COBIT 5

SoftEng
http://softeng.polito.it

COBIT

- COBIT (Control Objectives for Information and Related Technology)
- Issued by ISACA and IT Governance Institute

- Reference document for
  - IT governance
  - IT process and risk management
- Aims at aligning Business and IT Strategy
- Process oriented view starting with business requirements
- For managers and auditors

COBIT 5 – key elements

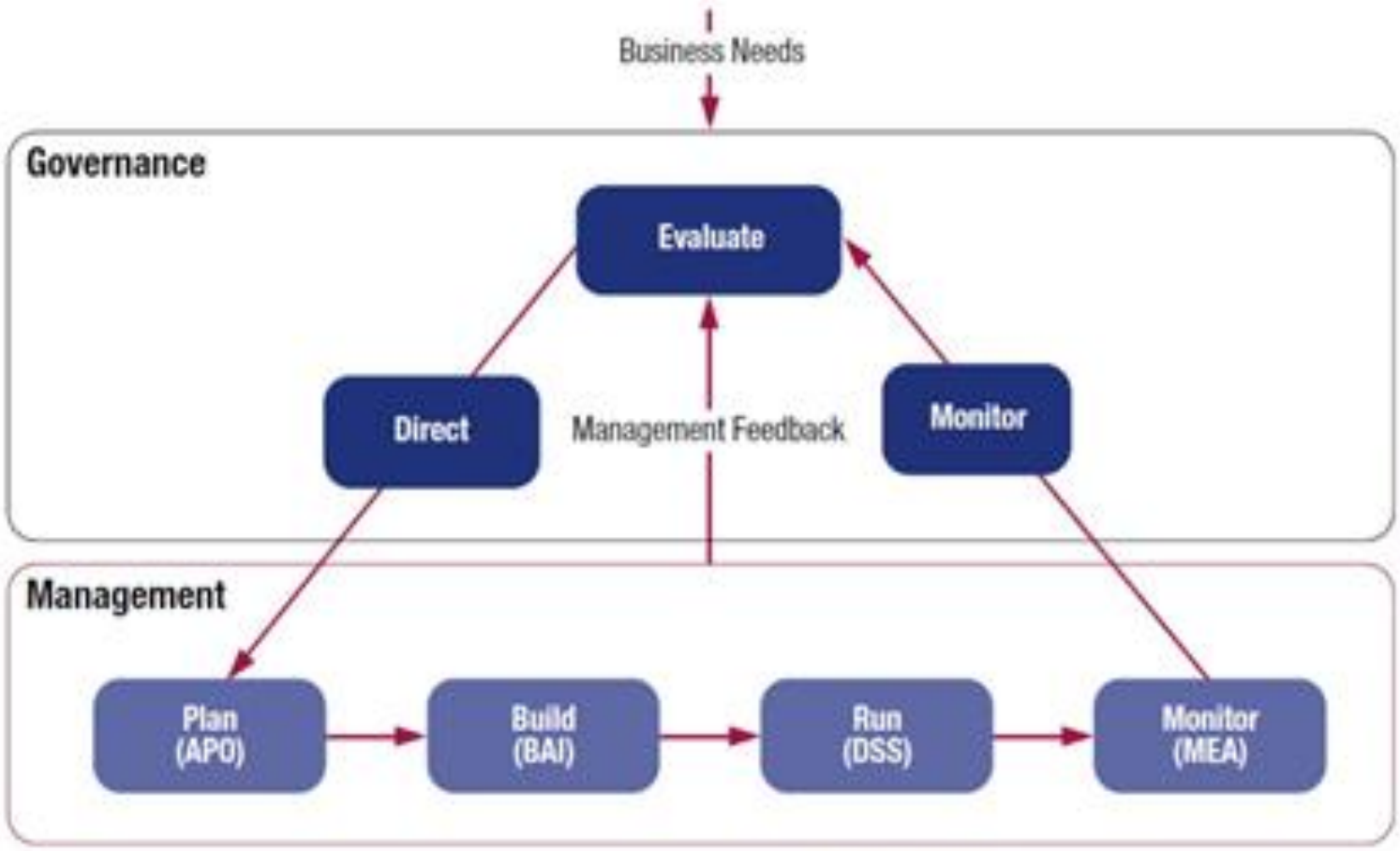
- Domains Processes Activities
- Principles
- Enablers
- Lifecycle approach
- Process Capability Model

