The autonomous management school of the University of Antwerp

antwerp management school

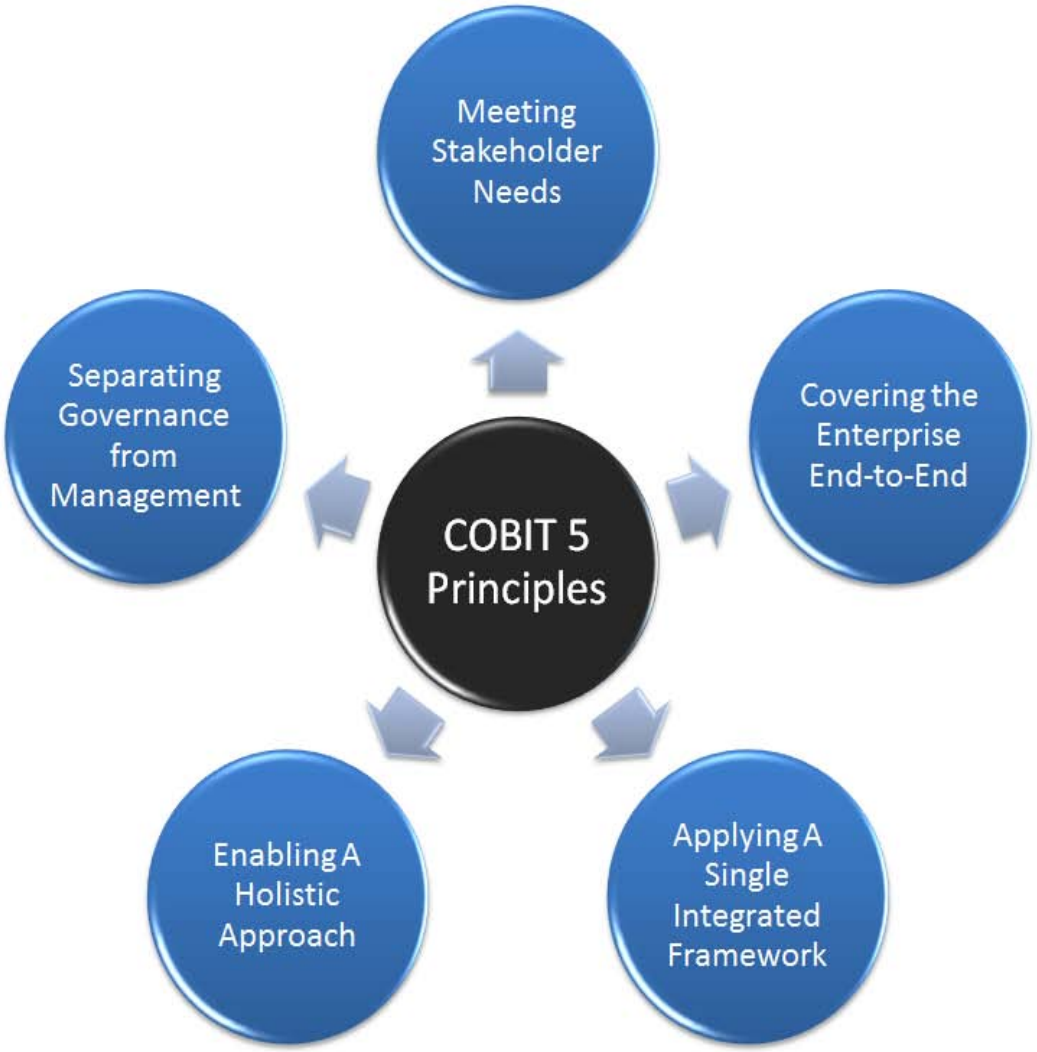
COBIT 5

Prof. dr. Wim Van Grembergen

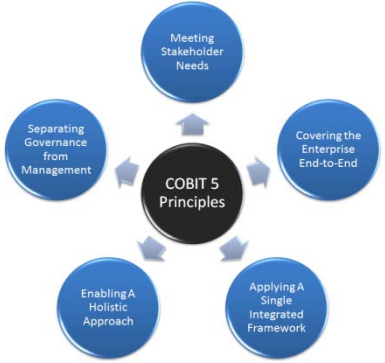
University of Antwerp (UA)
Antwerp Management School (AMS)
IT Alignment and Governance Research Institute (ITAG)
wim.vangrembergen@ua.ac.be

