

IT Processes



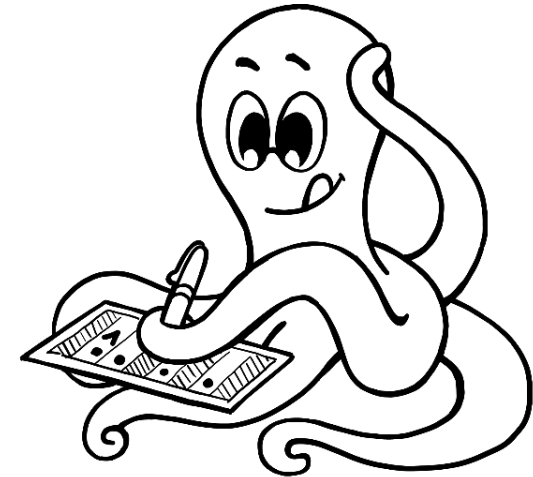
KNOW*Digital*



April 27, 2020
Lionel Pilorget

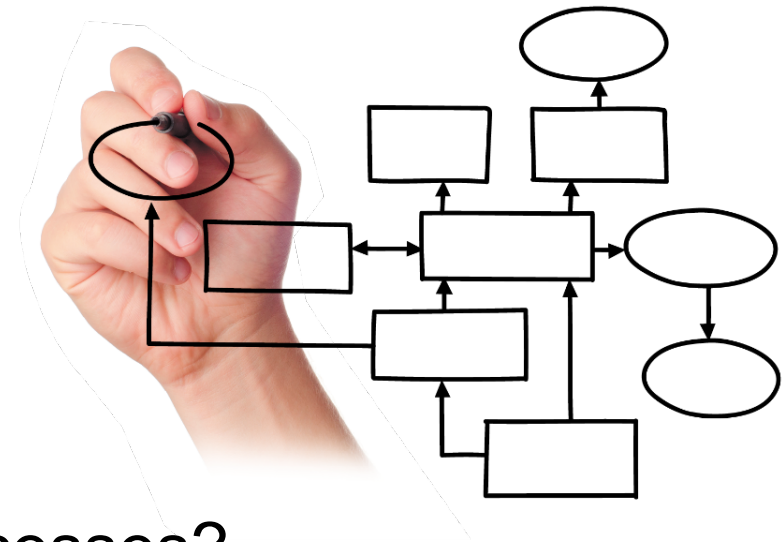


- Modeling Techniques
- Current Standards for IT Processes
- Implementing IT Processes
- Backup Slides for ITIL and COBIT