PROCESSES

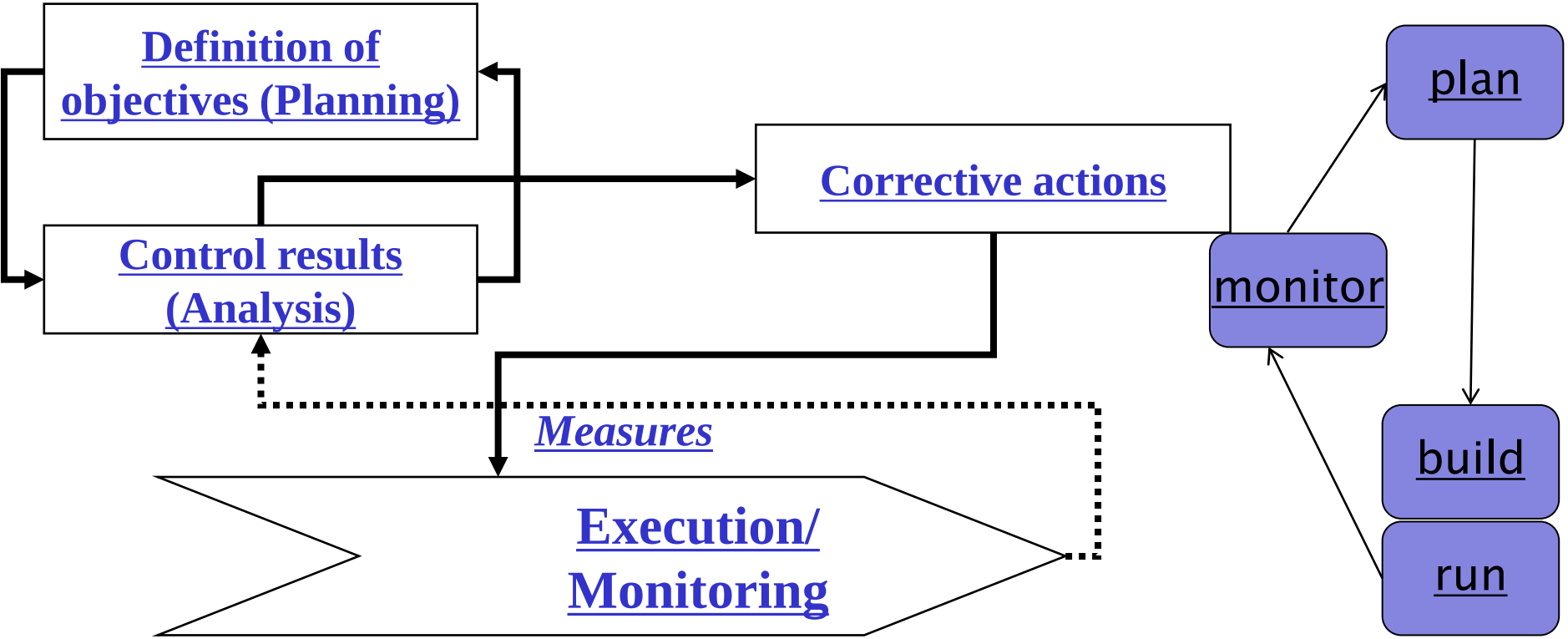
Processes

- Governance
- Management
  - Plan
  - Build
  - Run
  - Monitor

Governance and Management



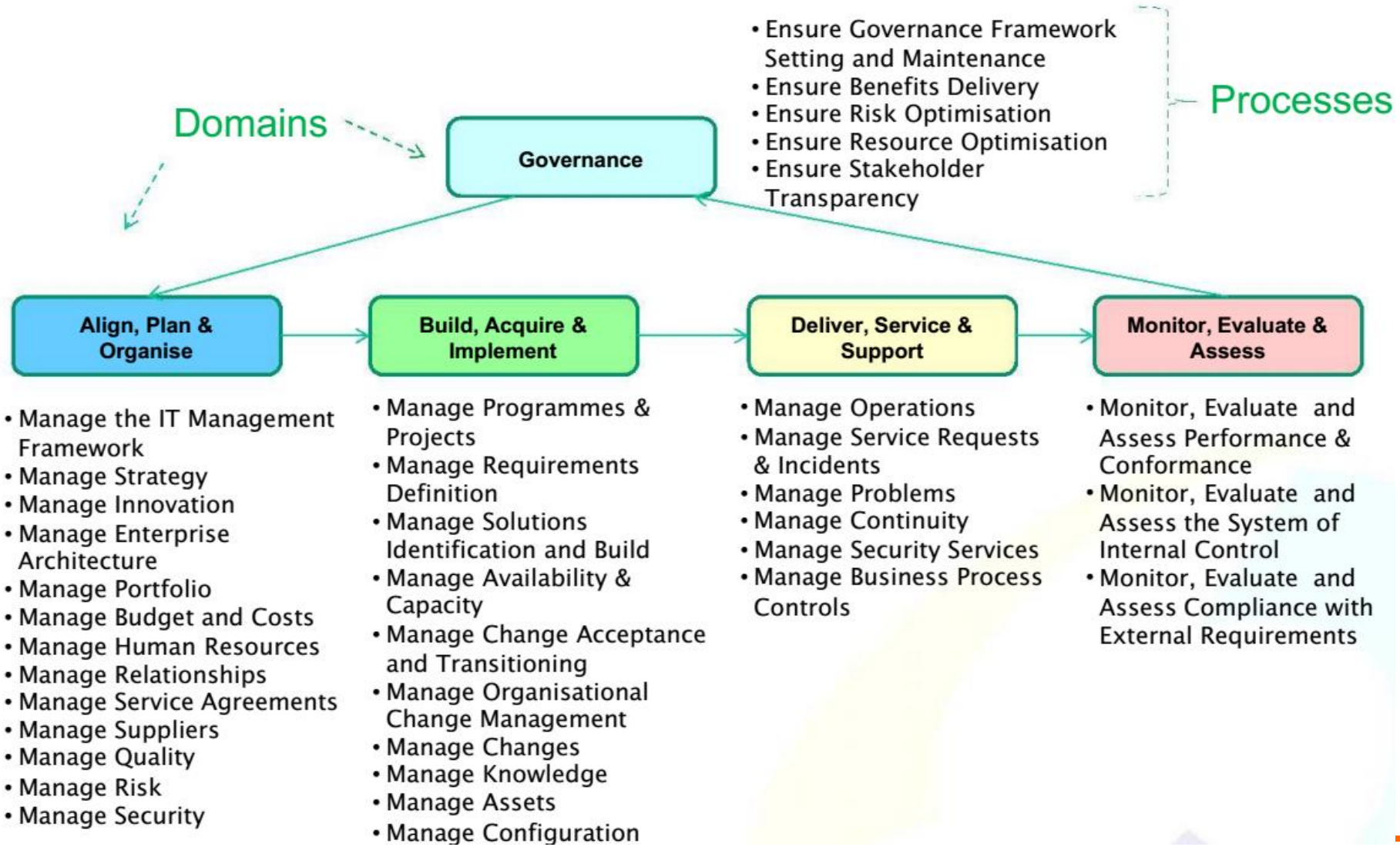
The control loop



Processes

- Domains = group of processes
  - Governance
  - Management
    - Plan
    - Build
    - Run
    - Monitor
- Each process further decomposed in activities and practices
- Input / output list per each activity
- Measures

Domains, processes, activities



Domain: APO

Align Plan Organize

- Manage the IT Management Framework
- Manage Strategy
- Manage Innovation
- Manage Enterprise Architecture
- Manage Portfolio
- Manage Budget and Costs
- Manage Human Resources
- Manage Relationships
- Manage Service Agreements
- Manage Suppliers
- Manage Quality
- Manage Risk
- Manage security

Domain: BAI

Build Acquire Implement

- BAI01 Manage programmes and projects
- BAI02 Manage requirements definition
- BAI03 Manage solutions identification and build
- BAI04 Manage availability and capacity
- BAI05 Manage change acceptance and transitioning
- BAI06 Manage organisational change management
- BAI07 Manage changes
- BAI08 Manage knowledge
- BAI09 Manage assets
- BAI10 Manage configuration

BAI

- Programme == many related projects
- For one project:
  - Define requirements
  - Identify solutions, build
- Horizontal / support activities
  - Change test and deploy
  - Org change
  - Changes, knowledge, assets, configuration