COBIT 5

antwerp management school



Meeting stakeholder needs

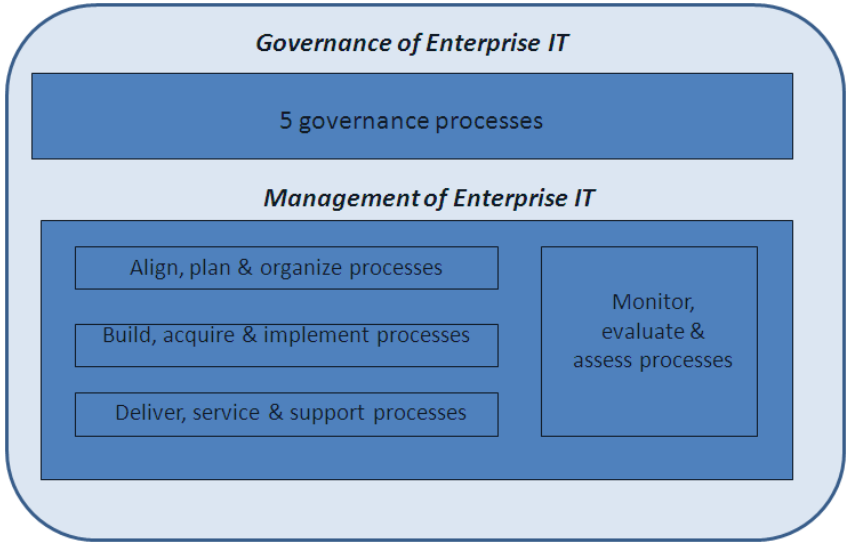


antwerp management school

Enterprise Goals

IT related Goals

COBIT 5 Processes

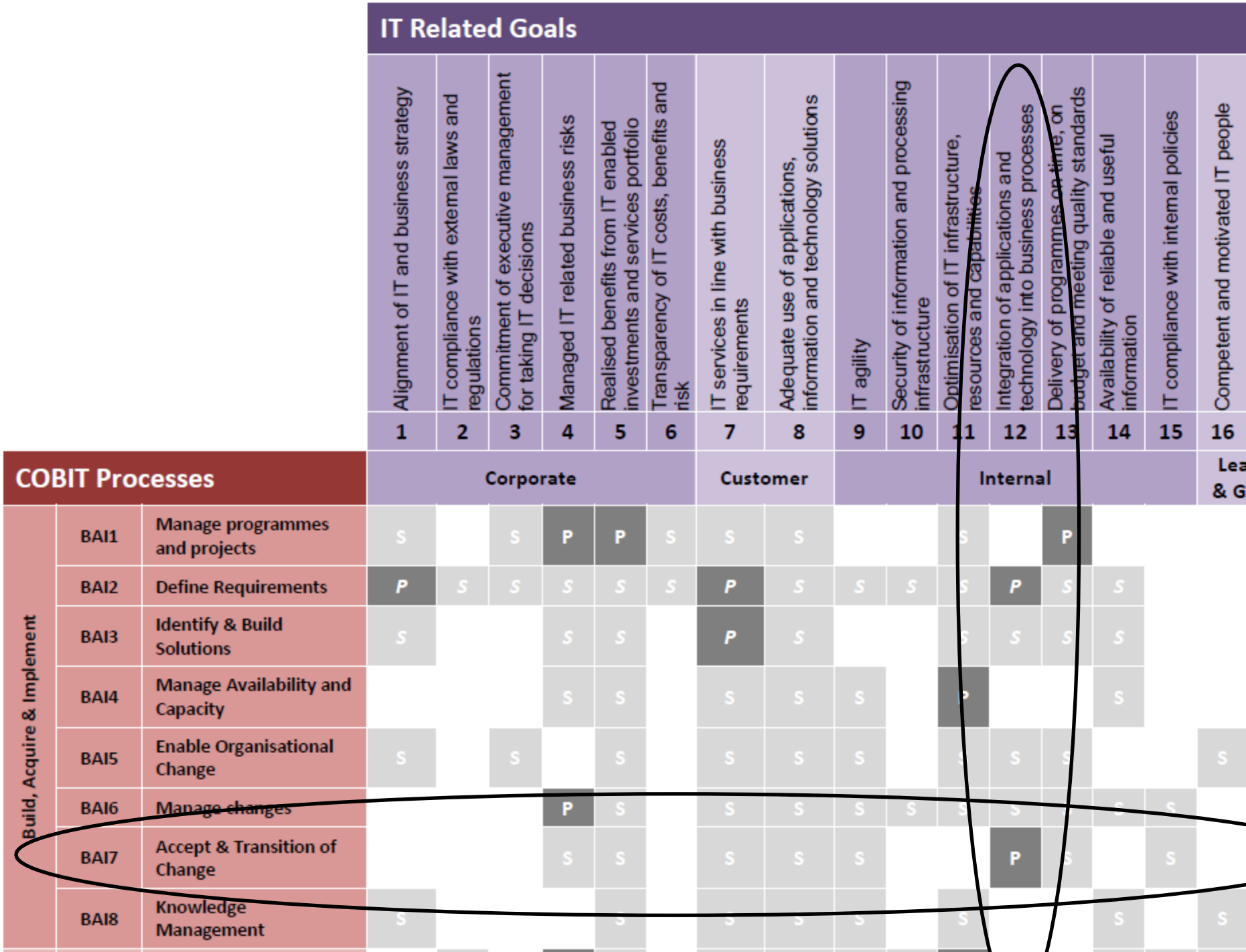


antwerp management school

Portfolio of competitive products and services

			Enterprise Goals																
			Compliance with external laws and regulations	Managed business risks	Portfolio of competitive products and services	Stakeholder value of business investments	Financial transparency	Customer orientation and service culture	Business service continuity and availability	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			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

Integration of applications into business processes


IT Related Goals
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
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
COBIT Processes
Corporate
Customer
Internal
Lea & G
Build, Acquire & Implement
BAI1 Manage programmes and projects
BAI2 Define Requirements
BAI3 Identify & Build Solutions
BAI4 Manage Availability and Capacity
BAI5 Enable Organisational Change
BAI6 Manage changes
BAI7 Accept & Transition of Change
BAI8 Knowledge Management

End-to-End

antwerp management school

COBIT 4.1

VALIT 2.0

RISKIT

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

antwerp management school

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		

Roles and organisational structures

antwerp management school

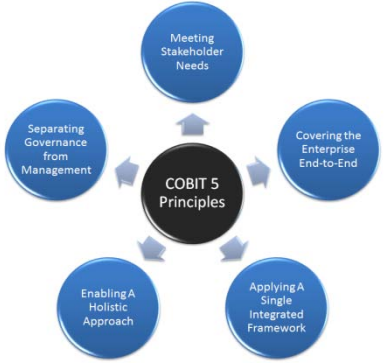
Role/Structure	Definition/Description
Board	The group of the most senior executives and/or non-executive directors of the enterprise who are accountable for the governance of the enterprise and have overall control of its resources
Chief Executive Officer (CEO)	The highest-ranking officer who is in charge of the total management of the enterprise
Chief Financial Officer (CFO)	The most senior official of the enterprise who is accountable for all aspects of financial management including financial risk and controls and reliable and accurate accounts
Chief Operating Officer (COO)	The most senior official of the enterprise who is accountable for the operation of the enterprise
