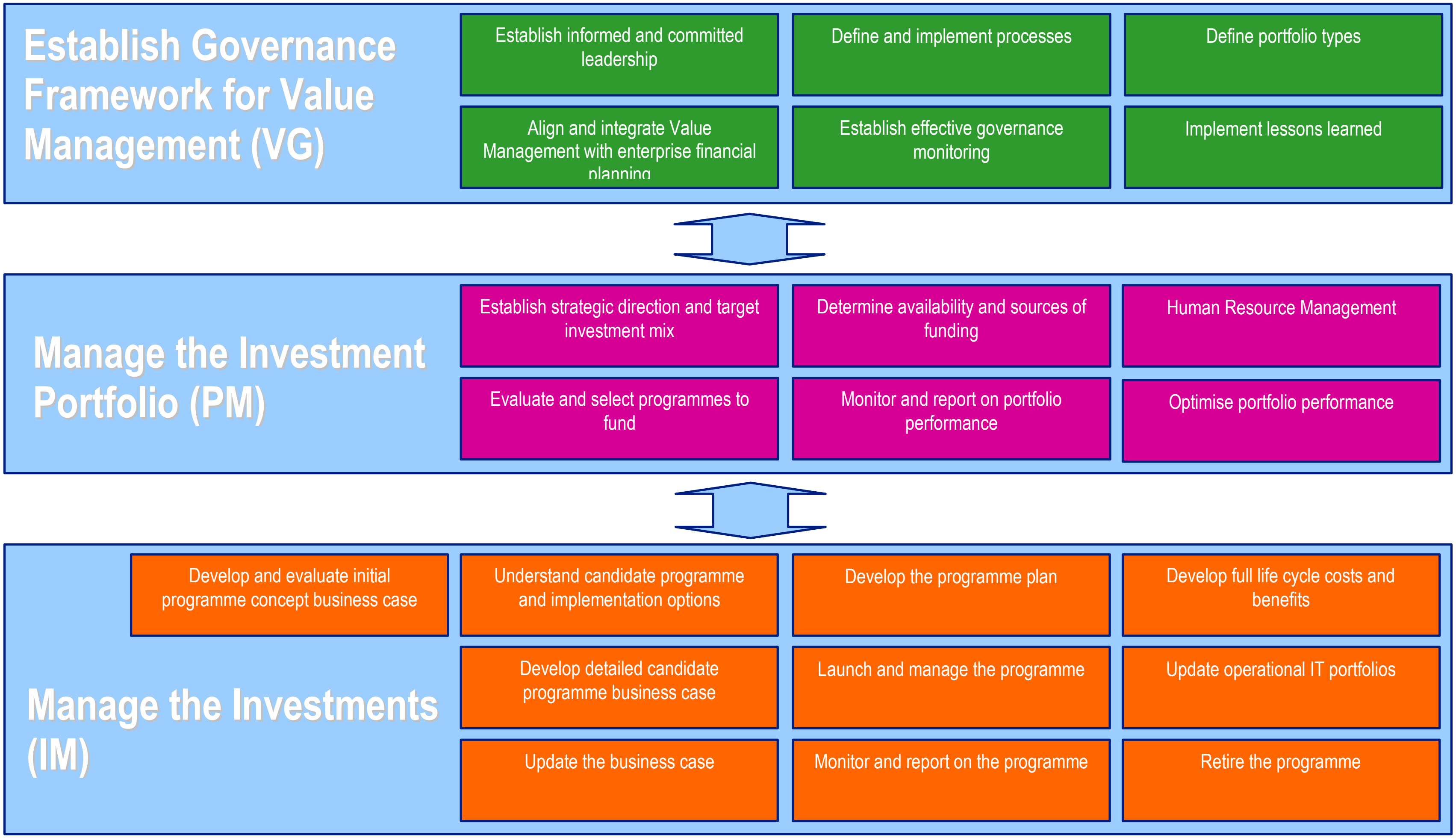
Portfolio – a suite of business programmes managed to optimise overall **enterprise value**

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)

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Val IT: Relationship between Processes & Practices



Establish Governance Framework for Value Management (VG)

- Establish informed and committed leadership
- Define and implement processes
- Define portfolio types
- Align and integrate Value Management with enterprise financial planning
- Establish effective governance monitoring
- Implement lessons learned

Manage the Investment Portfolio (PM)

- Establish strategic direction and target investment mix
- Determine availability and sources of funding
- Human Resource Management
- Evaluate and select programmes to fund
- Monitor and report on portfolio performance
- Optimise portfolio performance

Manage the Investments (IM)

- Develop and evaluate initial programme concept business case
- Understand candidate programme and implementation options
- Develop the programme plan
- Develop full life cycle costs and benefits
- Develop detailed candidate programme business case
- Launch and manage the programme
- Update operational IT portfolios
- Update the business case
- Monitor and report on the programme
- Retire the programme

Relational mechanisms *(Peterson, 2003)*

Effective communications and knowledge sharing

- **Active participation and collaboration of principle stakeholders**
- **Partnership rewards and incentives**
- **Business/IT collocation**
- **Cross-functional business/IT training and job rotation**
- **IT leadership**
- **…**

Índice

1. Enterprise Governance of IT
2. Enterprise Governance of IT practices
3. Enterprise Governance of IT as enabler for business / IT alignment
4. Enterprise Governance of IT as enabler for business value
5. COBIT 5

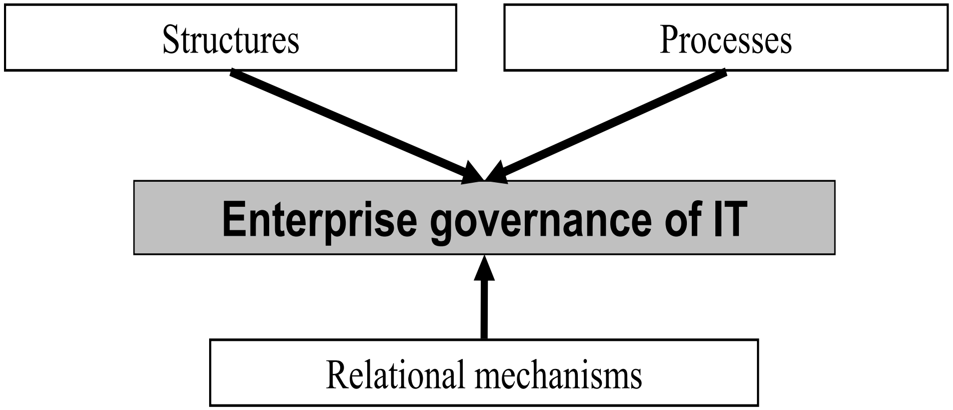
Implementation of EGIT in practice

Requires:

A holistic set of

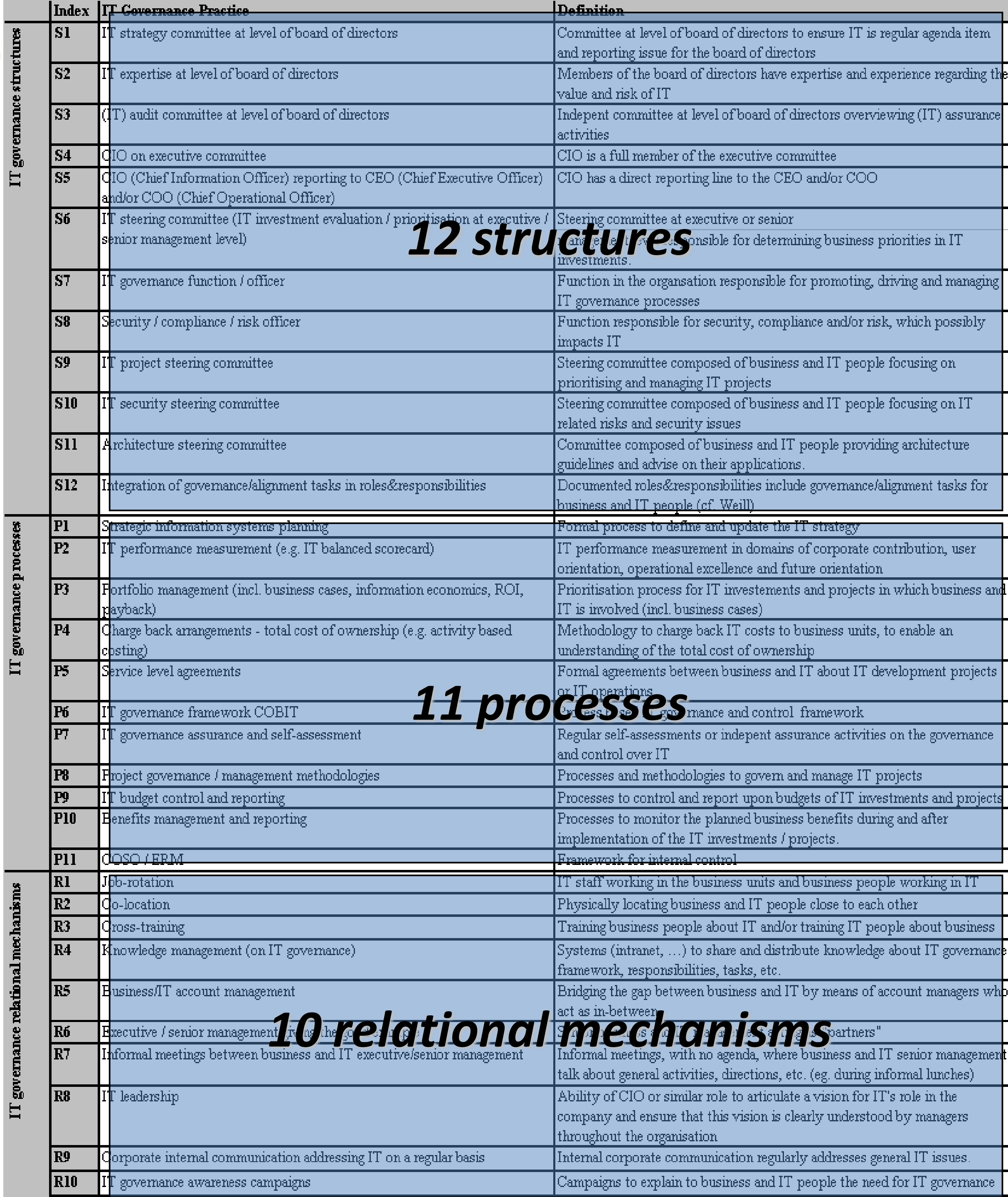
- **Governance Processes**
- **Structures**
- **Relational Mechanisms**

at all 3 layers of the organization.



Implementation…

"a list of 33 EGIT practices based on delphi research"



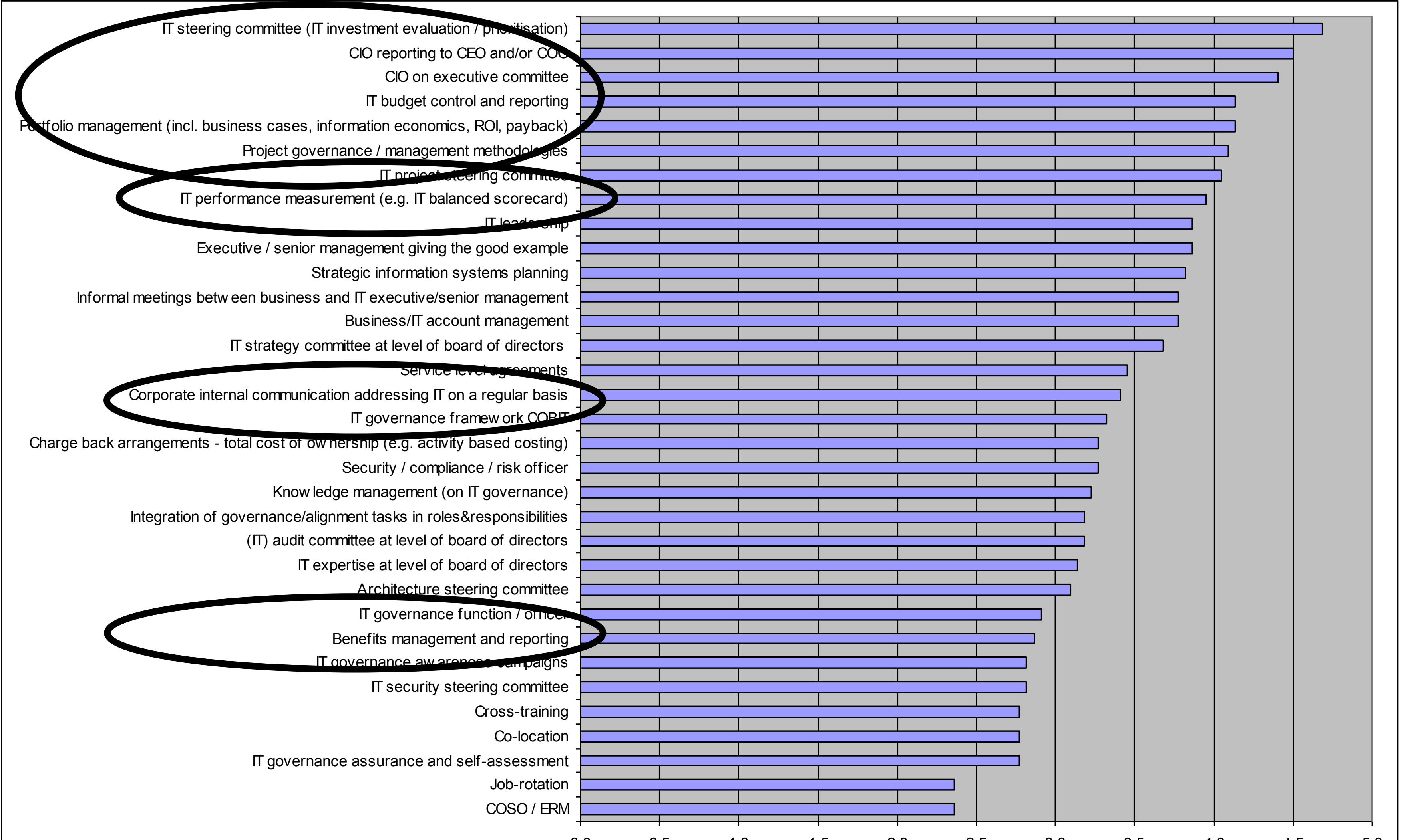
	Index	IT Governance Practice	Definition
IT governance structures	S1	IT strategy committee at level of board of directors	Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors
	S2	IT expertise at level of board of directors	Members 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 management level 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	Process based IT 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 giving the good example	Senior business and IT management acting as "partners"
	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