Domain: DSS

Deliver Service and Support

- Manage operations
- Manage service requests and incidents
- Manage problems
- Manage continuity
- Manage security services
- Manage business process controls

Domain: MEA

- Monitor evaluate and assess
  - MEA performance and conformance
  - MEA the system of internal control
  - MEA compliance with external requirements

Domain: Governance

Ensure Governance Framework Setting and Maintenance

Ensure Benefits Delivery

Ensure Risk Optimisation

Ensure Resource Optimisation

Ensure Stakeholder Transparency

Process → activity

BAI01 Manage programmes and projects

process

activity

- Maintain a standard approach for programme and project management
- Initiate a programme
- Manage stakeholder engagement
- Develop and maintain the programme plan.
- Launch and execute the programme
- Monitor, control and report on the programme outcomes.
- Start up and initiate projects within a programme.
- Plan projects
- ….
- Close a project
- Close a programme

Activity → practice

process

BAI01 Manage programmes and projects

activity

- Maintain a standard approach for programme and project management
- Initiate a programme

practice

  - Agree on programme sponsorship. Appoint a programme committee with members who have a strategic interest in the programme and capability of investment + decision making
  - Confirm the programme mandate with sponsors and stakeholders
  - Develop a detailed business case for the programme
  - ….

RACI charts

- For each practice a RACI chart

R Responsible: The person who does the work to achieve the task. One or more persons

A Accountable: The person who is accountable for the correct and thorough completion of the task. ONE person. R reports to A, A approves work.

C Consulted: The people who provide information – Many persons , 2 way communication

I Informed: The people kept informed of progress – Many persons 1 way communication

RACI chart, BAI 01 practices

BAI01 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
BAI01.01 Maintain a standard approach for programme and project management.	I	A	C	C	R		R		C		C					C	C	R								
BAI01.02 Initiate a programme.	I	R	C	C	A	R	R	R	R									C	C	C	C		C	C	C	C
BAI01.03 Manage stakeholder engagement.		A	C	R	R	R	C	R	I	I								R	C	C	C		C	C	C	C
BAI01.04 Develop and maintain the programme plan.			C	C	A	C		R	R	R	C					C	C	C	C	C	C		C	C	C	C
BAI01.05 Launch and execute the programme.			C	C	A	R		R	R	I	C					C	C	R	R	R	R		C	C	C	C
BAI01.06 Monitor, control and report on the programme outcomes.					A	C	I	R	R	R	C					C	R	R		C	C			C		
BAI01.07 Start up and initiate projects					R	R	I	A	R									C	C	R	C		C	C	C	C

Input / outputs per activity

Management Practice	Inputs		Outputs	
BAI01.02 Initiate a programme. Initiate a programme to confirm the expected benefits and obtain authorisation to proceed. This includes agreeing on programme sponsorship, confirming the programme mandate through approval of the conceptual business case, appointing programme board or committee members, producing the programme brief, reviewing and updating the business case, developing a benefits realisation plan, and obtaining approval from sponsors to proceed.	**From**	**Description**	**Description**	**To**
	AP003.04	• Implementation phase descriptions • Resource requirements	Programme concept business case	AP005.03
	AP005.03	Programme business case	Programme mandate and brief	AP005.03
	AP007.03	Skills and competencies matrix	Programme benefit realisation plan	AP005.03 AP006.05
	BAI05.02	Common vision and goals		

Measures per IT goals

The process supports the achievement of a set of primary IT-related goals:	
IT-related Goal	**Related Metrics**
01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
04 Managed IT-related business risk	• Percent of 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 of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	• Number of programmes/projects on time and within budget • Percent of stakeholders satisfied with programme/project quality • Number of programmes needing significant rework due to quality defects • Cost of application maintenance vs. overall IT cost