Chief Risk Officer (CRO)	The most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.
Chief Information Officer (CIO)	The most senior official of the enterprise who is responsible for aligning IT and business strategies and accountable for planning, resourcing and managing the delivery of IT services and solutions to support enterprise objectives
Chief Information Security Officer (CISO)	The most senior official of the enterprise who is accountable for the security of enterprise information in all its forms
Business Executive	A senior management individual accountable for the operation of a specific business unit or subsidiary

antwerp management school

Business Executive	A senior management individual accountable for the operation of a specific business unit or subsidiary
Business Process Owner	An individual accountable for the performance of a process in realising its objectives, driving process improvement and approving process changes.
Strategy (IT Executive) 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 portfolios of IT-enabled investments, IT services and IT assets, ensuring that value is delivered and risks are managed. The committee is normally chaired by a board member, not the CIO.
(Project and Programme) Steering Committees	A group of stakeholders and experts who are accountable for guidance of programmes and projects, including management and monitoring of plans, allocation of resources, delivery of benefits and value, and management of programme and project risks
Architecture Board	A group of stakeholders and experts who are accountable for guidance on enterprise architecture-related matters and decisions, and for setting architectural policies and standards
Enterprise Risk Committee	The group of executives of the enterprise who are accountable for the enterprise-level collaboration and consensus required to support enterprise risk management activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the Enterprise Risk Committee.
Head of Human Resources	The most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise
Compliance	The function in the enterprise responsible for guidance on legal, regulatory and contractual compliance
Audit	The function in the enterprise responsible for provision of internal audits