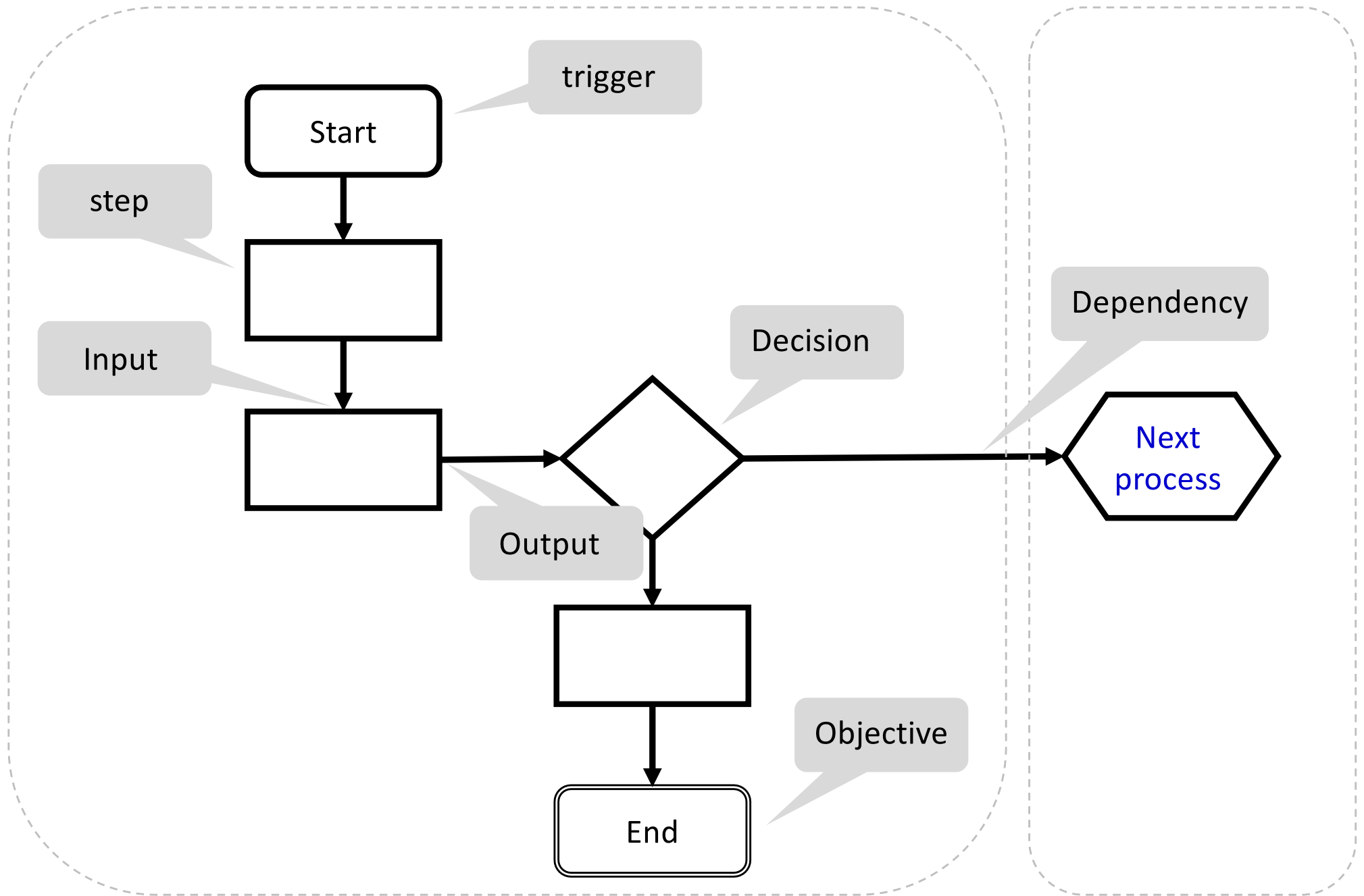


- What is the objective?
- What are the main steps?
- Which roles are needed?
- What triggers the process?
- Which dependencies to other processes?
- What is the output of the process?



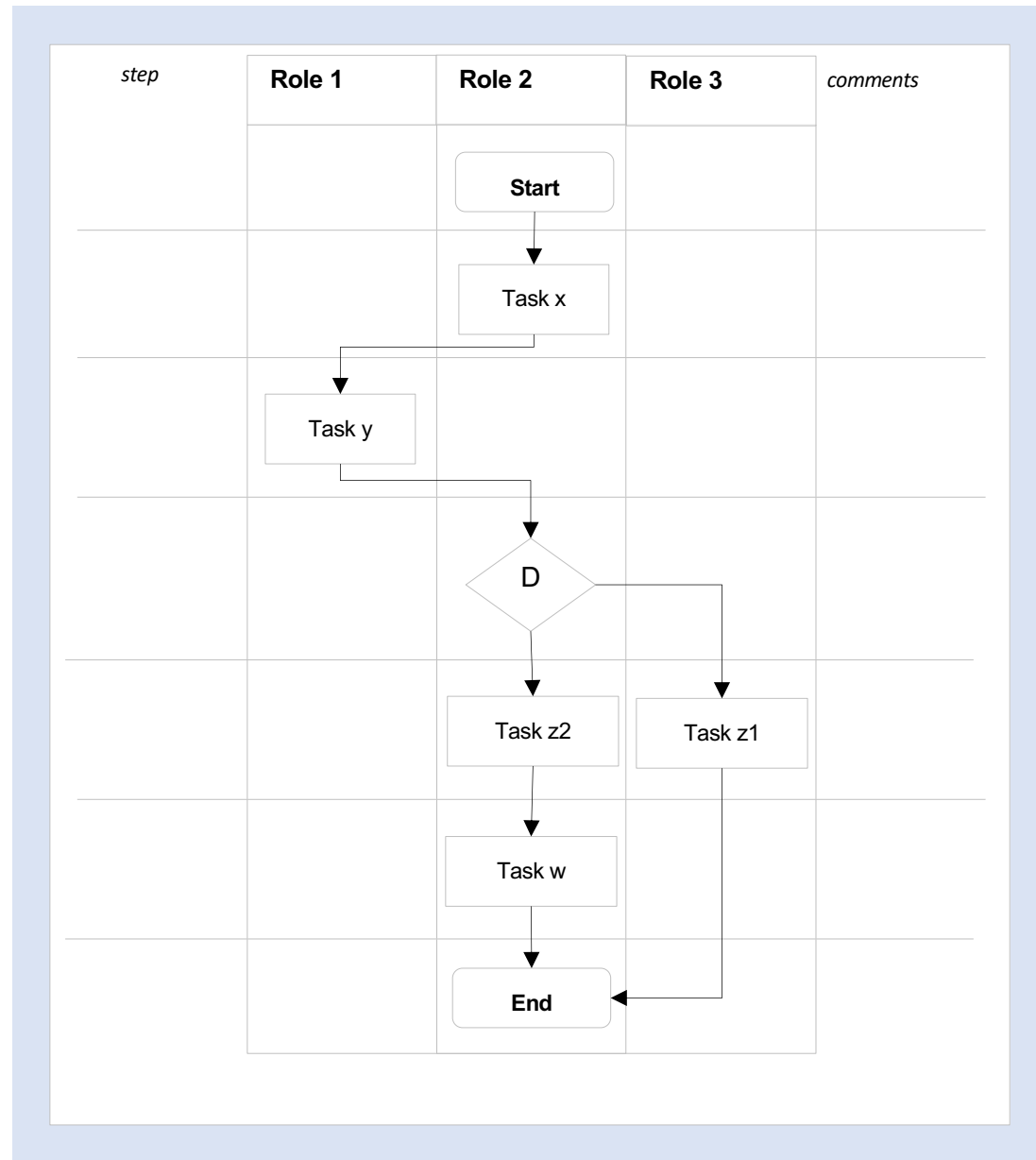
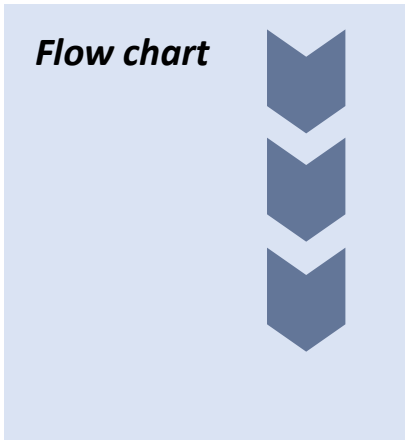
-
- Which KPIs (Key Performance Indicators)?
 - Which CSFs (Critical Success Factors)?