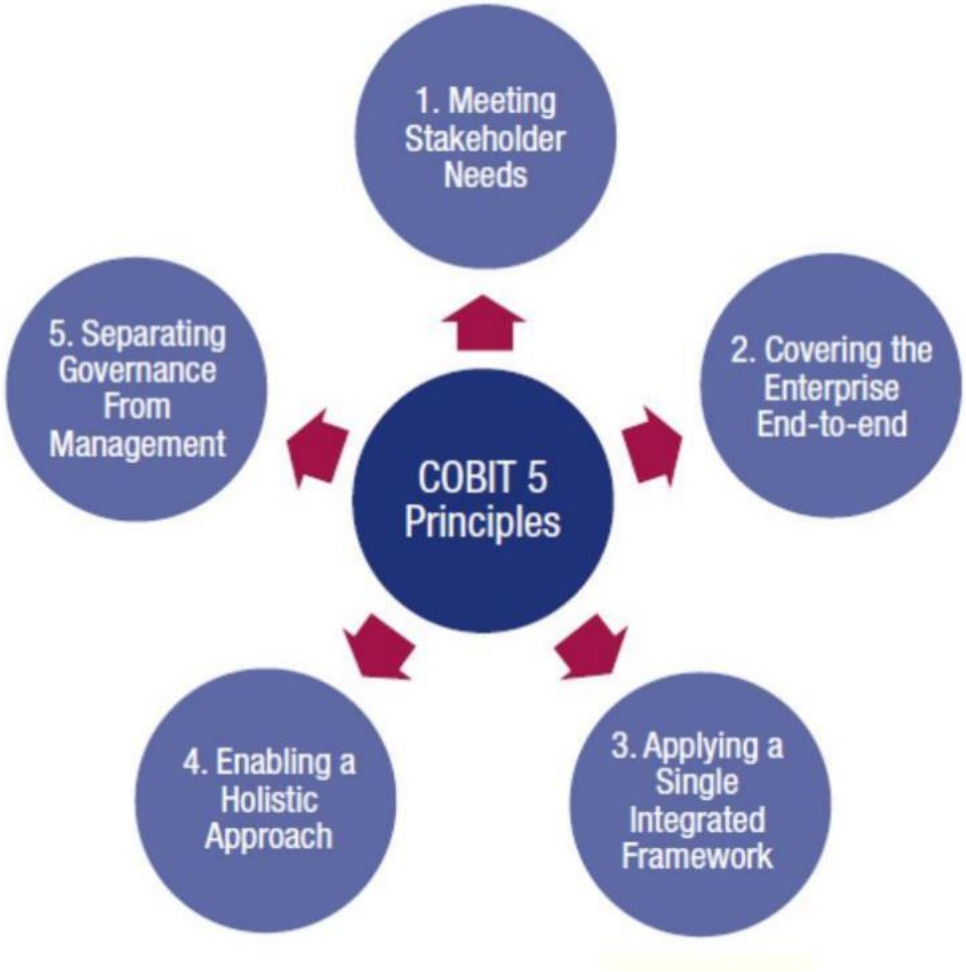
Measures per process goals

BAI process

Process Goals and Metrics	
Process Goal	**Related Metrics**
1. Relevant stakeholders are engaged in the programmes and projects.	• Percent of stakeholders effectively engaged • Level of stakeholder satisfaction with involvement
2. The scope and outcomes of programmes and projects are viable and aligned with objectives.	• Percent of stakeholders approving enterprise need, scope, planned outcome and level of project risk • Percent of projects undertaken without approved business cases
3. Programme and project plans are likely to achieve the expected outcomes.	• Percent of activities aligned to scope and expected outcomes • Percent of active programmes undertaken without valid and updated programme value maps
4. The programme and project activities are executed according to the plans.	• Frequency of status reviews • Percent of deviations from plan addressed • Percent of stakeholder sign-offs for stage-gate reviews of active programmes
5. There are sufficient programme and project resources to perform activities according to the plans.	• Number of resource issues (e.g., skills, capacity)
6. The programme and project expected benefits are achieved and accepted.	• Percent of expected benefits achieved • Percent of outcomes with first-time acceptance • Level of stakeholder satisfaction expressed at project closure review

PRINCIPLES

Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

P1: Meeting stakeholder needs

Enterprise goals (BSC)

Figure 4—COBIT 5 Enterprise Goals				
BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Enterprise goals – metrics