Head of Architect	A senior individual accountable for the enterprise architecture process
Head of Development	A senior individual accountable for IT-related solution development processes
Head of IT Operations	A senior individual accountable for the IT operational environments and infrastructure
Head of IT Administration	A senior individual accountable for IT-related records and responsible for supporting IT-related administrative matters
Programme and Project Management Office (PMO)	The function responsible for supporting programme and project managers, and gathering, assessing and reporting information about the conduct of their programmes and constituent projects
Value Management Office (VMO)	The function that acts as the secretariat for managing investment and service portfolios, including assessing and advising on investment opportunities and business cases, recommending value governance/management methods and controls, and reporting on progress on sustaining and creating value from investments and services
Service Manager	An individual who manages the development, implementation, evaluation and on-going management of new and existing products and services for a specific customer (user) or group of customers (users)
Information Security Manager	An individual who manages, designs, oversees and/or assesses an enterprise's information security
Business Continuity Manager	An individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
Privacy Officer	An individual who is responsible for monitoring the risks and business impacts of privacy laws and for guiding and co-ordinating the implementation of policies and activities that will ensure that the privacy directives are met. Also called 'Data Protection Officer'

Governance and management



antwerp management school

Governance of Enterprise IT

5 governance processes

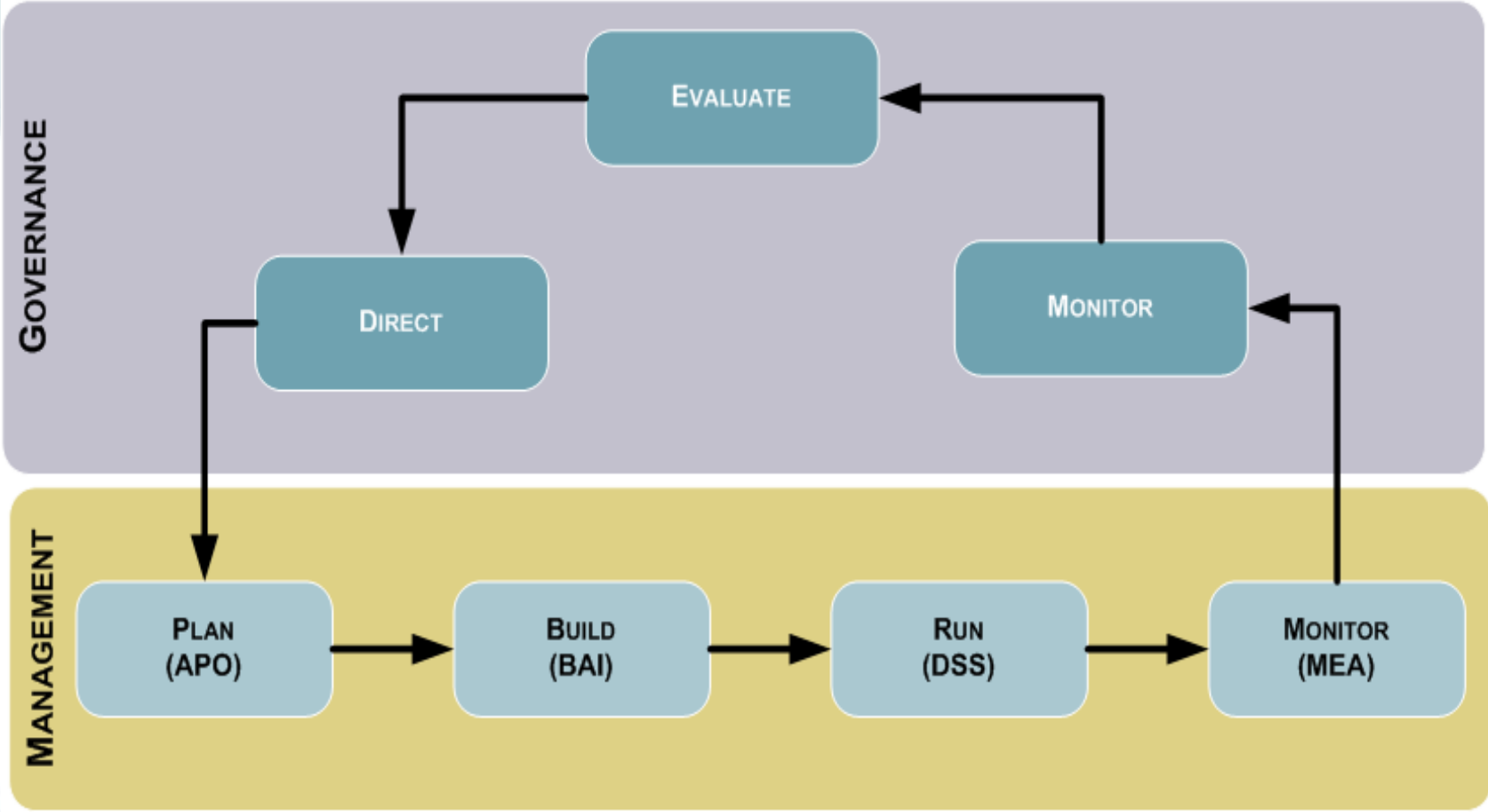
Management of Enterprise IT

Align, plan & organize processes

Build, acquire & implement processes

Deliver, service & support processes

Monitor, evaluate & assess processes



- **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.

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.

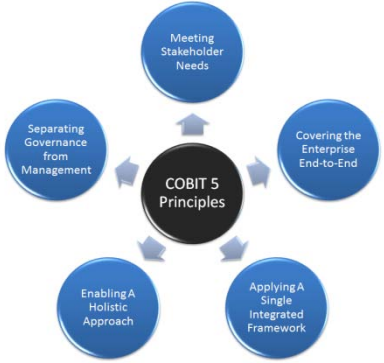
3 Assess the effectiveness of the governance design and identify actions to rectify any deviations found.

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

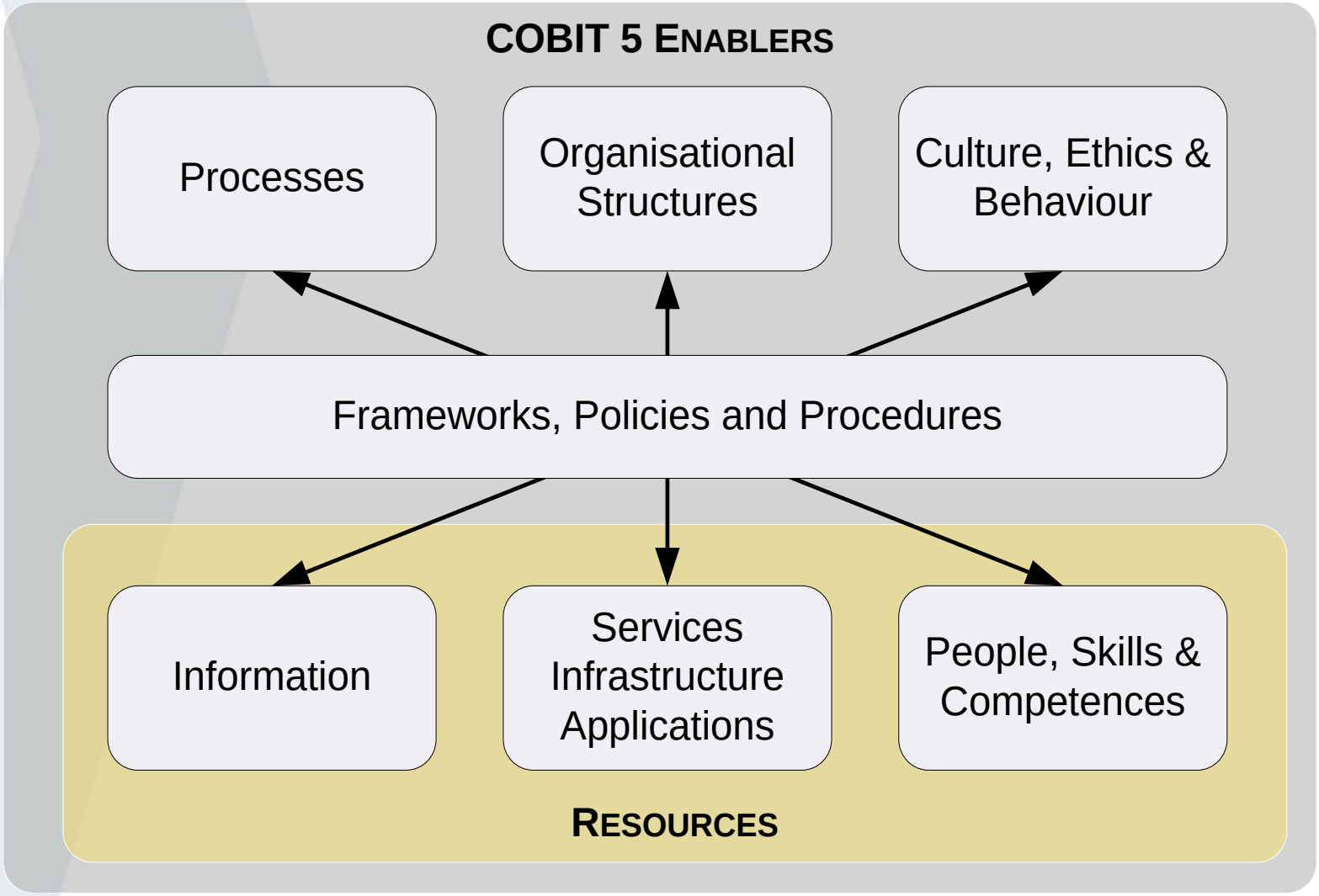
5 Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.