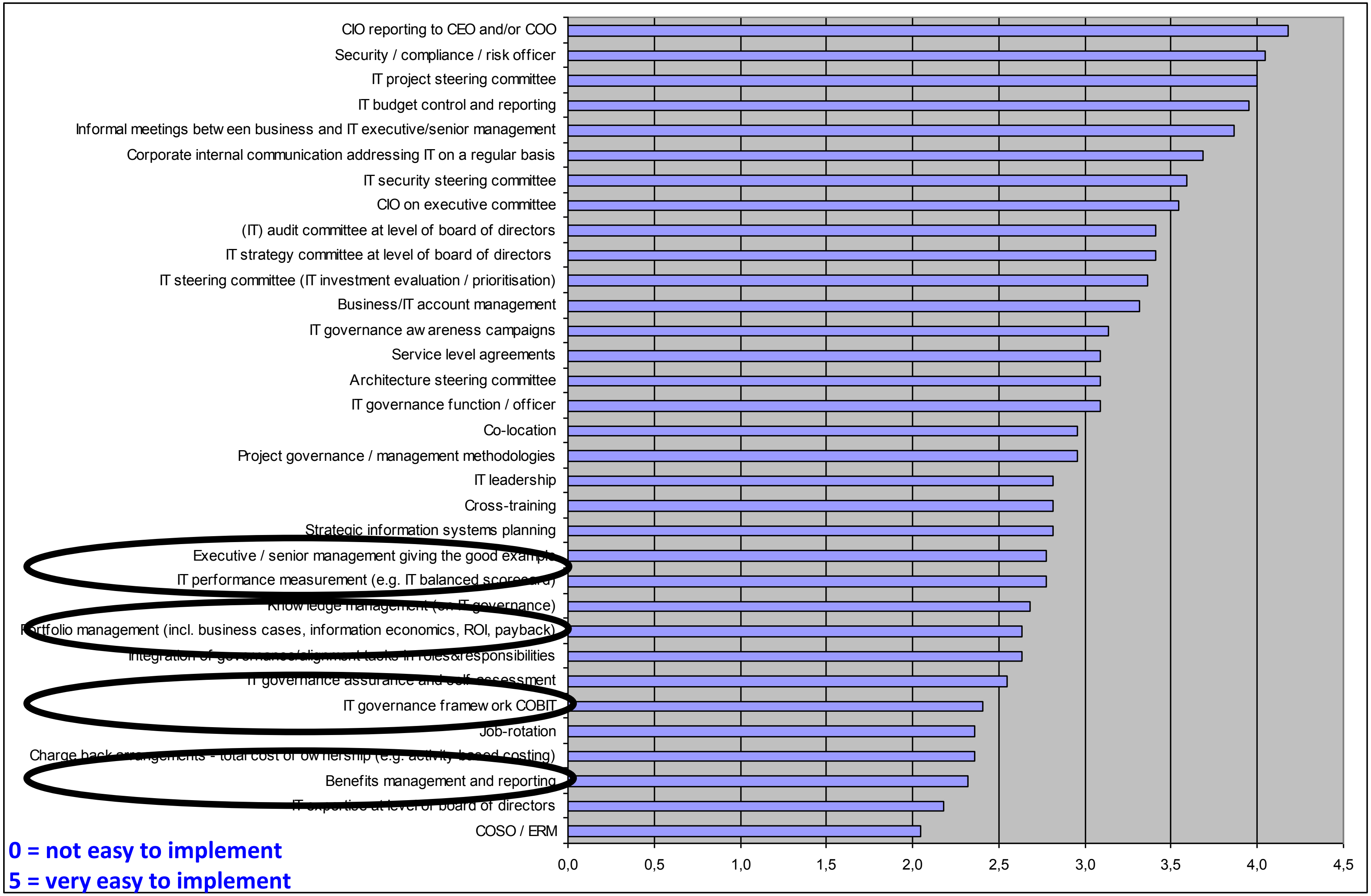
10 relational mechanisms

Perceived effectiveness of EGIT practices



0 = not effective, 5 = very effective

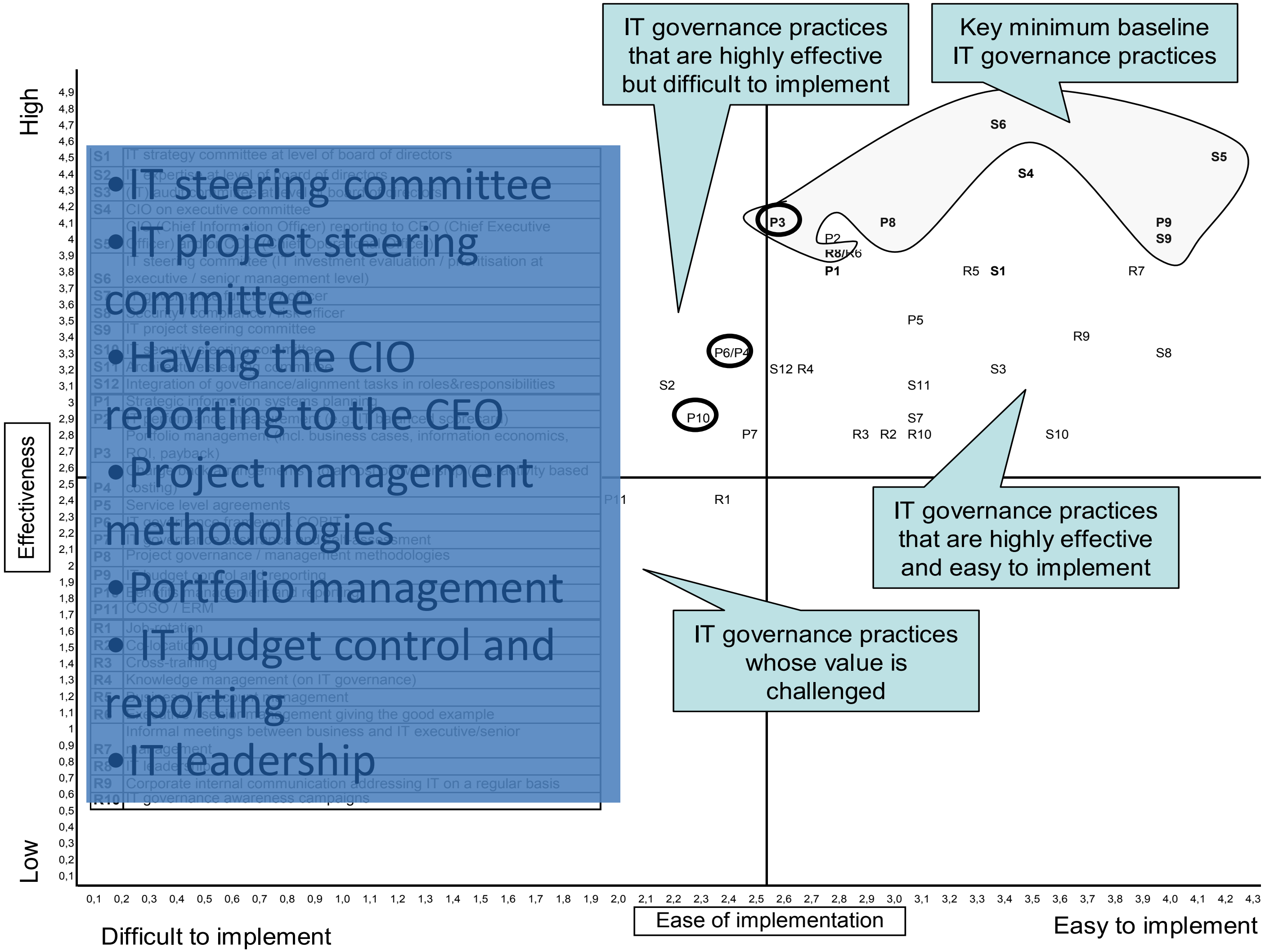
Perceived ease of implementation of EGIT practices



0 = not easy to implement

5 = very easy to implement

Effectiveness vs ease of implementation



IT governance practices that are highly effective but difficult to implement

Key minimum baseline IT governance practices

IT governance practices that are highly effective and easy to implement

IT governance practices whose value is challenged

- IT steering committee
- IT project steering committee
- Having the CIO reporting to the CEO
- Project management methodologies
- Portfolio management
- IT budget control and reporting
- IT leadership

S1	IT strategy committee at level of board of directors
S2	IT expertise at level of board of directors
S3	(IT) audit committee at level of board of directors
S4	CIO on executive committee
S5	CIO (Chief Information Officer) reporting to CEO (Chief Executive Officer) and/or COO (Chief Operational Officer)
S6	IT steering committee (IT investment evaluation / prioritisation at executive / senior management level)
S7	IT governance function / officer
S8	Security / compliance / risk officer
S9	IT project steering committee
S10	IT security steering committee
S11	Architecture steering committee
S12	Integration of governance/alignment tasks in roles&responsibilities
P1	Strategic information systems planning
P2	IT performance measurement (e.g. IT balanced scorecard)
P3	Portfolio management (incl. business cases, information economics, ROI, payback)
P4	Charge back arrangements - total cost of ownership (e.g. activity based costing)
P5	Service level agreements
P6	IT governance framework COBIT
P7	IT governance assurance and self-assessment
P8	Project governance / management methodologies
P9	IT budget control and reporting
P10	Benefits management and reporting
P11	COSO / ERM
R1	Job-rotation
R2	Co-location
R3	Cross-training
R4	Knowledge management (on IT governance)
R5	Business/IT account management
R6	Executive / senior management giving the good example
R7	Informal meetings between business and IT executive/senior management
R8	IT leadership
R9	Corporate internal communication addressing IT on a regular basis
R10	IT governance awareness campaigns

Índice

1. Enterprise Governance of IT
2. Enterprise Governance of IT practices
3. Enterprise Governance of IT as enabler for business / IT alignment
4. Enterprise Governance of IT as enabler for business value
5. COBIT 5

Luftman assessment of business/IT alignment maturity

Validated instrument

Used in many studies to assess business/IT alignment

6 attributes

- Communications maturity
- Competency/value measurements maturity
- Governance maturity
- Partnership maturity
- Scope & architecture maturity
- Skills maturity

Luftman assessment of business/IT alignment maturity…

attribute	characteristics level 1	characteristic level 5
•communications maturity		
• understanding of business by IT	minimum	pervasive
• understanding of IT by business	minimum	pervasive
• inter/intra-organizational learning	casual, ad hoc	strong and structured
• protocol rigidity	command and control	informal
• knowledge sharing	ad hoc	extra-enterprise
• liaison(s) breath/effectiveness	none or ad hoc	extra-enterprise
• competency/value measurements maturity		
• IT metrics	technical	extended to external partners
• business metrics	ad hoc	extended to external partners
• balanced metrics	ad hoc, unlinked	business, partner and IT metrics
• service level agreements	sporadically present	extended to external partners
• benchmarking	not generally practiced	routinely performed with partners
• formal assessments/reviews	none	routinely performed
• continuous improvement	none	routinely performed
• governance maturity		
• business strategic planning	ad hoc	integrated across & external
• IT strategic planning	ad hoc	integrated across & external
• reporting/organization structure	CIO reports to CFO central/decentral	CIO reports to CEO federated
• budgetary/control	cost center, erratic	investment center, profit center
• IT investment management	cost based, erratic	business value
• steering committee(s)	not formal, regular	partnership
• prioritization process	reactive	value added partner

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Luftman assessment of business/IT alignment maturity…

attribute	characteristics level 1	characteristic level 5
• partnership maturity		
• business perception of IT value	IT perceived as a cost	IT co -adapts with business
• role of IT in strategic business planning	no seat at business table	co-adaptive with business
• shared goals, risk, rewards/penalties	IT takes risk	risks and rewards shared
• IT program management	ad hoc	continuous improvement
• relationship/trust style	conflict/minimum	valued partnership
• business sponsor/champion	none	at the CEO level
• scope & architecture maturity		
• traditional, enabler/driver	traditional systems	business strategy driver/enabler
• standards articulation	none or ad hoc	inter-enterprise standards
• architectural integration:	no formal integration	evolve with partners
• functional organization		integrated
• enterprise		standard enterprise architecture
• inter-enterprise		with all partners
• architectural transparency, flexibility	none	across the infrastructure
• skills maturity		
• innovation, entrepreneurship	discouraged	the norm
• locus of power	in the business	all executives, including CIO
• management style	command and control	relationship based
• change readiness	resistant to change	high, focused
• career crossover	none	across the enterprise
• education, cross-training	none	across the enterprise
• attract & retain best talent	no program	effective program for hiring & retaining

Example questions (partnership maturity)