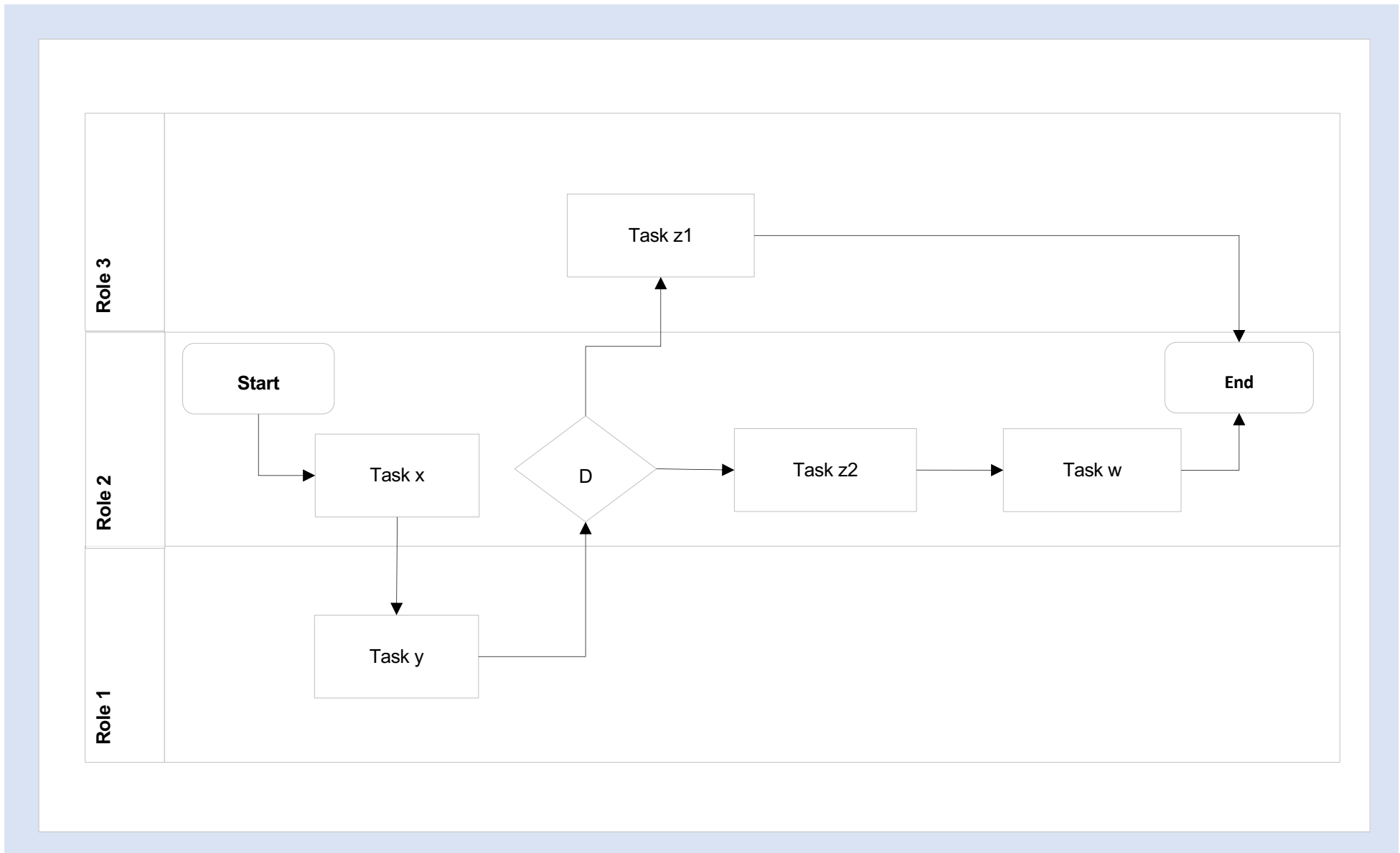
Key Elements for Process Modelling

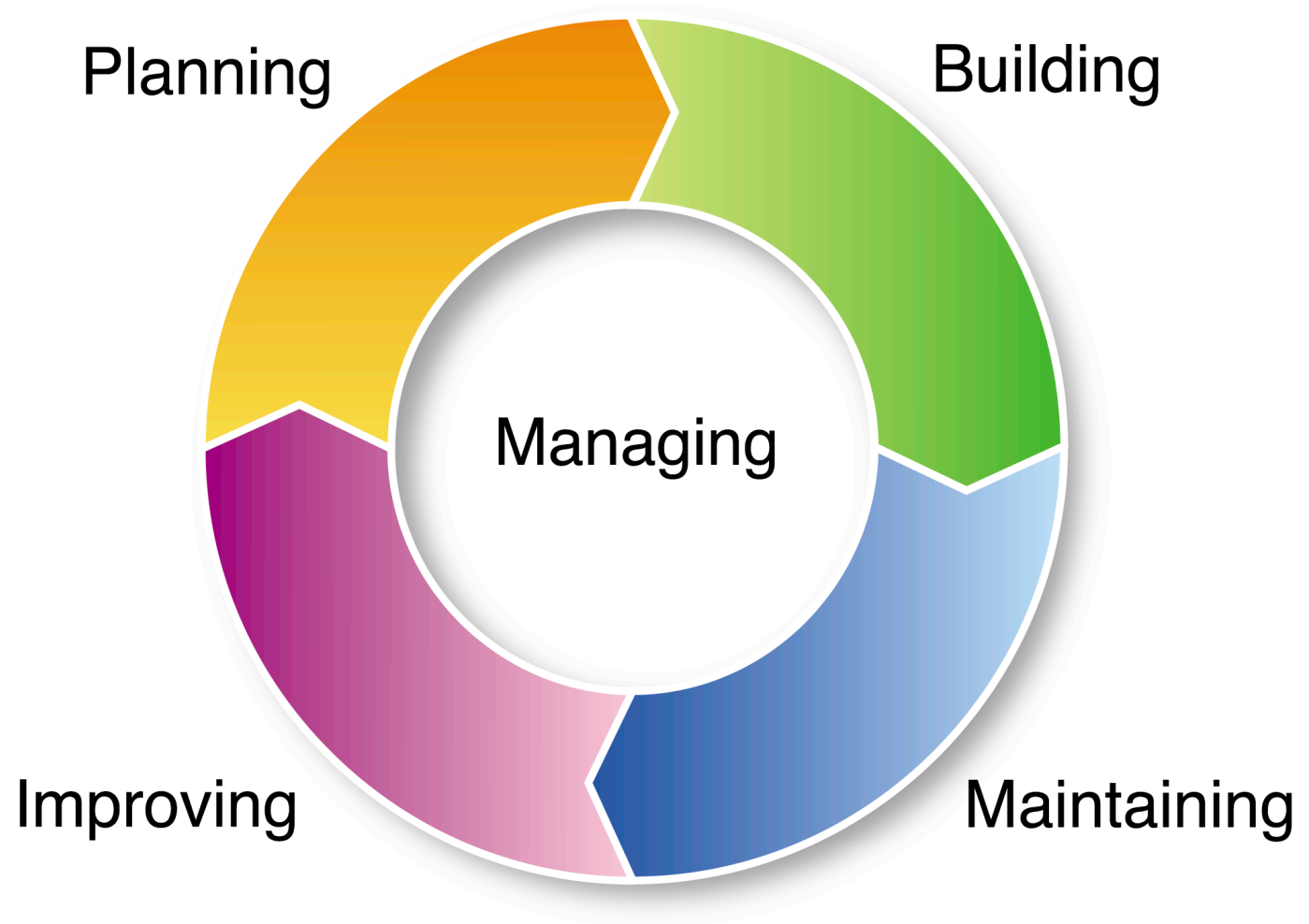
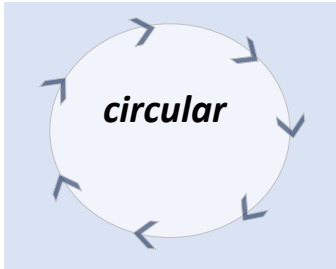




- Flow Chart
- Swim Lane
- Cycle
- SIPOC
- RACI







SIPOC (Supplier-Input-Process-Output-Customer)



Supplier



Input