Figure 6—Enterprise Goal Sample Metrics		
BSC Dimension	**Enterprise Goal**	**Metric**
Financial	1. Stakeholder value of business investments	• Percent of investments where value delivered meets stakeholder expectations • Percent of products and services where expected benefits are realised • Percent of investments where claimed benefits are met or exceeded
	2. Portfolio of competitive products and services	• Percent of products and services that meet or exceed targets in revenues and/or market share • Ratio of products and services per life cycle phase • Percent of products and services that meet or exceed customer satisfaction targets • Percent of products and services that provide competitive advantage
	3. Managed business risk (safeguarding of assets)	• Percent of critical business objectives and services covered by risk assessment • Ratio of significant incidents that were not identified in risk assessments vs. total incidents • Frequency of update of risk profile
	4. Compliance with external laws and regulations	• Cost of regulatory non-compliance, including settlements and fines • Number of regulatory non-compliance issues causing public comment or negative publicity • Number of regulatory non-compliance issues relating to contractual agreements with business partners
	5. Financial transparency	• Percent of investment business cases with clearly defined and approved expected costs and benefits • Percent of products and services with defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of enterprise financial information • Percent of service cost that can be allocated to users

IT related goals

Figure 5—IT-related Goals		
IT BSC Dimension	**Information and Related Technology Goal**	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

IT related metrics

Figure 7—IT-related Goal Sample Metrics

BSC Dimension	IT-related Goal	Metric
Financial	01 Alignment of IT and business strategy	• Percent of enterprise strategic goals and requirements supported by IT strategic goals • Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services • Percent of IT value drivers mapped to business value drivers
	02 IT compliance and support for business compliance with external laws and regulations	• Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss • Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment • Number of non-compliance issues relating to contractual agreements with IT service providers • Coverage of compliance assessments
	03 Commitment of executive management for making IT-related decisions	• Percent of executive management roles with clearly defined accountabilities for IT decisions • Number of times IT is on the board agenda in a proactive manner • Frequency of IT strategy (executive) committee meetings • Rate of execution of executive IT-related decisions

Figure 7—IT-related Goal Sample Metrics *(cont.)*

BSC Dimension	IT-related Goal	Metric
Financial *(cont.)*	04 Managed IT-related business risk	• Percent of 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 of enterprise risk assessments including IT-related risk • Frequency of update of risk profile
	05 Realised benefits from IT-enabled investments and services portfolio	• Percent of IT-enabled investments where benefit realisation is monitored through the full economic life cycle • Percent of IT services where expected benefits are realised • Percent of IT-enabled investments where claimed benefits are met or exceeded
	06 Transparency of IT costs, benefits and risk	• Percent of investment business cases with clearly defined and approved expected IT-related costs and benefits • Percent of IT services with clearly defined and approved operational costs and expected benefits • Satisfaction survey of key stakeholders regarding the level of transparency, understanding and accuracy of IT financial information

Enterprise goals – IT goals

Figure 17—Mapping COBIT 5 Enterprise Goals to IT-related Goals

		IT-related Goal	Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented 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	Skilled 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.
			Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					

P5: governance vs management

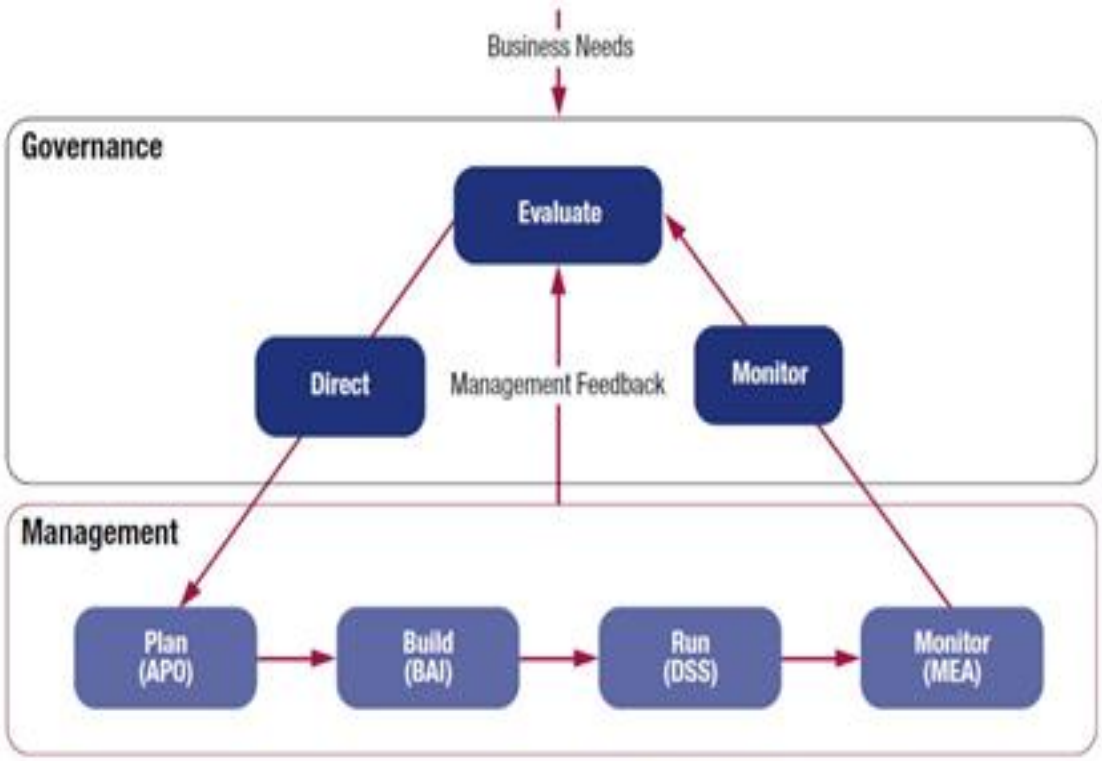
01 Ensure governance framework setting and maintenance.