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

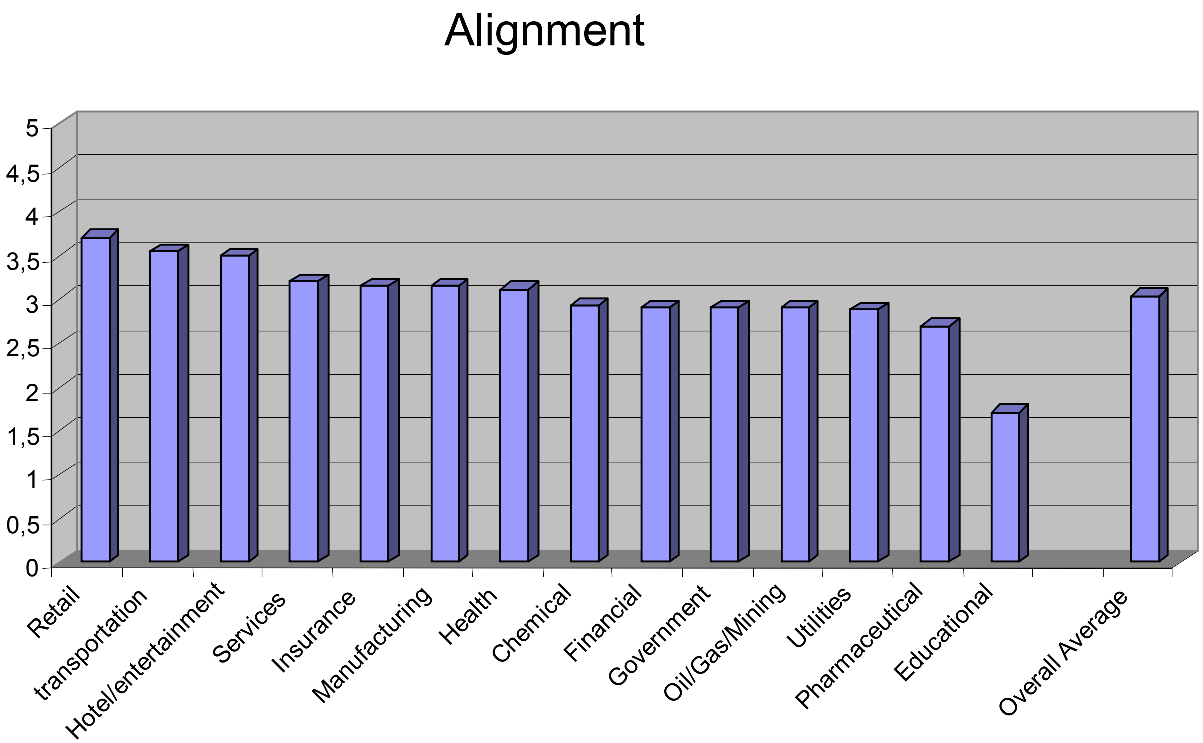
The following statements are about the IT and business relationship and trust.

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

Business / IT alignment international benchmark



Business / IT alignment Belgian benchmark

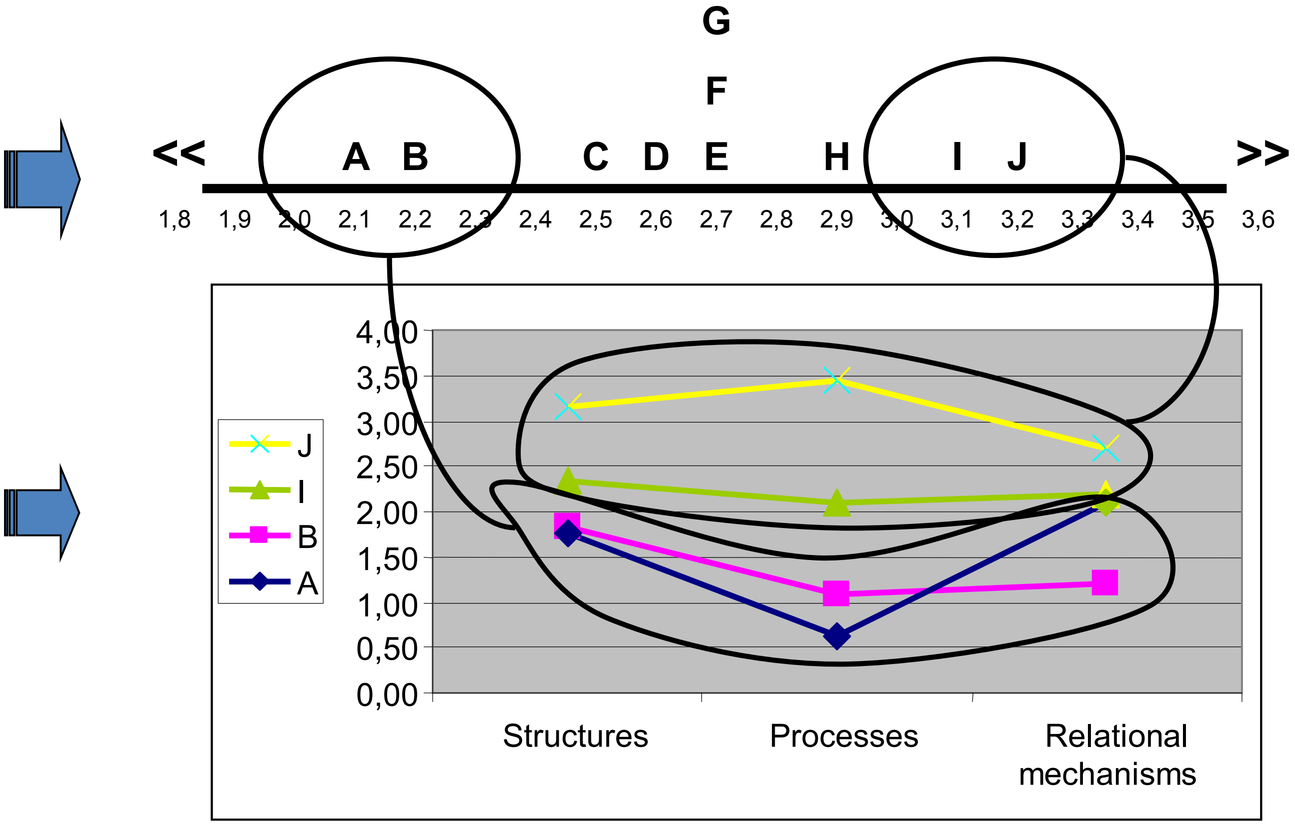
Organisation	Total number of respondents	Number of IT respondents	Number of business respondents	Average maturity score by IT	Average maturity score by business	Delta	Total Alignment maturity Score	Deviation from average	
A	9	5	4	2,06	2,14	-0,07	2,10	-0,59	-22%
B	5	3	2	2,27	2,00	0,27	2,16	-0,52	-19%
C	9	3	6	2,59	2,55	0,05	2,56	-0,12	-5%
D	6	3	3	2,98	2,35	0,64	2,67	-0,02	-1%
E	9	5	4	2,69	2,74	-0,05	2,71	0,03	1%
F	8	3	5	3,15	2,46	0,69	2,72	0,04	1%
G	10	5	5	2,75	2,73	0,03	2,74	0,06	2%
H	9	6	2	2,89	2,95	-0,06	2,91	0,22	8%
I	8	5	4	3,23	2,97	0,26	3,11	0,43	16%
J	11	6	5	3,09	3,26	-0,17	3,17	0,48	18%
	Total	Total	Total				Average		
	84	44	40				2,69		

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

The relationship between EGIT and business/IT alignment

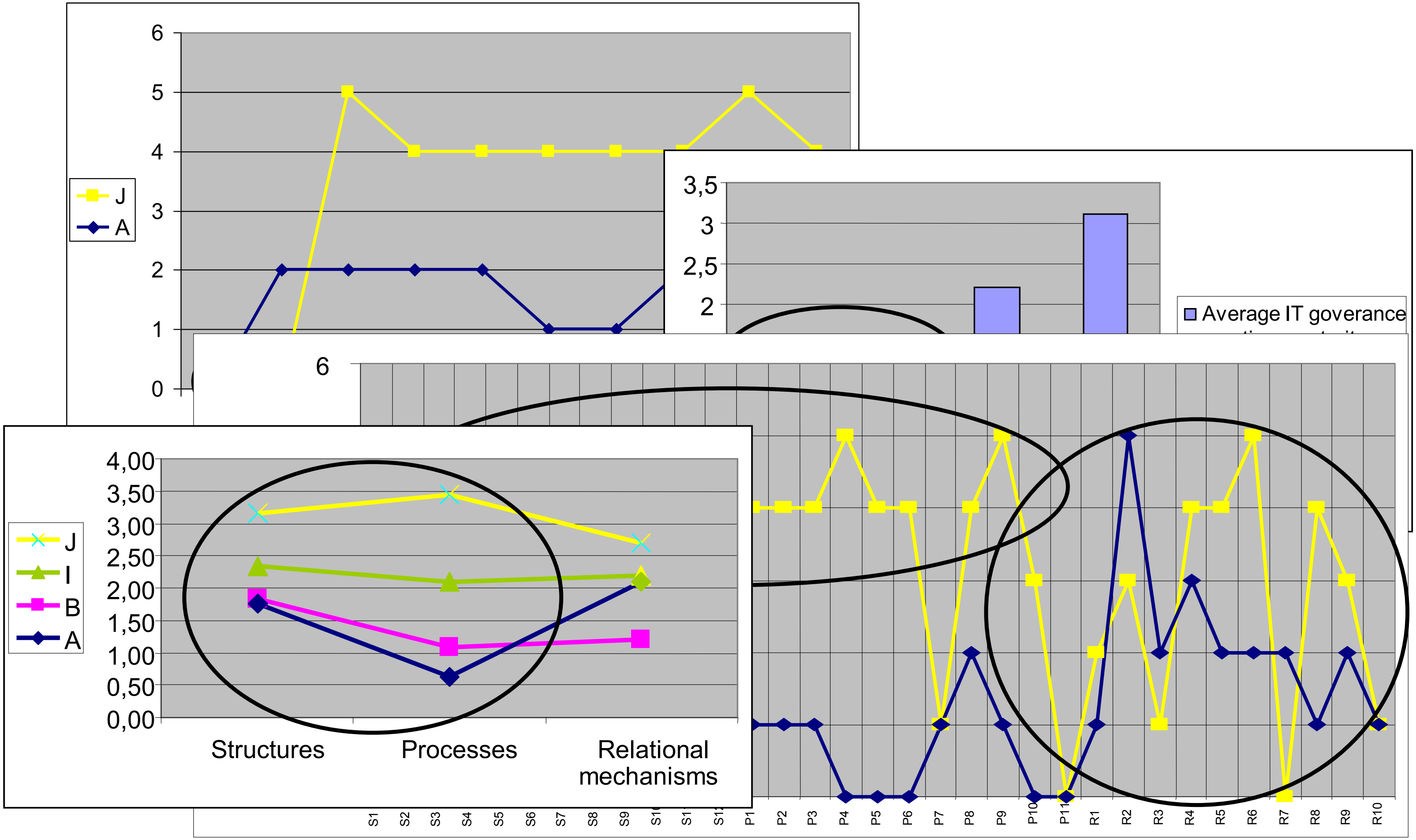
Business/IT alignment maturity

Maturity of IT governance practices



Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Extreme cases analysis EGIT practices versus business / IT alignment

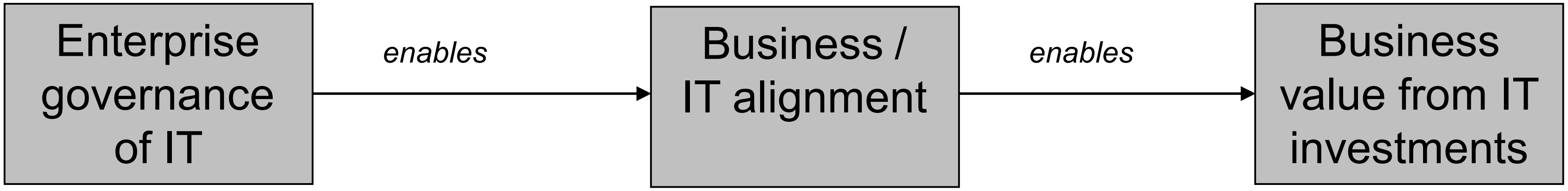


Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Índice

1. Enterprise Governance of IT
2. Enterprise Governance of IT practices
3. Enterprise Governance of IT as enabler for business / IT alignment
4. Enterprise Governance of IT as enabler for business value
5. COBIT 5

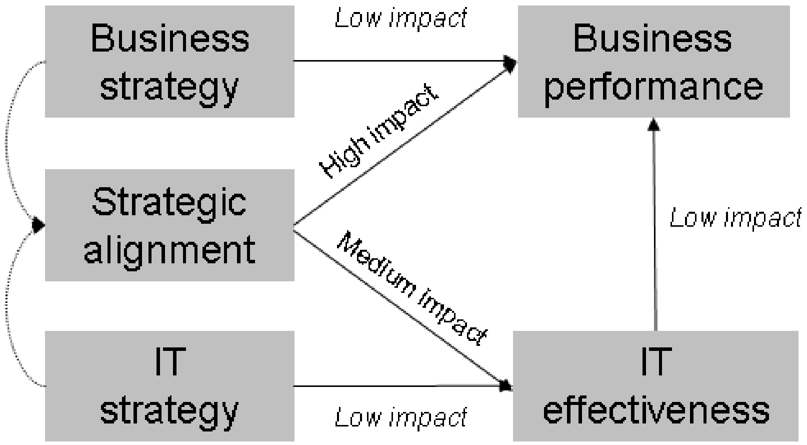
From enterprise governance of IT to business value


Enterprise governance of IT
enables
Business / IT alignment
enables
Business value from IT investments

Business/IT alignment and Business Value from IT

Why is alignment important to an organization's success?