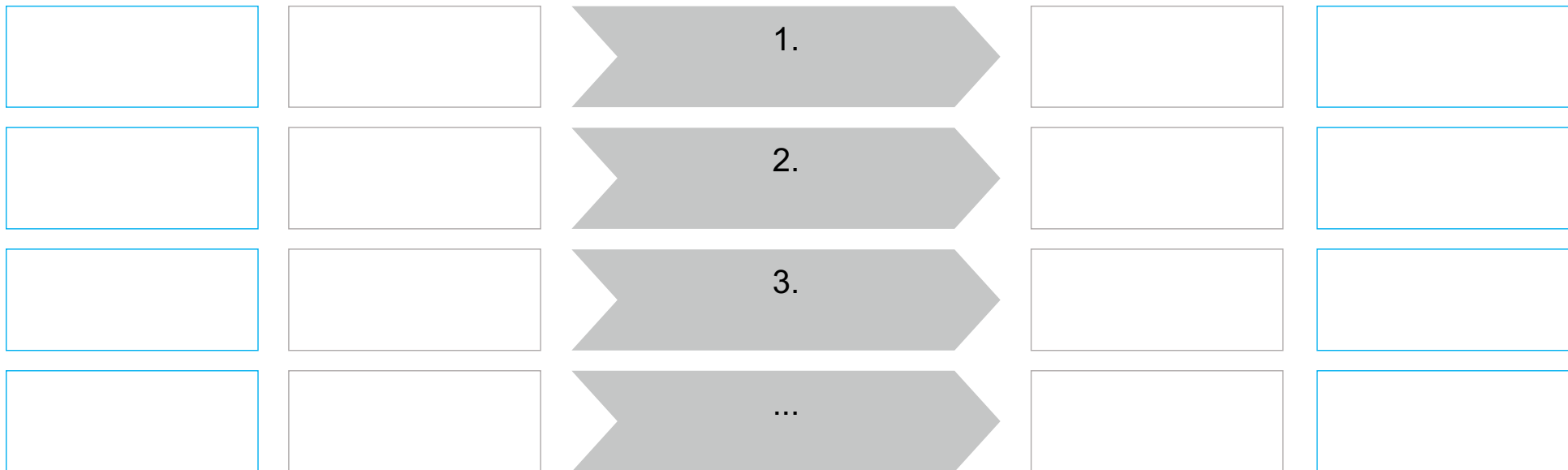
Process step



Output



Customer



RACI (Responsible-Accountable-Consulted-Informed)



RACI Matrix

Process Name:

Process Owner:

Nr.	Process step	Department / Area / Role					Inputs	Outputs	Comments
		A	B	C	D	E			
1									
2									
3									
4									
...									