02 Ensure benefits delivery.

03 Ensure risk optimisation.

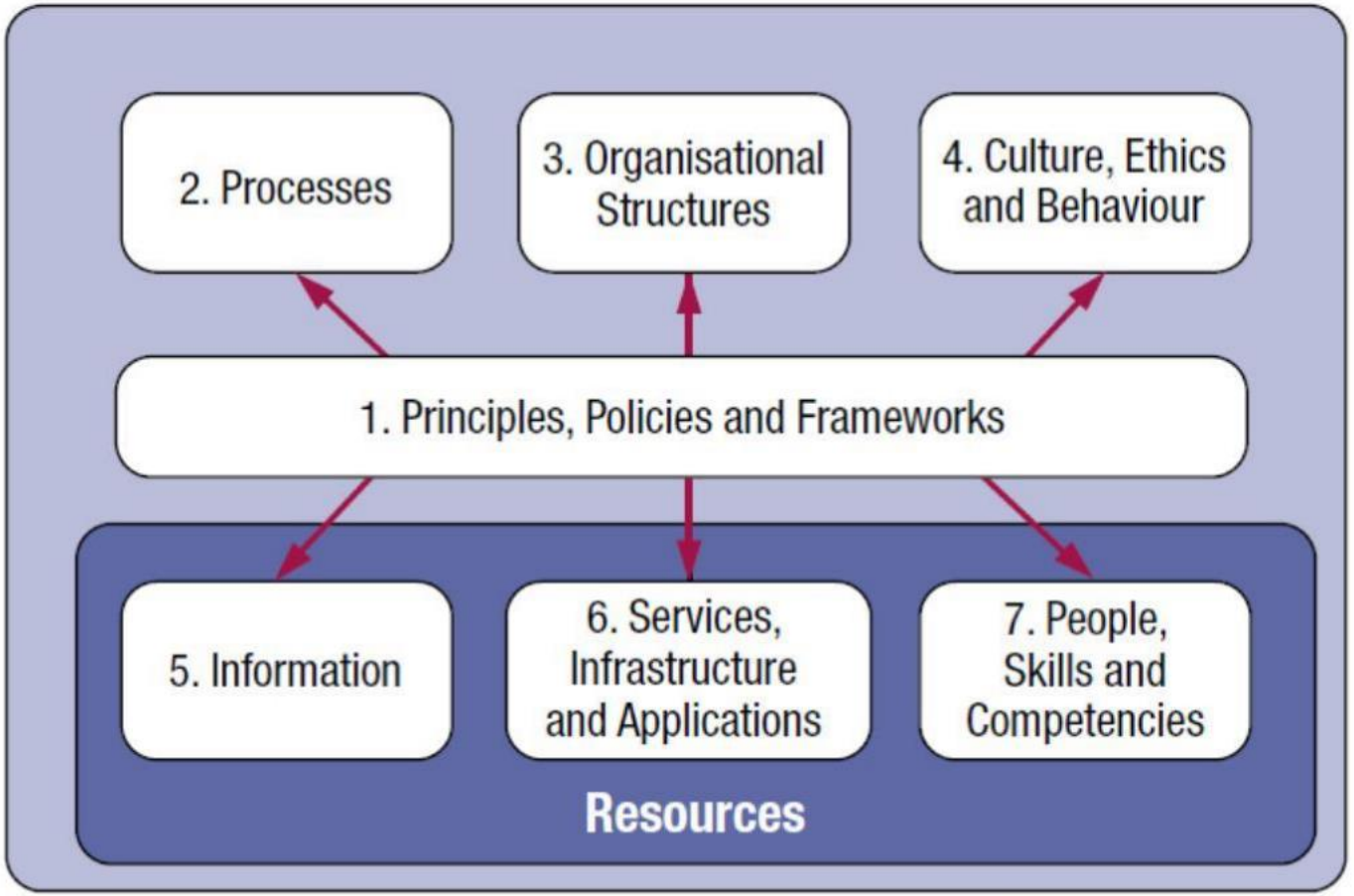
04 Ensure resource optimisation.