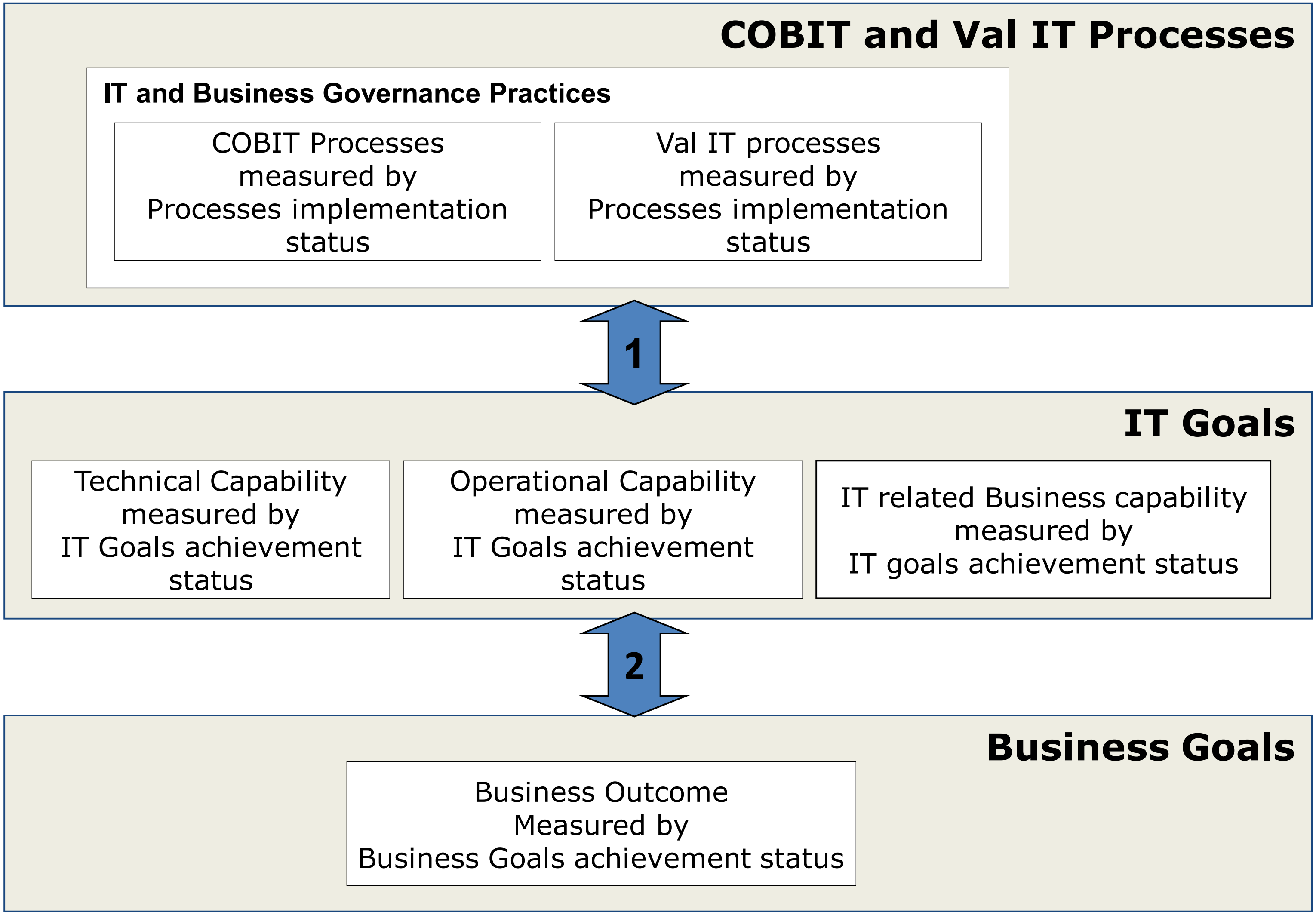
- Research from Chan and Bergeron: impact of alignment on business performance is higher than impact of business strategy or IT strategy
- Productivity paradox (Brynjolfson)


Business strategy
Strategic alignment
IT strategy
Business performance
IT effectiveness

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

COBIT, VALIT and Business Value

The validated research cascade model



COBIT and Val IT Processes

IT and Business Governance Practices

COBIT Processes measured by Processes implementation status

Val IT processes measured by Processes implementation status

1

IT Goals

Technical Capability measured by IT Goals achievement status

Operational Capability measured by IT Goals achievement status

IT related Business capability measured by IT goals achievement status

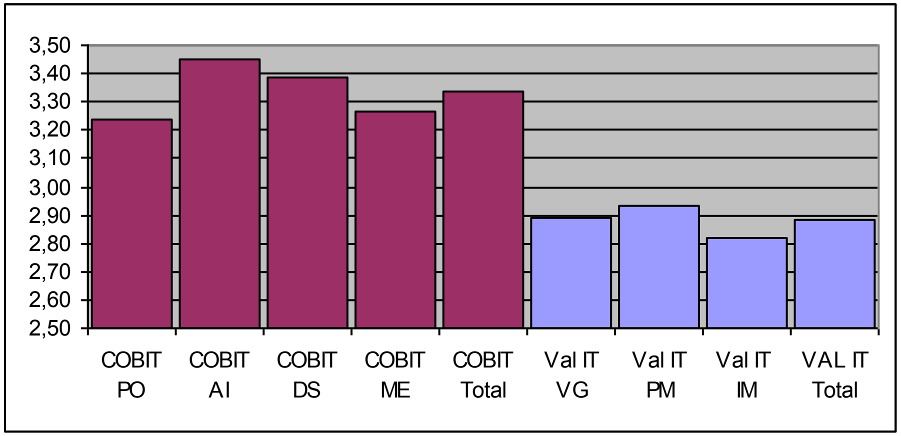
2

Business Goals

Business Outcome Measured by Business Goals achievement status

Implementation status COBIT and VALIT

- Operational oriented processes (AI and DS) are better implemented than planning (PO) monitoring (ME) processes.
- COBIT processes are better implemented than Val IT processes

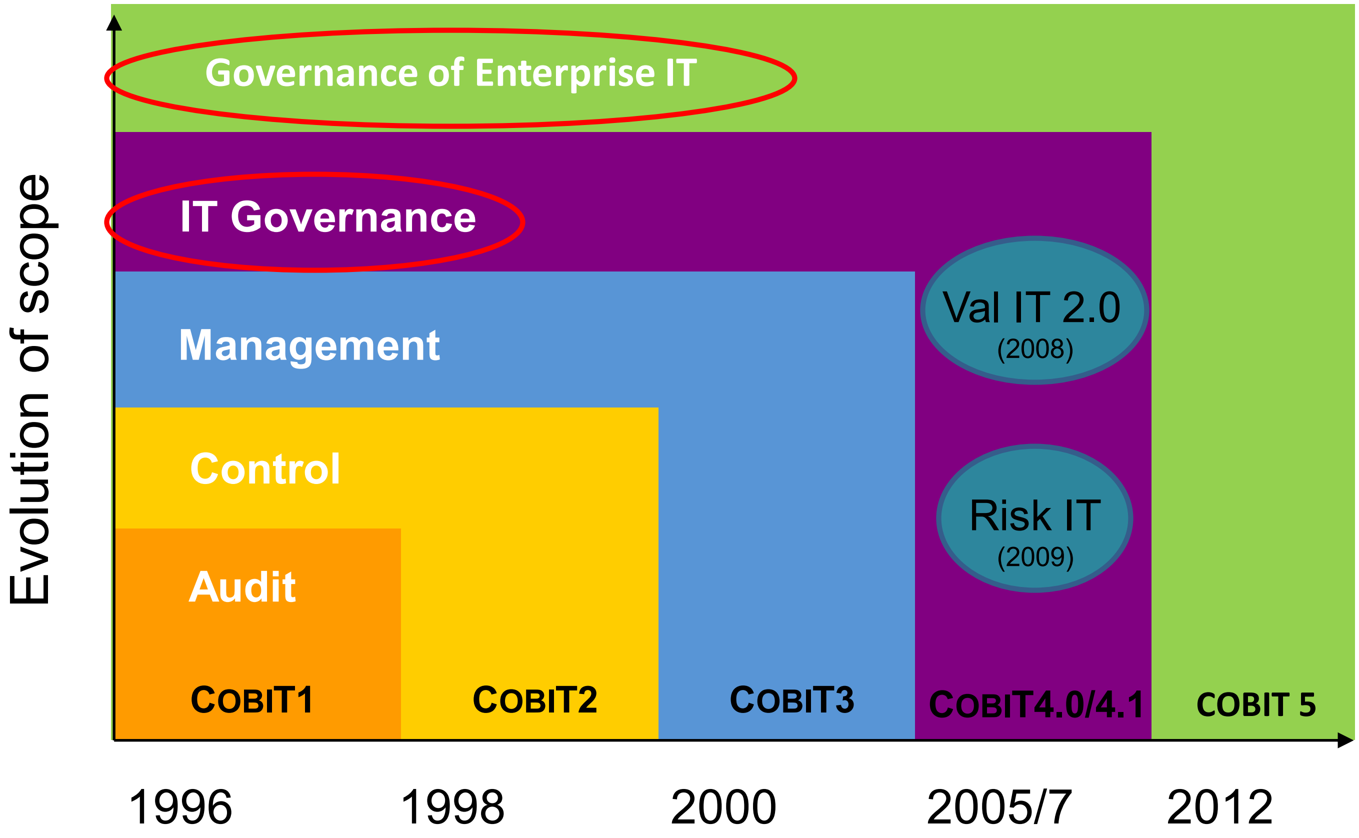


Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

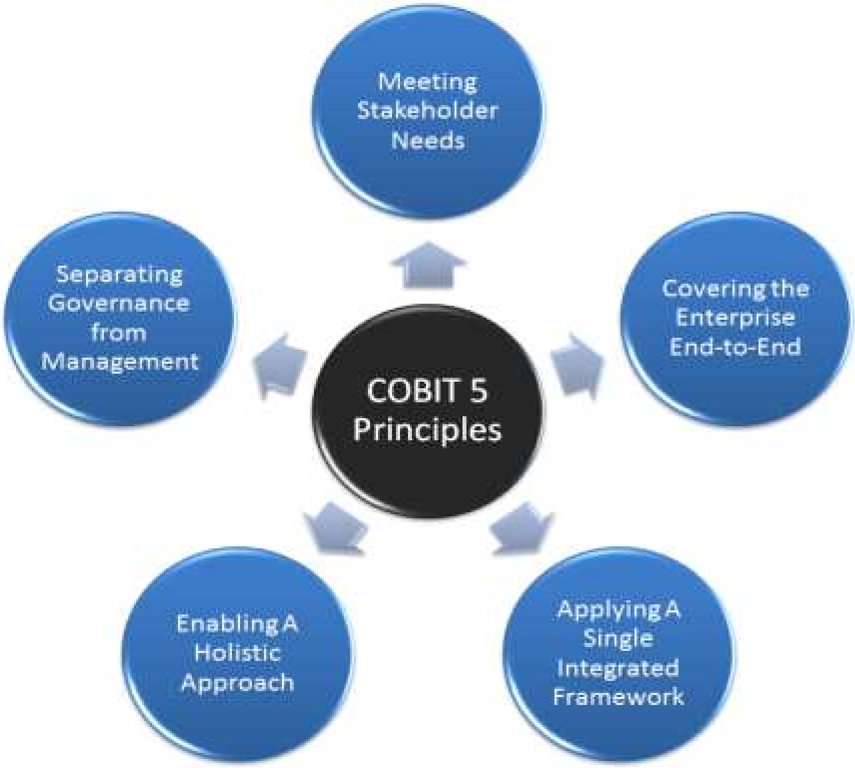
Índice

1. Enterprise Governance of IT
2. Enterprise Governance of IT practices
3. Enterprise Governance of IT as enabler for business / IT alignment
4. Enterprise Governance of IT as enabler for business value
5. COBIT 5

COBIT evolution



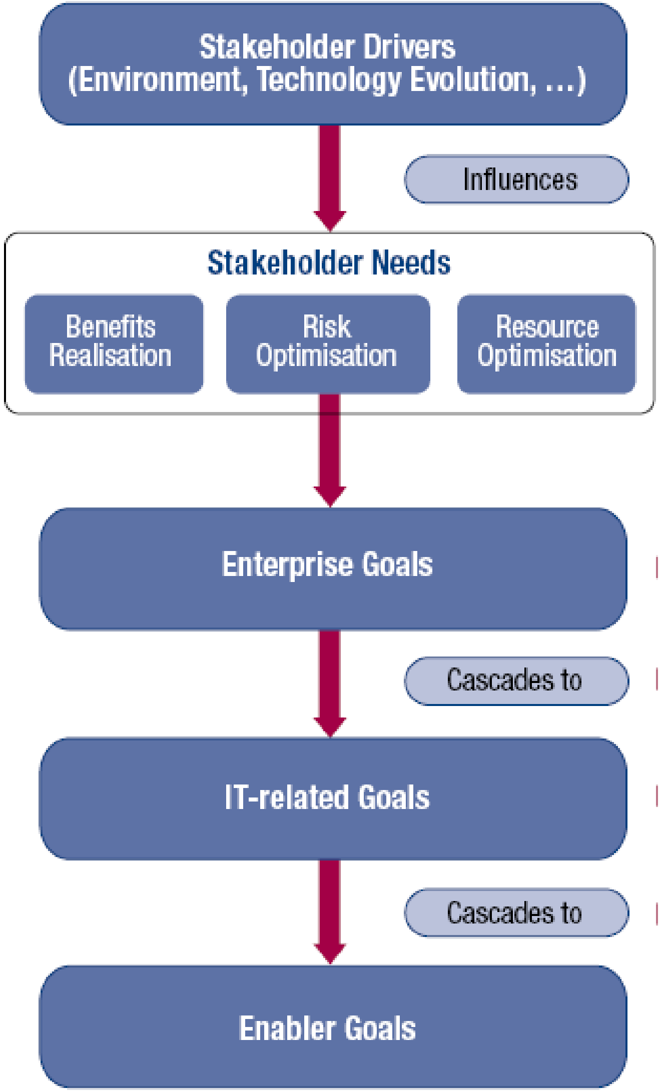
COBIT 5


COBIT 5 Principles
Meeting Stakeholder Needs
Covering the Enterprise End-to-End
Applying A Single Integrated Framework
Enabling A Holistic Approach
Separating Governance from Management

COBIT 5 brings together the **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.