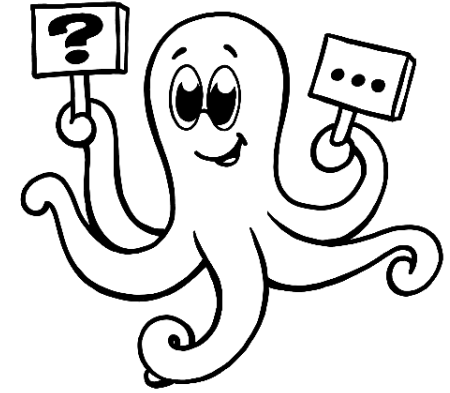
R: Responsible ("doer" who performs the task and ensures that everything has been completed)

A: Accountable (person in charge, no delegation possible to another role)

C: Consulted (person who gives advice before or during a task completion, can influence a decision)




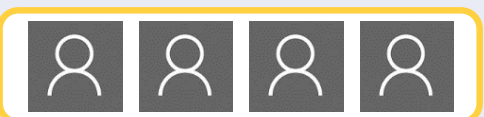

I: Informed (people or roles informed after finalisation of the task)

Which IT Processes do you know?

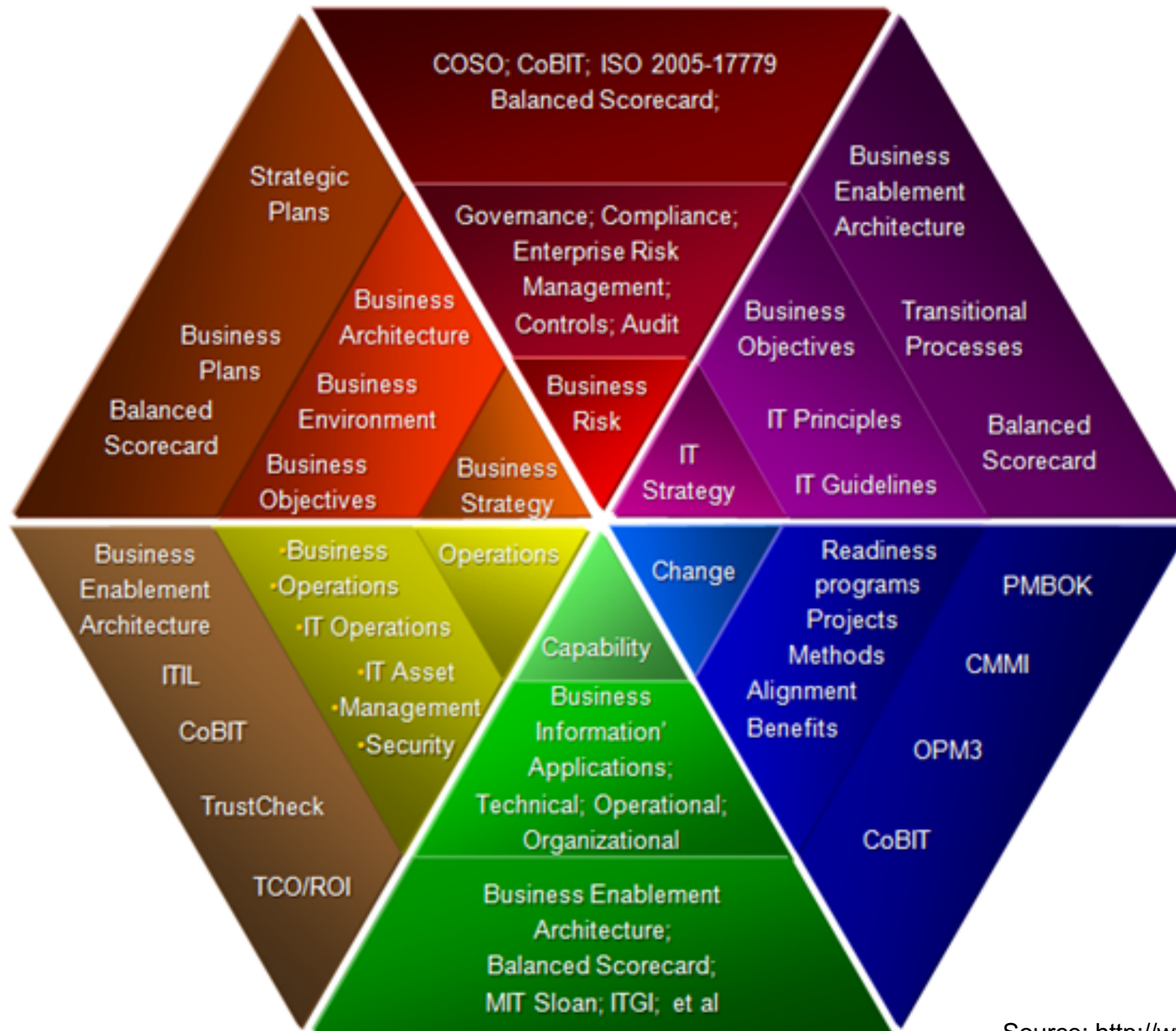


Let's start modelling!