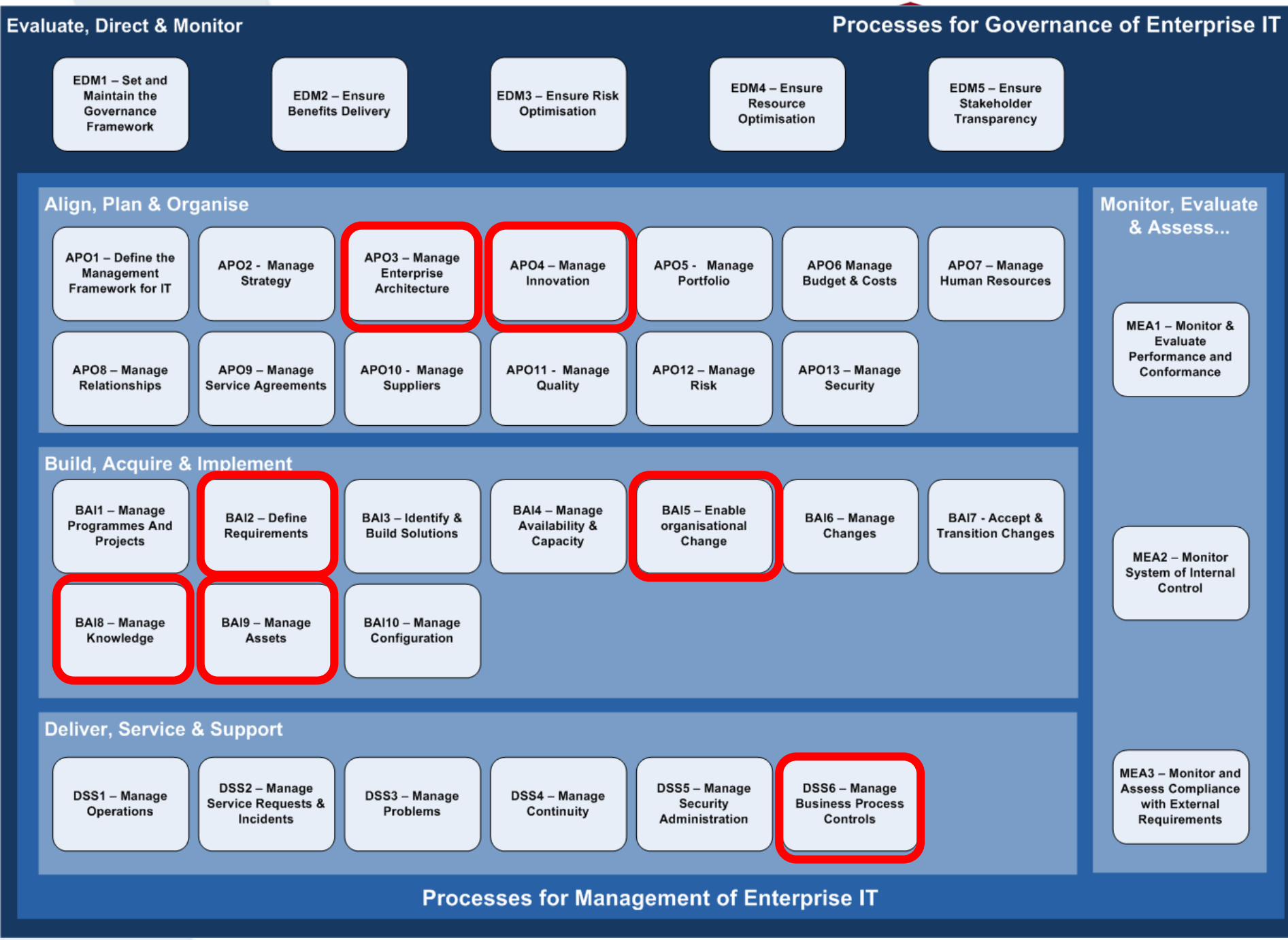
6 Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.