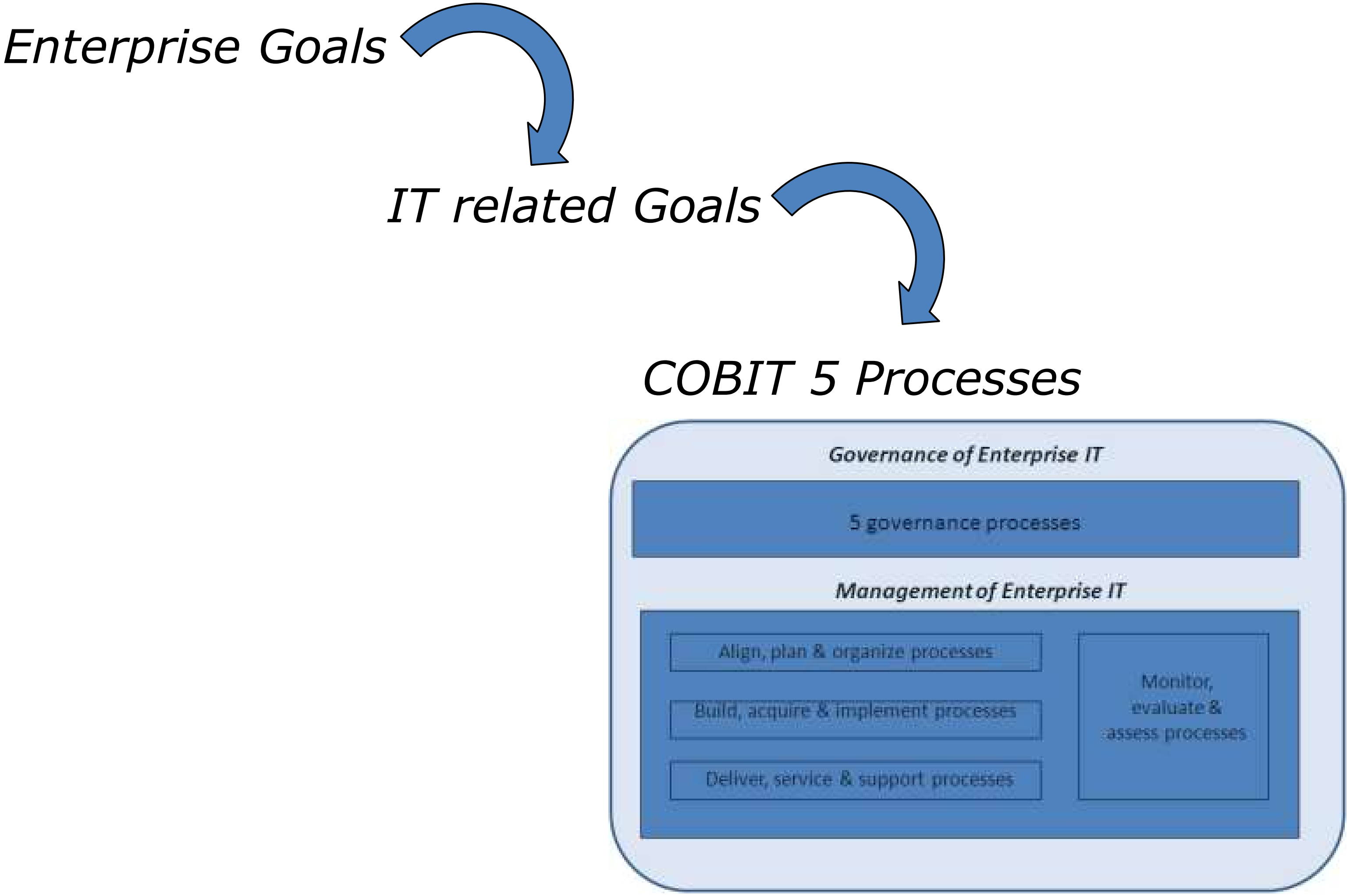
COBIT 5 - 1. Meeting stakeholder needs

- 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.



Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

COBIT 5 - 1. Meeting stakeholder needs



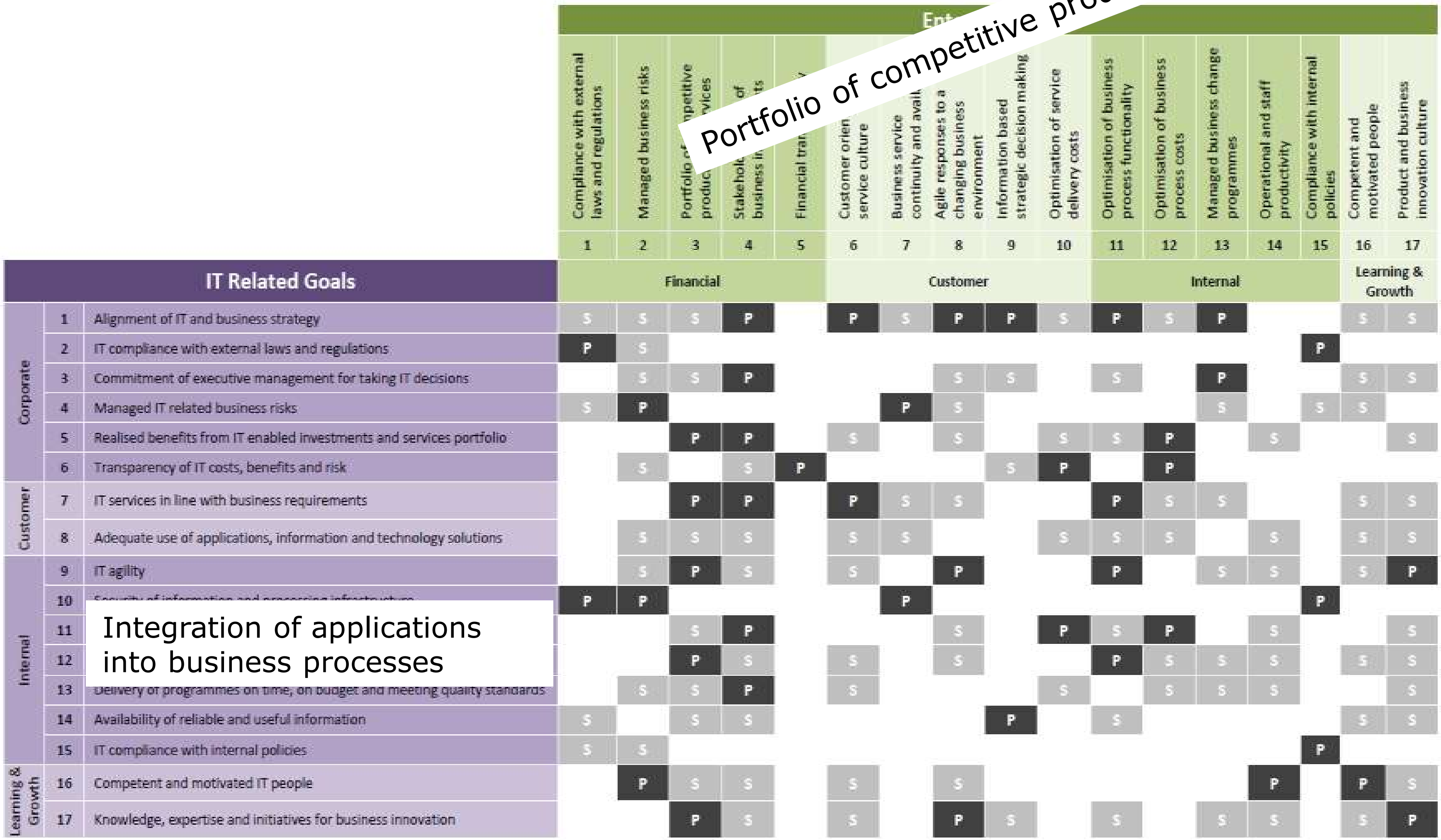
Enterprise Goals

IT related Goals

COBIT 5 Processes

Governance of Enterprise IT
5 governance processes
Management of Enterprise IT
Align, plan & organize processes
Build, acquire & implement processes
Deliver, service & support processes
Monitor, evaluate & assess processes

COBIT 5 - 1. Meeting stakeholder needs

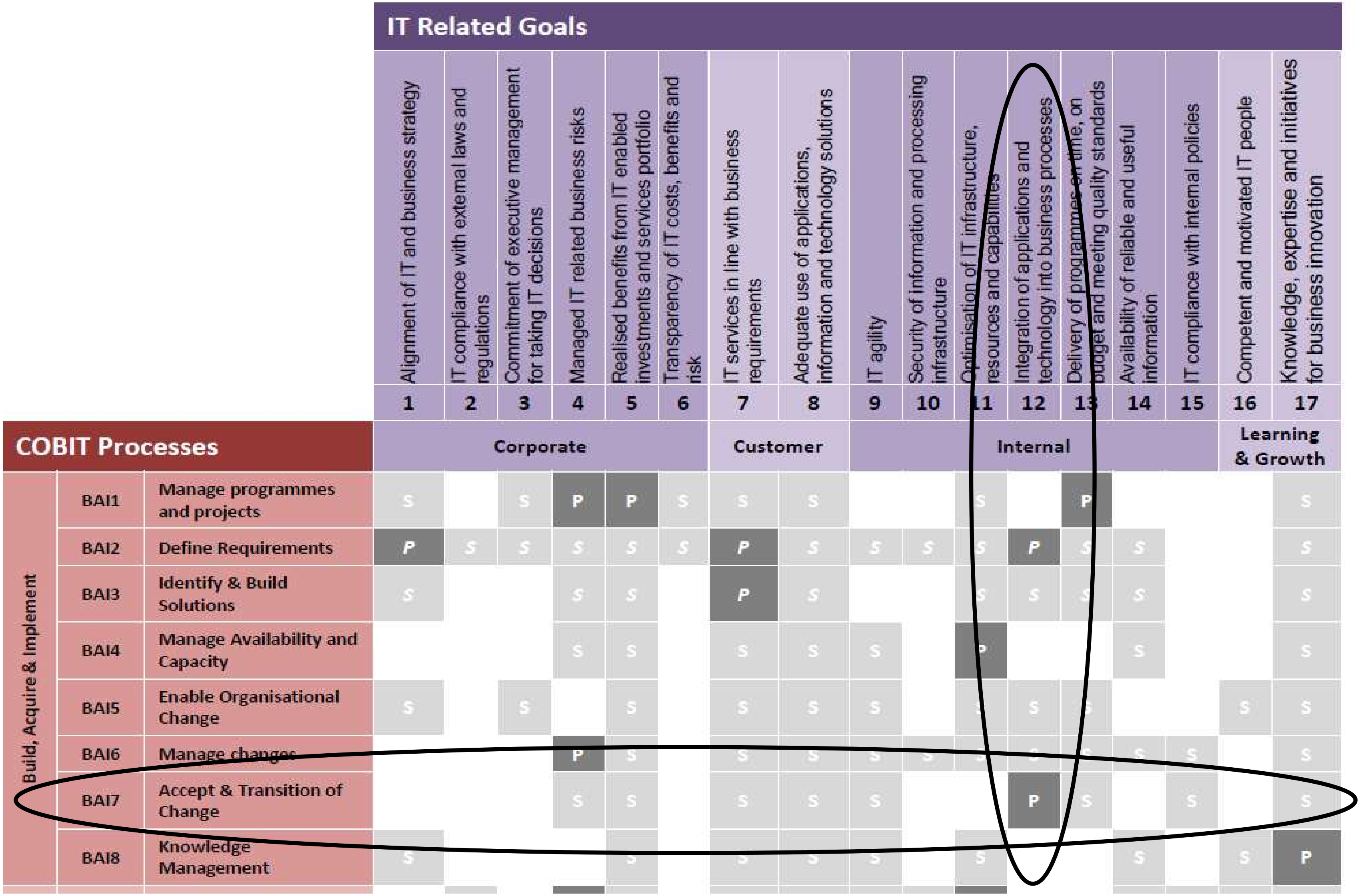


			Ent																
			Compliance with external laws and regulations	Managed business risks	Portfolio o produc mpetitive vices	Stakehol of business in ts	Financial tra	Customer orien service culture	Business service continuity and avail	Agile responses to a changing business environment	Information based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Competent and motivated people	Product and business innovation culture
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
IT Related Goals			Financial					Customer					Internal					Learning & Growth	
Corporate	1	Alignment of IT and business strategy	S	S	S	P		P	S	P	P	S	P	S	P			S	S
	2	IT compliance with external laws and regulations	P	S													P		
	3	Commitment of executive management for taking IT decisions		S	S	P				S	S		S		P			S	S
	4	Managed IT related business risks	S	P					P	S					S		S	S	
	5	Realised benefits from IT enabled investments and services portfolio			P	P		S		S		S	S	P		S			S
	6	Transparency of IT costs, benefits and risk		S		S	P				S	P		P					
Customer	7	IT services in line with business requirements			P	P		P	S	S			P	S	S			S	S
	8	Adequate use of applications, information and technology solutions		S	S	S		S	S			S	S	S		S		S	S
Internal	9	IT agility		S	P	S		S		P			P		S	S		S	P
	10	Security of information and processing infrastructure	P	P					P								P		
	11				S	P				S		P	S	P		S			S
	12				P	S		S		S			P	S	S	S		S	S
	13	Delivery of programmes on time, on budget and meeting quality standards		S	S	P		S				S		S	S	S			S
	14	Availability of reliable and useful information	S		S	S					P		S					S	S
	15	IT compliance with internal policies	S	S													P		
Learning & Growth	16	Competent and motivated IT people		P	S	S		S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation			P	S		S		P	S		S		S	S		S	P