Group	Step 1: IT Process	Step 2: Design technique	<u>Exercise: Modelling</u>
	Choose an IT process	Select a design technique	<u>Exercise:</u> do the modelling of your chosen process with the selected technique
	Choose an IT process	Select a design technique	<u>Exercise:</u> do the modelling of your chosen process with the selected technique
	Choose an IT process	Select a design technique	<u>Exercise:</u> do the modelling of your chosen process with the selected technique
	Choose an IT process	Select a design technique	<u>Exercise:</u> do the modelling of your chosen process with the selected technique
	Choose an IT process	Select a design technique	<u>Exercise:</u> do the modelling of your chosen process with the selected technique

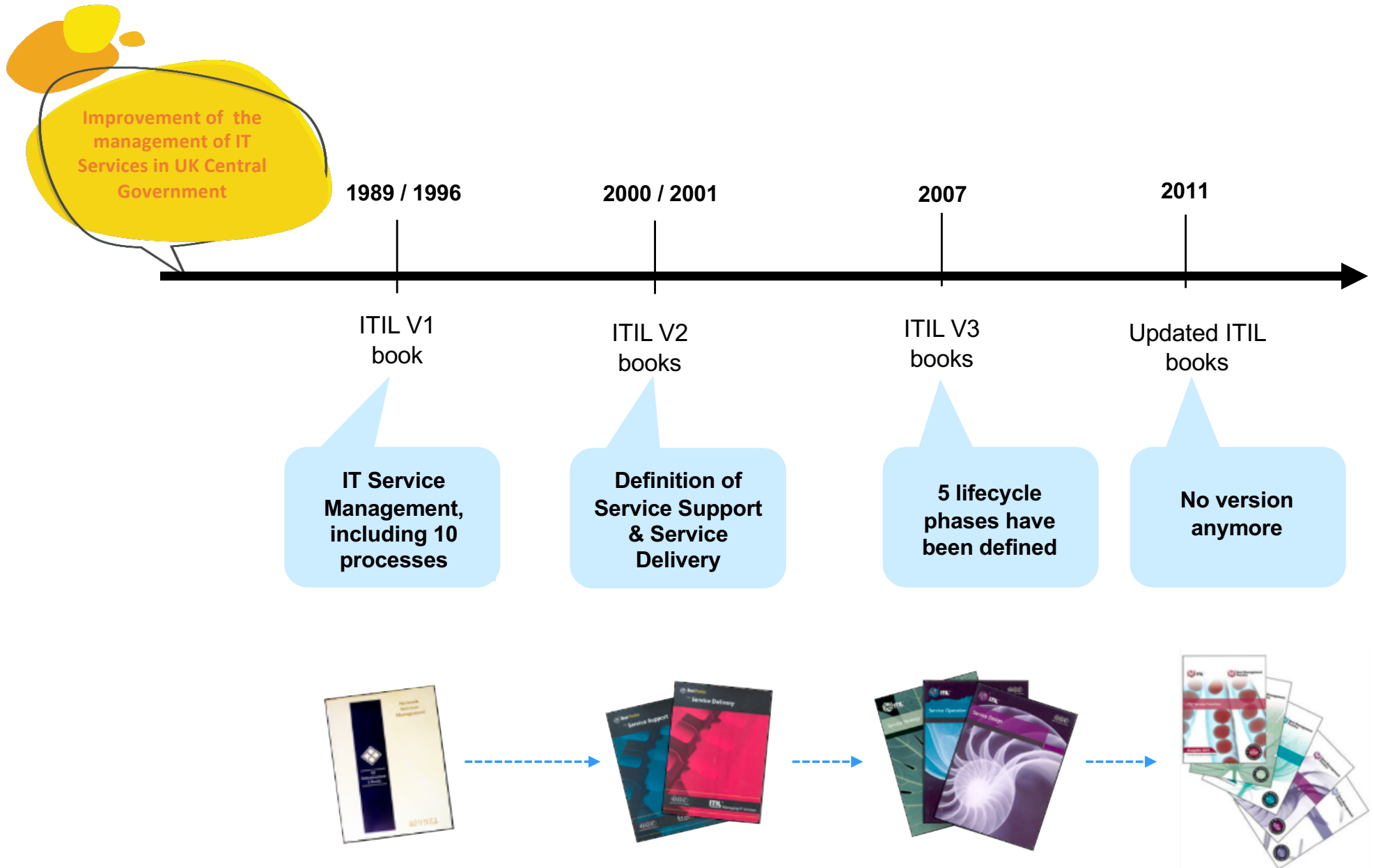
Many standards are available!





- ITIL
- COBIT
- IT4IT

Short history of ITIL (IT Infrastructure Library)