Holistic view



antwerp management school




Evaluate, Direct & Monitor
Processes for Governance of Enterprise IT
EDM1 – Set and Maintain the Governance Framework
EDM2 – Ensure Benefits Delivery
EDM3 – Ensure Risk Optimisation
EDM4 – Ensure Resource Optimisation
EDM5 – Ensure Stakeholder Transparency
Align, Plan & Organise
APO1 – Define the Management Framework for IT
APO2 - Manage Strategy
APO3 – Manage Enterprise Architecture
APO4 – Manage Innovation
APO5 - Manage Portfolio
APO6 Manage Budget & Costs
APO7 – Manage Human Resources
APO8 – Manage Relationships
APO9 – Manage Service Agreements
APO10 - Manage Suppliers
APO11 - Manage Quality
APO12 – Manage Risk
APO13 – Manage Security
Build, Acquire & Implement
BAI1 – Manage Programmes And Projects
BAI2 – Define Requirements
BAI3 – Identify & Build Solutions
BAI4 – Manage Availability & Capacity
BAI5 – Enable organisational Change
BAI6 – Manage Changes
BAI7 - Accept & Transition Changes
BAI8 – Manage Knowledge
BAI9 – Manage Assets
BAI10 – Manage Configuration
Deliver, Service & Support
DSS1 – Manage Operations
DSS2 – Manage Service Requests & Incidents
DSS3 – Manage Problems
DSS4 – Manage Continuity
DSS5 – Manage Security Administration
DSS6 – Manage Business Process Controls
Monitor, Evaluate & Assess...
MEA1 – Monitor & Evaluate Performance and Conformance
MEA2 – Monitor System of Internal Control
MEA3 – Monitor and Assess Compliance with External Requirements
Processes for Management of Enterprise IT

antwerp management school

7 nearly new processes

APO03	Manage Enterprise Architecture	Area: Management
		Domain: Align, Plan and Organise

Process Description

Establish a common architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.

APO03.01	Develop the enterprise architecture vision.
APO03.02	Define reference architecture.
APO03.03	Select opportunities and solutions.
APO03.04	Define architecture implementation.
APO03.05	Provide enterprise architecture services.

antwerp management school

7 nearly new processes

APO04	Manage Innovation	Area: Management
		Domain: Align, Plan and Organise

Process Description

Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.

APO04.01	Create an environment conducive to innovation.
APO04.02	Maintain an understanding of the enterprise environment.
APO04.03	Monitor and scan the technology environment.
APO04.04	Assess the potential of emerging technologies and innovation ideas.
APO04.05	Recommend appropriate further initiatives.
APO04.06	Monitor the implementation and use of innovation.

antwerp management school

7 nearly new processes

BAI02	Define Requirements	Area: Management
		Domain: Build, Acquire and Implement

Process Description

Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.

BAI02.01	Define and maintain business functional and technical requirements.
BAI02.02	Perform a feasibility study and formulate alternative solutions.
BAI02.03	Manage requirements risk.
BAI02.04	Obtain approval of requirements and solutions.

antwerp management school

7 nearly new processes

BAI05	Enable Organisational Change	Area: Management
		Domain: Build, Acquire and Implement

Process Description

Maximise the likelihood of successfully implementing sustainable enterprisewide organisational change quickly and with reduced risk covering the complete life cycle of the change and all affected stakeholders in the business and IT.

BAI05.01	Establish the desire to change.	BAI05.04	Empower role players and identify short-term wins.
BAI05.02	Form an effective implementation team.	BAI05.05	Enable operation and use.
BAI05.03	Communicate desired vision.	BAI05.06	Embed new approaches.
		BAI05.07	Sustain changes.