Portfolio of competitive products and services

Integration of applications into business processes

COBIT 5 - 1. Meeting stakeholder needs



IT Related Goals

COBIT Processes			Alignment of IT and business strategy	IT compliance with external laws and regulations	Commitment of executive management for taking IT decisions	Managed IT related business risks	Realised benefits from IT enabled investments and services portfolio	Transparency of IT costs, benefits and risk	IT services in line with business requirements	Adequate use of applications, information and technology solutions	IT agility	Security of information and processing infrastructure	Optimisation of IT infrastructure, resources and capabilities	Integration of applications and technology into business processes	Delivery of programmes on time, on budget and meeting quality standards	Availability of reliable and useful information	IT compliance with internal policies	Competent and motivated IT people	Knowledge, expertise and initiatives for business innovation
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Corporate						Customer		Internal							Learning & Growth	
Build, Acquire & Implement	BAI1	Manage programmes and projects	S		S	P	P	S	S	S			S		P				S
	BAI2	Define Requirements	P	S	S	S	S	S	P	S	S	S	S	P	S	S			S
	BAI3	Identify & Build Solutions	S			S	S		P	S			S	S	S	S			S
	BAI4	Manage Availability and Capacity				S	S		S	S	S		P			S			S
	BAI5	Enable Organisational Change	S		S		S		S	S	S		S	S	S			S	S
	BAI6	Manage changes				P	S		S	S	S	S	S	S	S	S	S		S
	BAI7	Accept & Transition of Change				S	S		S	S	S			P	S		S		S
	BAI8	Knowledge Management	S				S		S	S	S		S			S		S	P

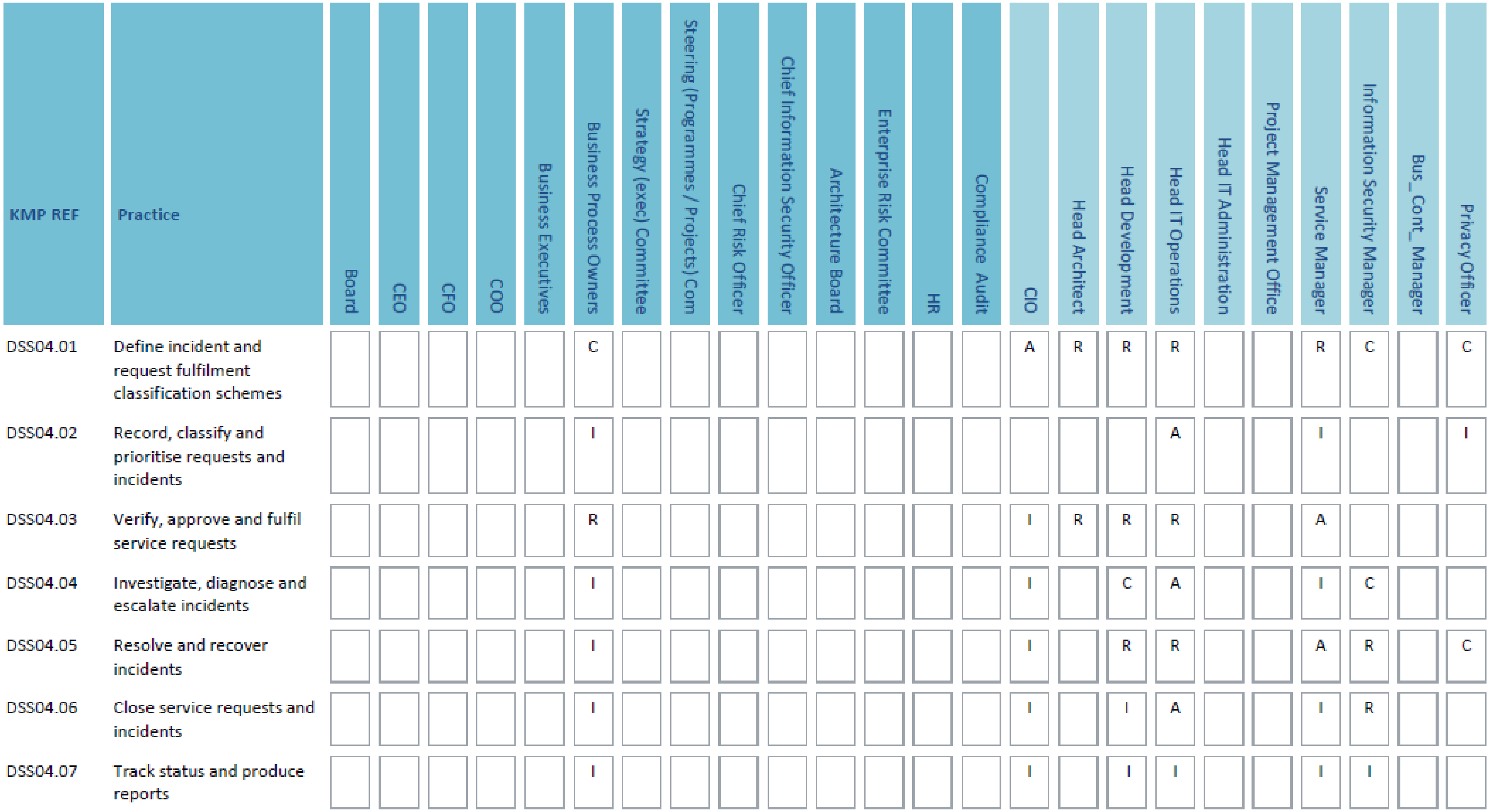
COBIT 5 - 2. Covering the Enterprise End-to-end

- COBIT 5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective.

- This means that COBIT 5:
  - Integrates governance of enterprise IT into enterprise governance, i.e., the governance system for enterprise IT proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance.

  - Covers all functions and processes within the enterprise; **COBIT 5 does not focus only on the 'IT function'**, but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

COBIT 5 - 2. Covering the Enterprise End-to-end



KMP REF	Practice	Board	CEO	CFO	COO	Business Executives	Business Process Owners	Strategy (exec) Committee	Steering (Programmes / Projects) Com	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	HR	Compliance Audit	CIO	Head Architect	Head Development	Head IT Operations	Head IT Administration	Project Management Office	Service Manager	Information Security Manager	Bus_ Cont_ Manager	Privacy Officer
DSS04.01	Define incident and request fulfilment classification schemes						C									A	R	R	R			R	C		C
DSS04.02	Record, classify and prioritise requests and incidents						I												A			I			I
DSS04.03	Verify, approve and fulfil service requests						R									I	R	R	R			A			
DSS04.04	Investigate, diagnose and escalate incidents						I									I		C	A			I	C		
DSS04.05	Resolve and recover incidents						I									I		R	R			A	R		C
DSS04.06	Close service requests and incidents						I									I		I	A			I	R		
DSS04.07	Track status and produce reports						I									I		I	I			I	I		

COBIT 5 - 3. Applying a Single Integrated Framework

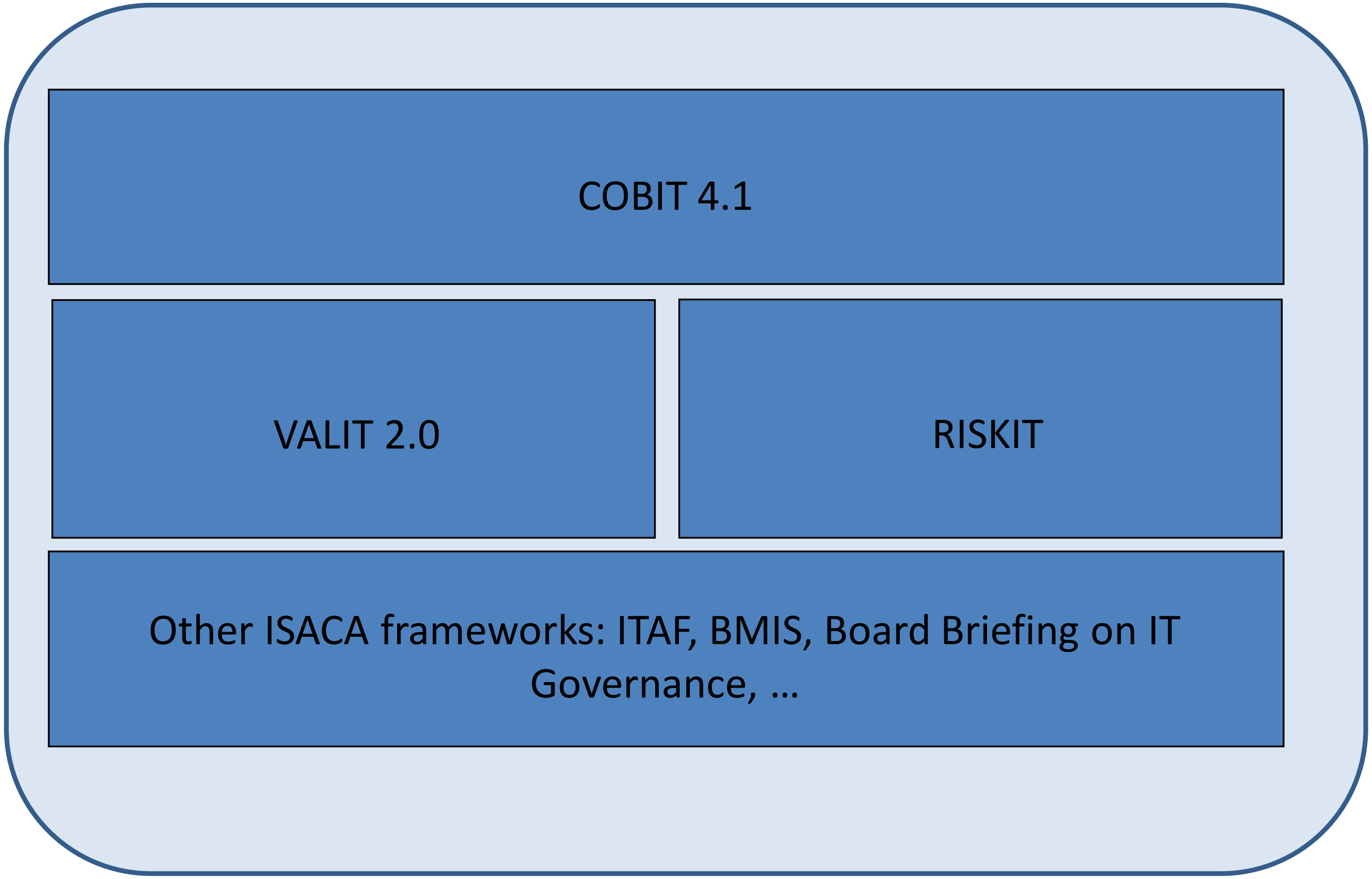
COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises:

- 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.

COBIT 5 - 3. Applying a Single Integrated Framework



COBIT 4.1

VALIT 2.0

RISKIT

Other ISACA frameworks: ITAF, BMIS, Board Briefing on IT Governance, …

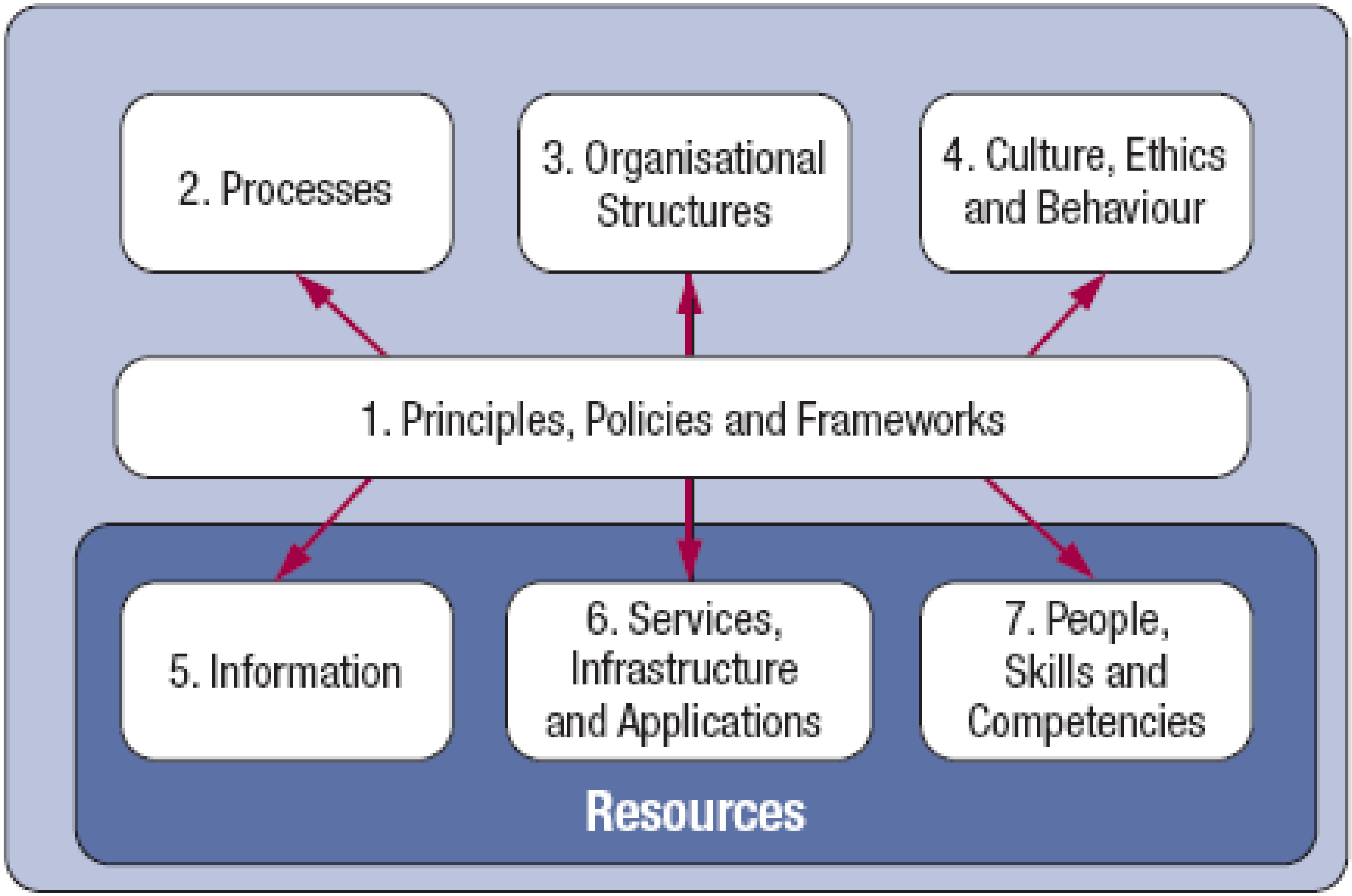
COBIT 5 - 4. Enabling a Holistic Approach