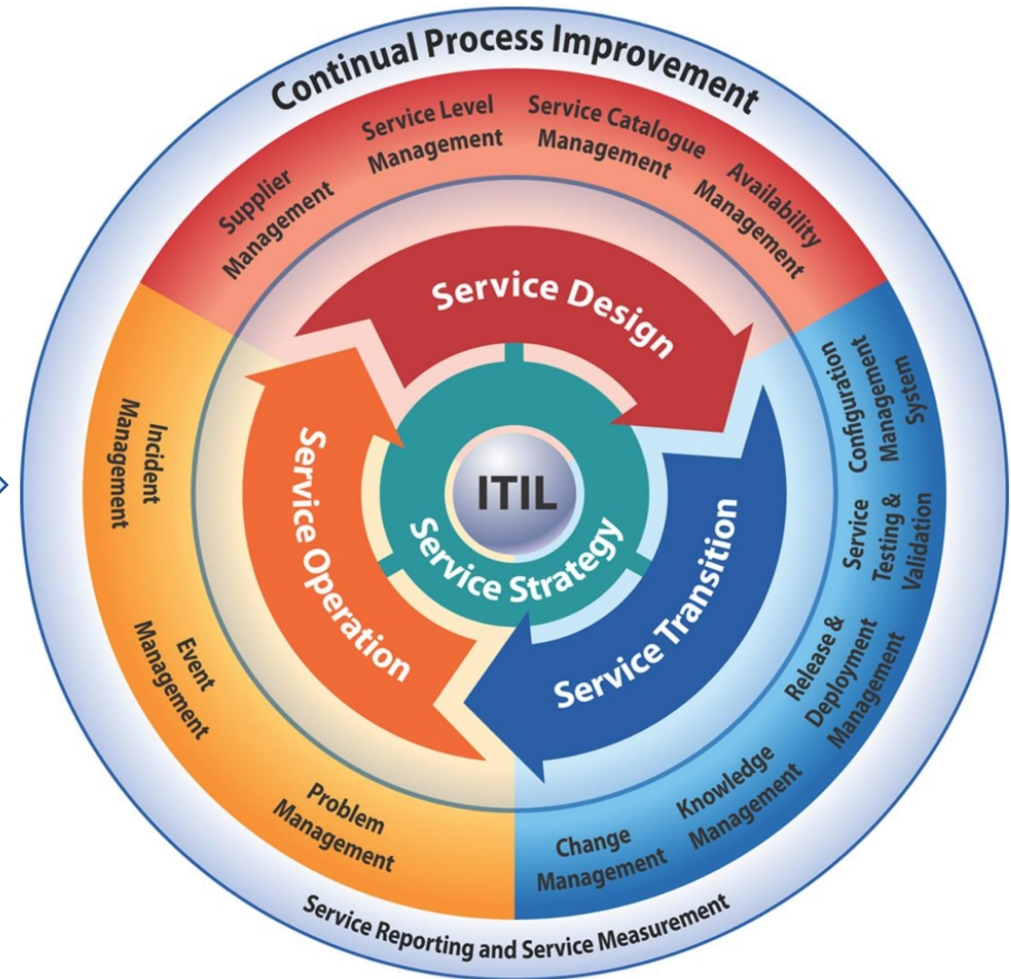
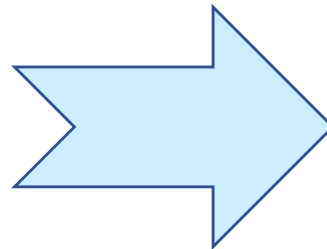
ITIL V1

Service Support

- Configuration Management
- Incident Management
- Problem Management
- Change Management
- Release Management

Service Delivery

- Service Level Management
- Capacity Management
- Availability Management
- Continuity Management
- Financial Management





Advantages

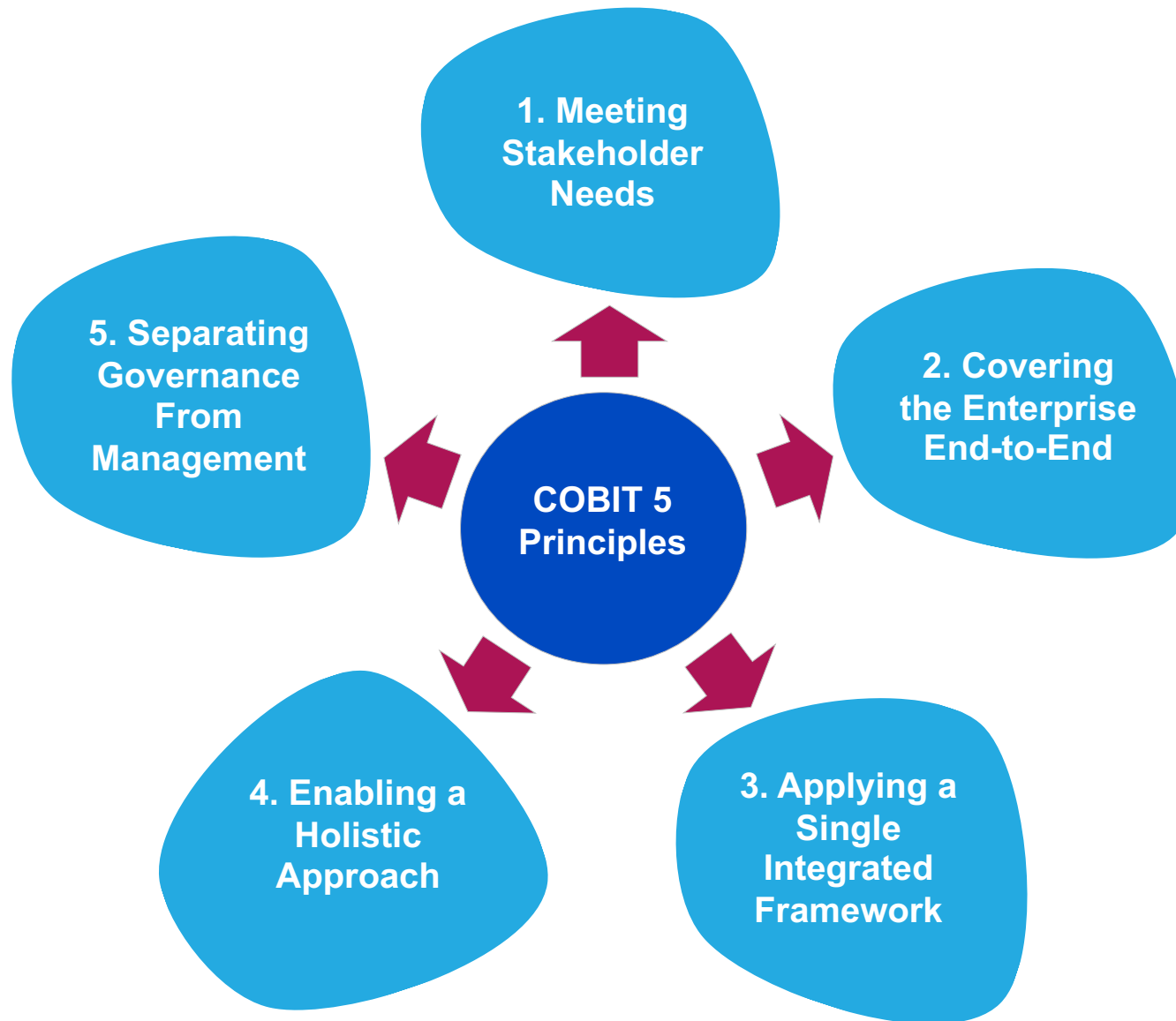
- reduced costs for the organization
- better productivity of the organization
- improved IT services through the use of proven best practice processes
- improved quality control
- improved utilization of skills and experience of the employees
- improved customer satisfaction
- utilization of industry standards
- improved delivery of third party services as the standard for service delivery in services procurements