05 Ensure stakeholder transparency.



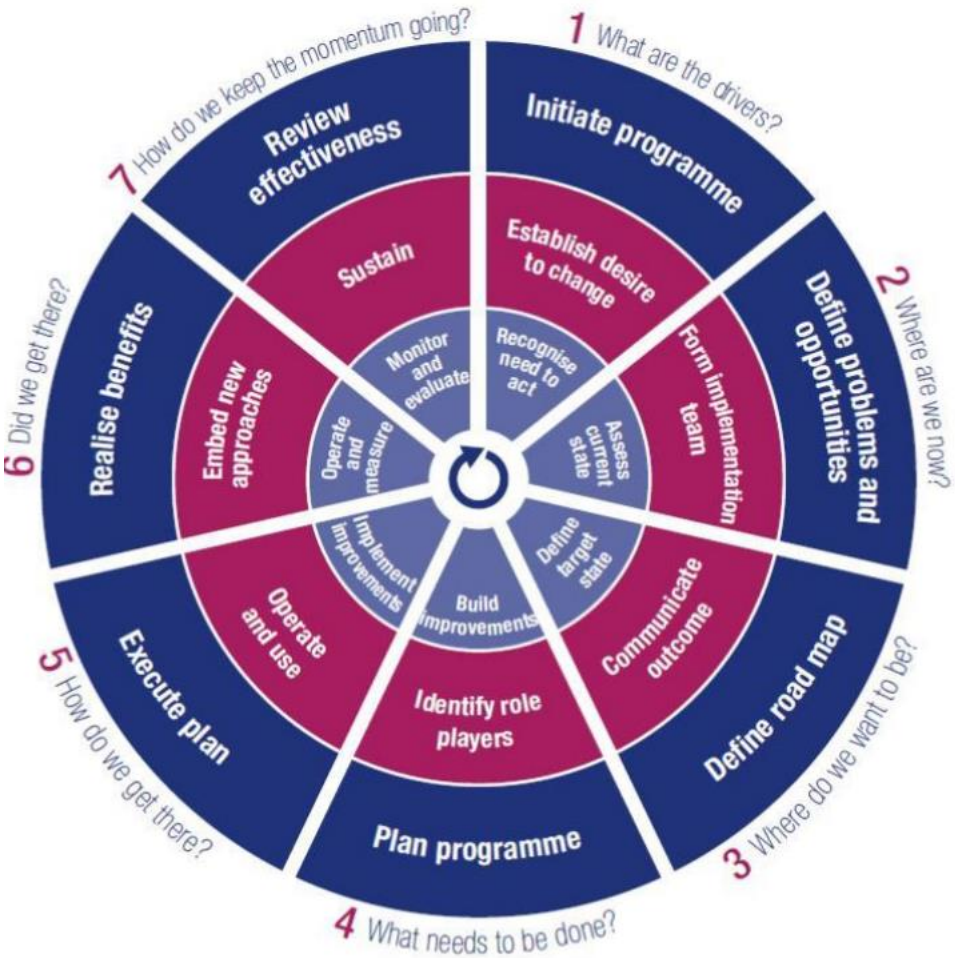
ENABLERS

Enablers


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

LIFE CYCLE APPROACH

Lifecycle approach



- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

PROCESS CAPABILITY MODEL

Process capability Model