COBIT 5 enablers are:

- 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**

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

COBIT 5 - 4. Enabling a Holistic Approach


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

COBIT 5 - 4. Enabling a Holistic Approach

1. **Processes**—Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals
2. **Organisational structures**—Are the key decision-making entities in an organisation
3. **Culture, ethics and behaviour**—Of individuals and of the organisation; very often underestimated as a success factor in governance and management activities
4. **Principles, policies and frameworks**—Are the vehicles to translate the desired behaviour into practical guidance for day-to-day management
5. **Information**—Is pervasive throughout any organisation, i.e., deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. **Services, infrastructure and applications**—Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services
7. **People, skills and competencies**—Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions

COBIT 5 - 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
  - Serve different purposes

- **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.

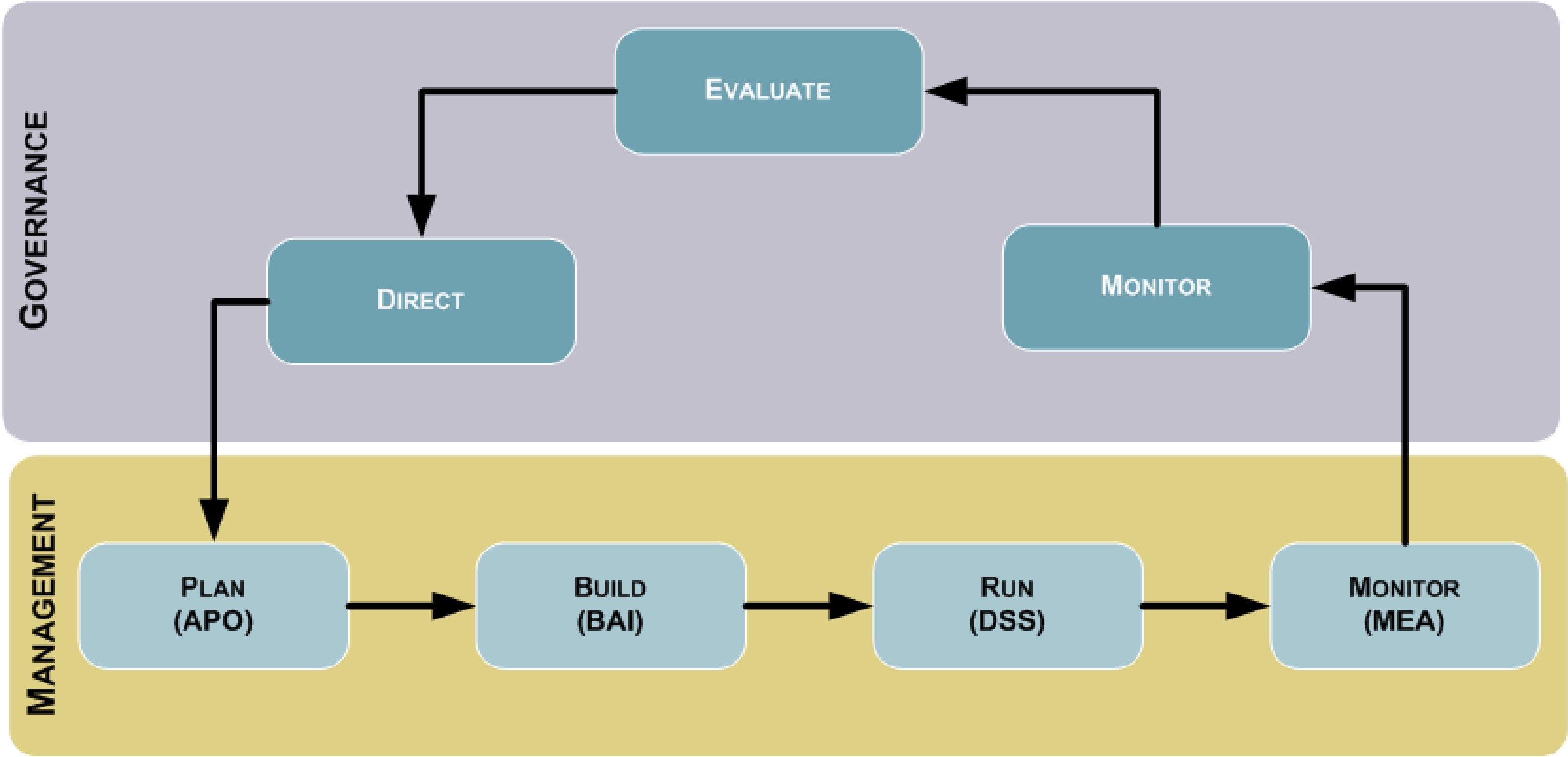
COBIT 5 - 5. Separating Governance From Management

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives **(EDM).**

- **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives **(PBRM).**

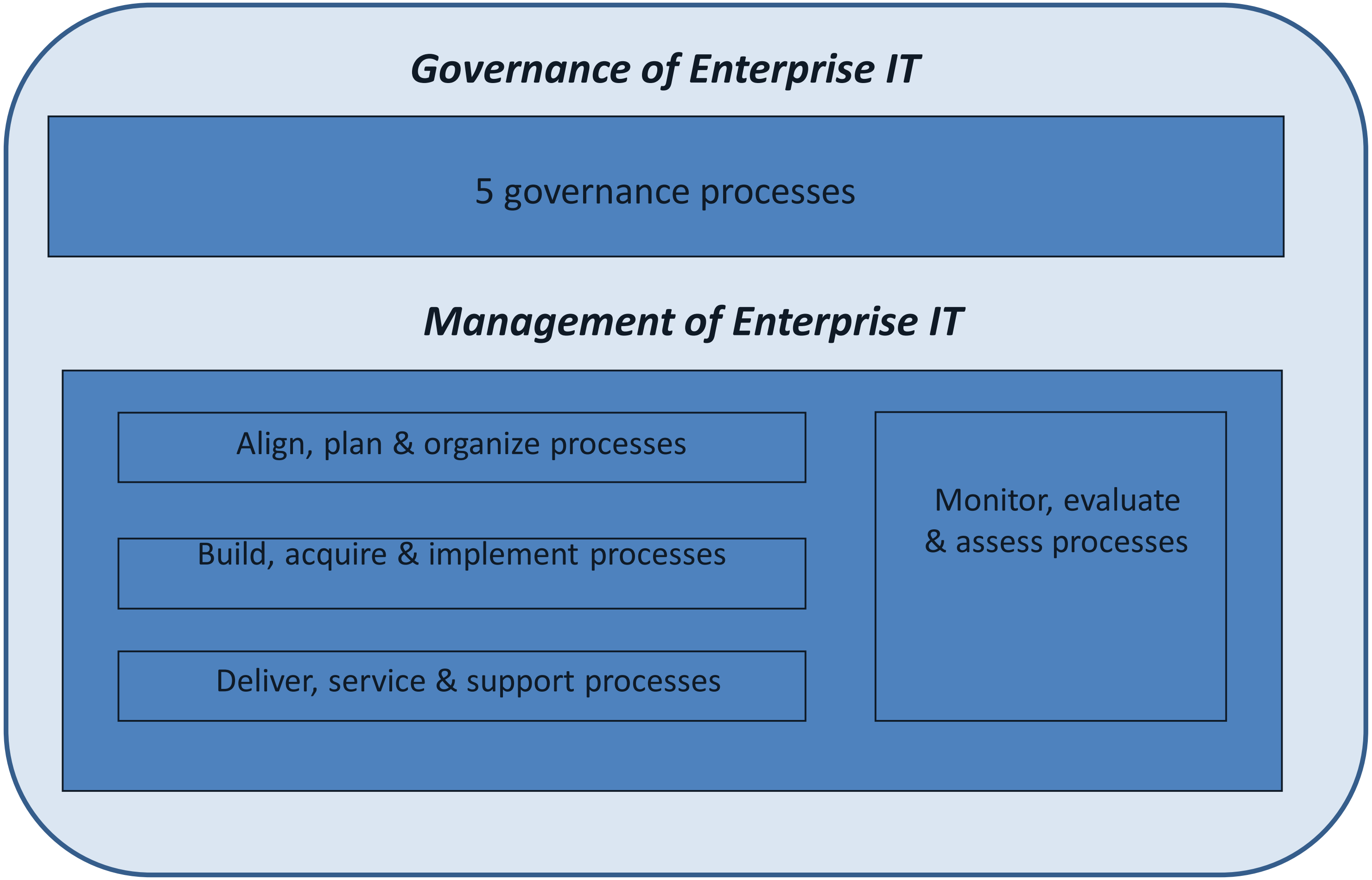
- *Exercising governance and management effectively in practice requires appropriately using all enablers. The COBIT process reference model allows us to focus easily on the relevant enterprise activities.*

COBIT 5 - 5. Separating Governance From Management



- **Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options, setting direction through prioritisation and decision making, and monitoring performance, compliance, and progress against plans.**
  - In most enterprises, governance is the responsibility of the board of directors under the leadership of the chairperson.
- **Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.**
  - In most enterprises, management is the responsibility of the executive management under the leadership of the CEO.

COBIT 5 - 5. Separating Governance From Management



Governance of Enterprise IT

5 governance processes

Management of Enterprise IT

Align, plan & organize processes

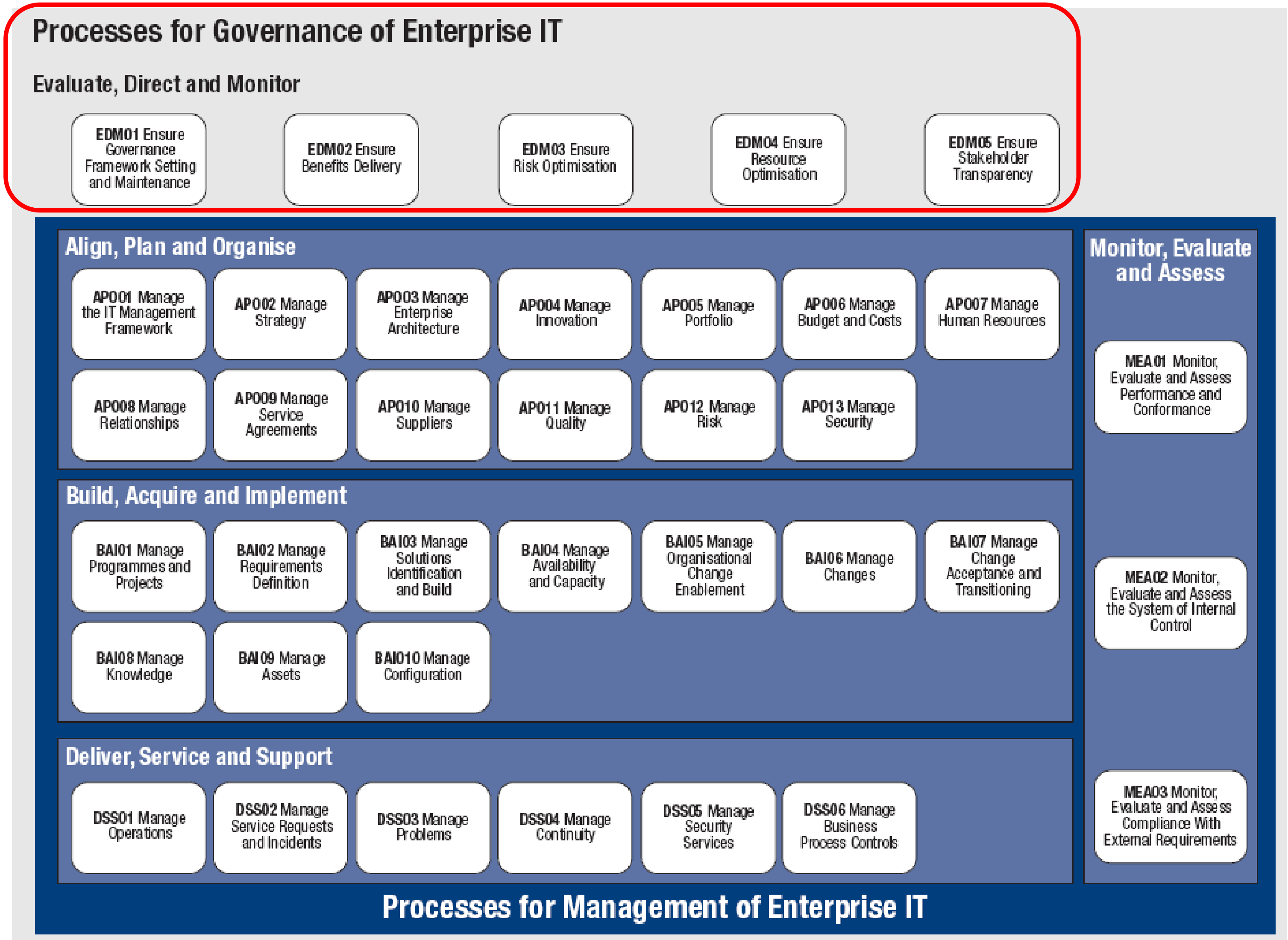
Build, acquire & implement processes

Deliver, service & support processes

Monitor, evaluate & assess processes

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

Governance in COBIT 5



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI010 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