7 nearly new processes

antwerp management school

BAI08	Manage Knowledge	Area: Management
		Domain: Build, Acquire and Implement

Process Description

Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organising, maintaining, use and retirement of knowledge.

BAI08.01	Nurture and facilitate a knowledge-sharing culture.
BAI08.02	Identify and classify sources of information.
BAI08.03	Organise and contextualise information into knowledge.
BAI08.04	Use and share knowledge.
BAI08.05	Evaluate and retire information.

antwerp management school

7 nearly new processes

BAI09	Manage Assets	Area: Management
		Domain: Deliver, Service and Support

Process Description

Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose) they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimum number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with licence agreements.

BAI09.01	Identify and record current assets.
BAI09.02	Manage critical assets.
BAI09.03	Manage the asset life cycle.
BAI09.04	Optimise asset costs.
BAI09.05	Manage licences.

antwerp management school

7 nearly new processes

DSS06	Manage Business Process Controls	Area: Management
		Domain: Deliver, Service and Support

Process Description

Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.

DSS06.01	Align control activities embedded in business processes with enterprise objectives.	DSS06.03	Manage roles, responsibilities, access privileges and levels of authority.	DSS06.05	Ensure traceability of Information events and accountabilities.
DSS06.02	Control the processing of information	DSS06.04	Manage errors and exceptions.	DSS06.06	Secure information assets.

antwerp management school

For each COBIT process:

- Process description
- Process purpose statement
- IT related goals & metrics
- Process goals & metrics
- RACI chart
- Management practices + inputs/outputs
- Activities

Example

antwerp management school

DSS02 Manage service request and incidents

DSS02	Manage Service Requests and Incidents	Area: Management
		Domain: Deliver, Service and Support

Process Description

Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.

Process Purpose Statement

Achieve increased productivity and minimise disruptions through quick resolution of user queries and incidents.

Example

antwerp management school

DSS02 Manage service request and incidents

The process supports the achievement of a set of primary IT-related goals:

IT related Goal		Related Metrics
04	Managed IT-related business risks	Percent critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent enterprise risk assessments including IT-related risks Update frequency of risk profile
07	Delivery of IT services in line with business requirements	Number of business disruptions due to IT service incidents Percent business stakeholders satisfied that IT service delivery meets agreed-upon service levels Percent users satisfied with quality of IT service delivery

Example

DSS02 Manage service request and incidents

antwerp management school

Process Goals and Metrics

Process Goal		Related Metrics
1	IT-related services are available for use.	Mean time between incidents per IT-enabled service Number and percent incidents causing disruption to business-critical processes
2	Incidents are resolved according to the agreed service levels.	Percent incidents resolved within an agreed-upon/acceptable period of time
3	Service requests are dealt with according to agreed service levels and to the satisfaction of users.	Level of user satisfaction with service request fulfilment Mean elapsed time for handling each type of service request

Example

antwerp management school

DSS02 Manage service request and incidents

RACI Chart

Key Management 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
DSS02.01	Define incident and service request classification schemes.						C					I	I						A	C	R	R		R	C	C	C
DSS02.02	Record, classify and prioritise requests and incidents.						I					I	I									A		R			I
DSS02.03	Verify, approve and fulfil service requests.						R												I		R	R		A			

Example

antwerp management school

DSS02 Manage service request and incidents

Process Practices, Inputs/Outputs and Activities

Management Practice		Inputs From	Inputs Description	Outputs Description	Outputs To
DSS02.01	**Define incident and service request classification schemes.** Define incident and service request classification schemes and models.	APO09.03	SLAs	Incident and service request classification schemes and models	Internal
		BAI10.02	Configuration repository	Rules for incident escalation	Internal
		BAI10.03	Updated repository with configuration items	Criteria for problem registration	DSS03.01
		BAI10.04	Configuration status reports		
		DSS01.03	Asset monitoring rules and event conditions		
		DSS03.01	Problem classification scheme		
		DSS04.03	Incident response actions and communications		

Activities

Example

antwerp management school

DSS02 Manage service request and incidents

Activities
1 Define incident and service request classification and prioritisation schemes and criteria for problem registration, to ensure consistent approaches for handling, informing users and conducting trend analysis.
2 Define incident models for known errors to enable efficient and effective resolution.
3 Define service request models per service request type to enable self-help and efficient service for standard requests.
4 Define incident escalation rules and procedures, especially for major incidents and security incidents.
5 Define incident and request knowledge sources and their use.

antwerp management school

- 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