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

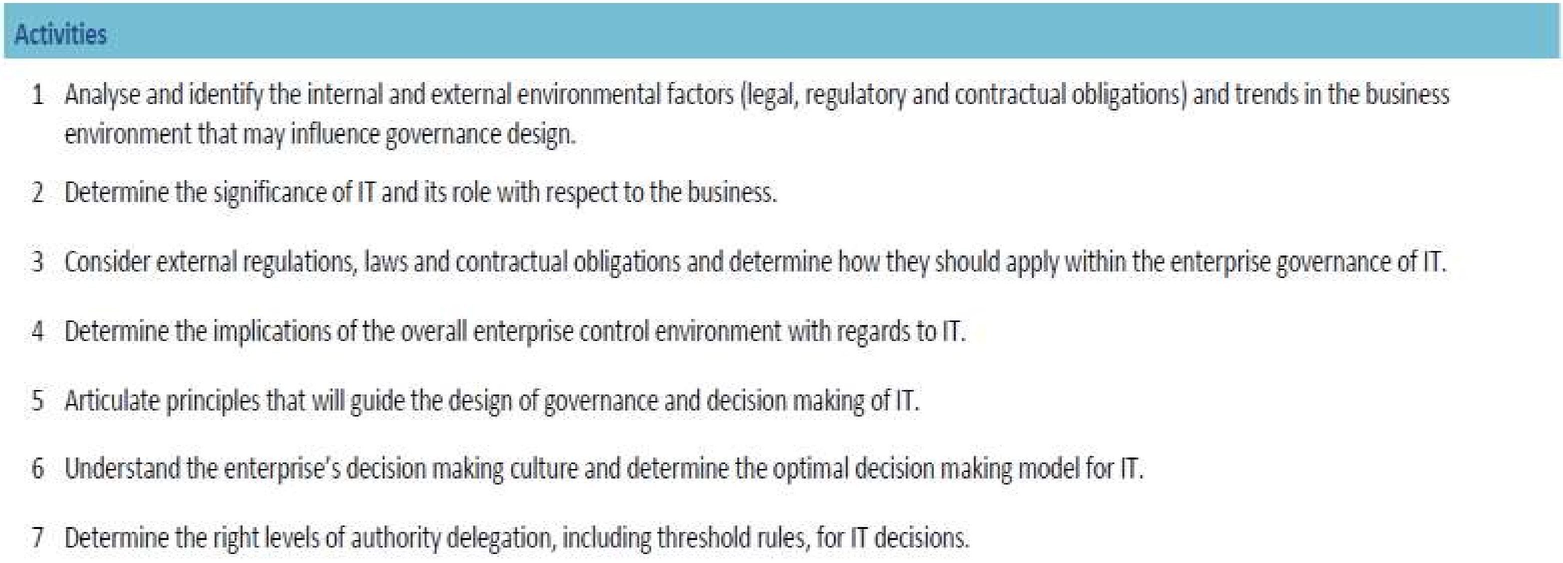
Governance versus Management

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

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.

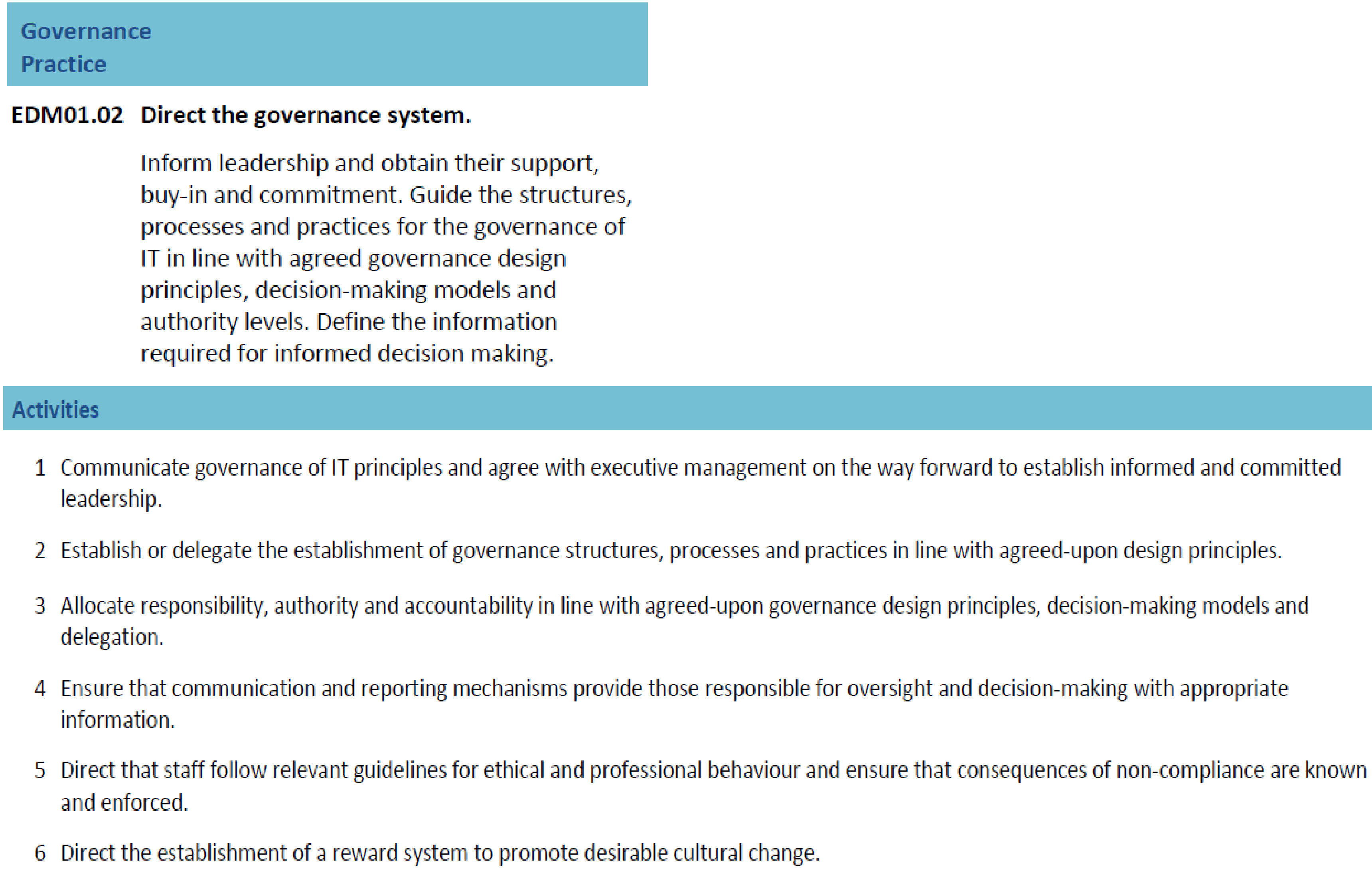
5 Articulate principles that will guide the design of governance and decision making of IT.

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.

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

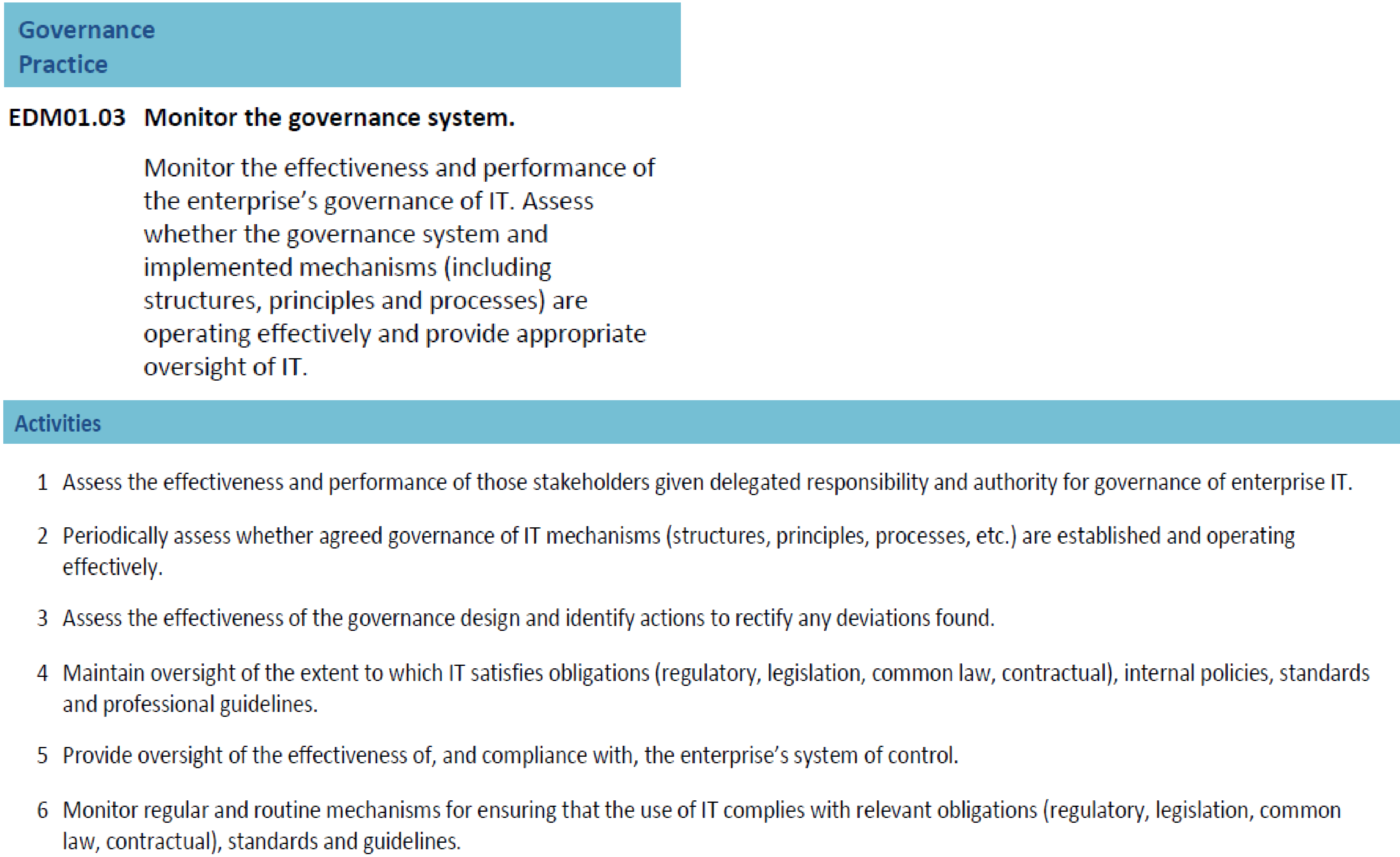
Governance versus Management



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



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.

Questions and discussion

More information

IT Governance and Alignment Research Institute

www.uams.be/ITAG

Email

wim.vangrembergen@ua.ac.be

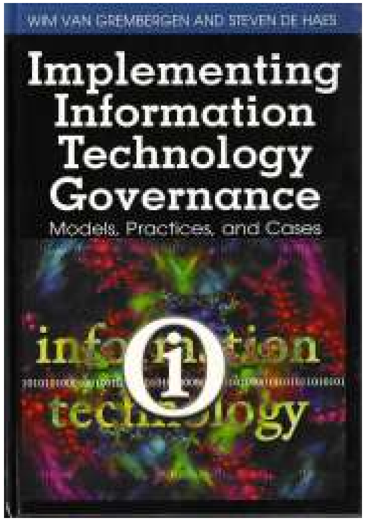
Books

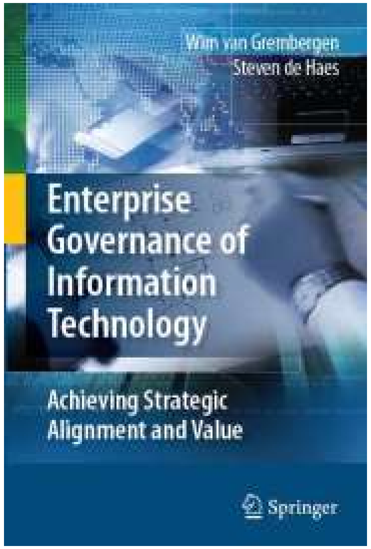
Van Grembergen W., De Haes S., Implementing Information Technology Governance: models, practices and cases, 255p., IGI Publishing, 2008

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


WIM VAN GREMBERGEN AND STEVEN DE HAES
Implementing Information Technology Governance
Models, Practices, and Cases
information technology


Wim van Grembergen
Steven de Haes
Enterprise Governance of Information Technology
Achieving Strategic Alignment and Value
Springer

Implantadores y Evaluadores del Gobierno de las Tecnologías de la Información en las Universidades, Baeza 2013

S5: Enterprise Governance of IT COBIT 5

Prof. Dr. Wim Van Grembergen