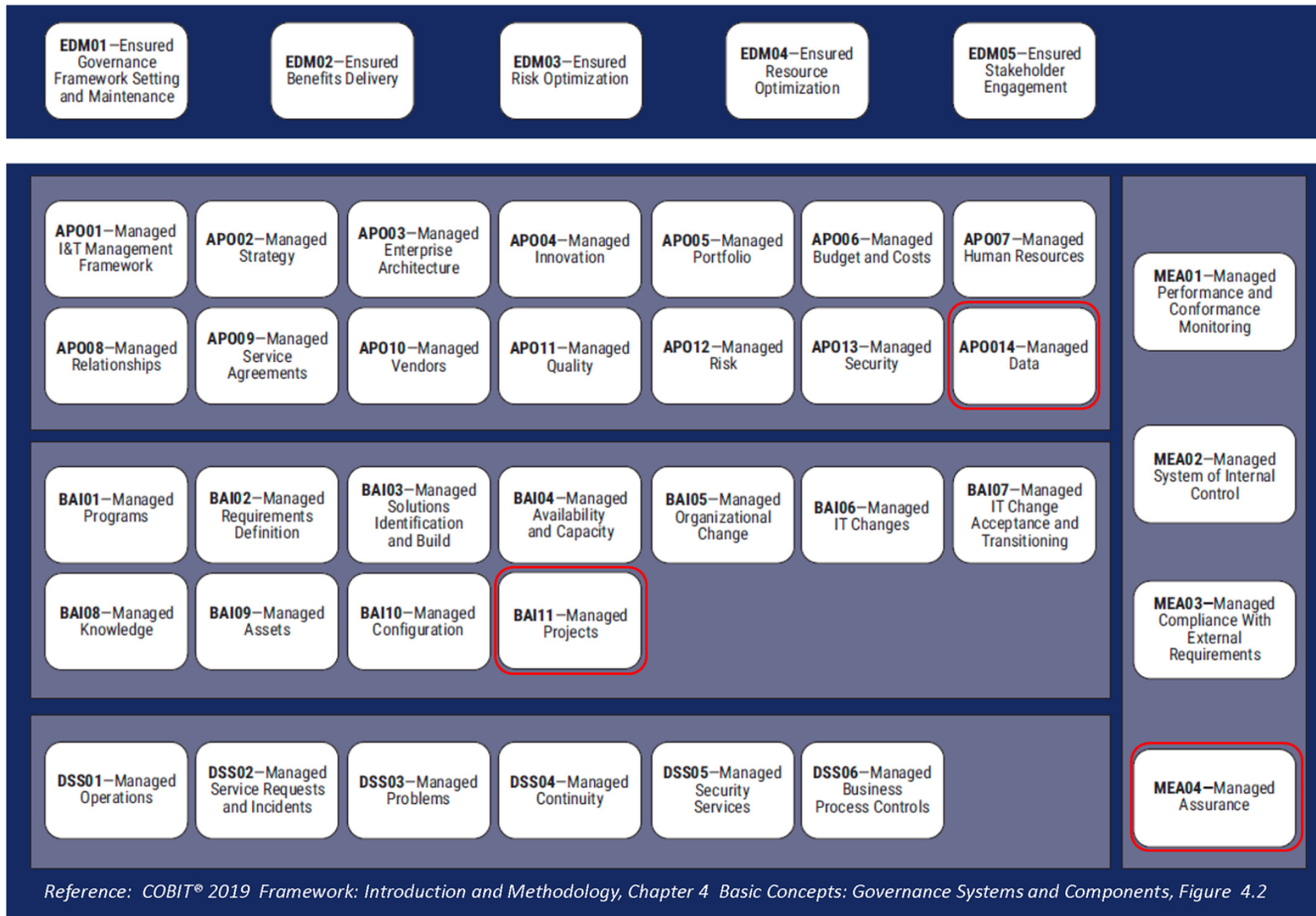
Disadvantages

- extensive use may lead to considerable costs
- not easily understandable (Version 2 is more easily understandable)
- expensive books and not affordable for non-commercial users.
- specific training required



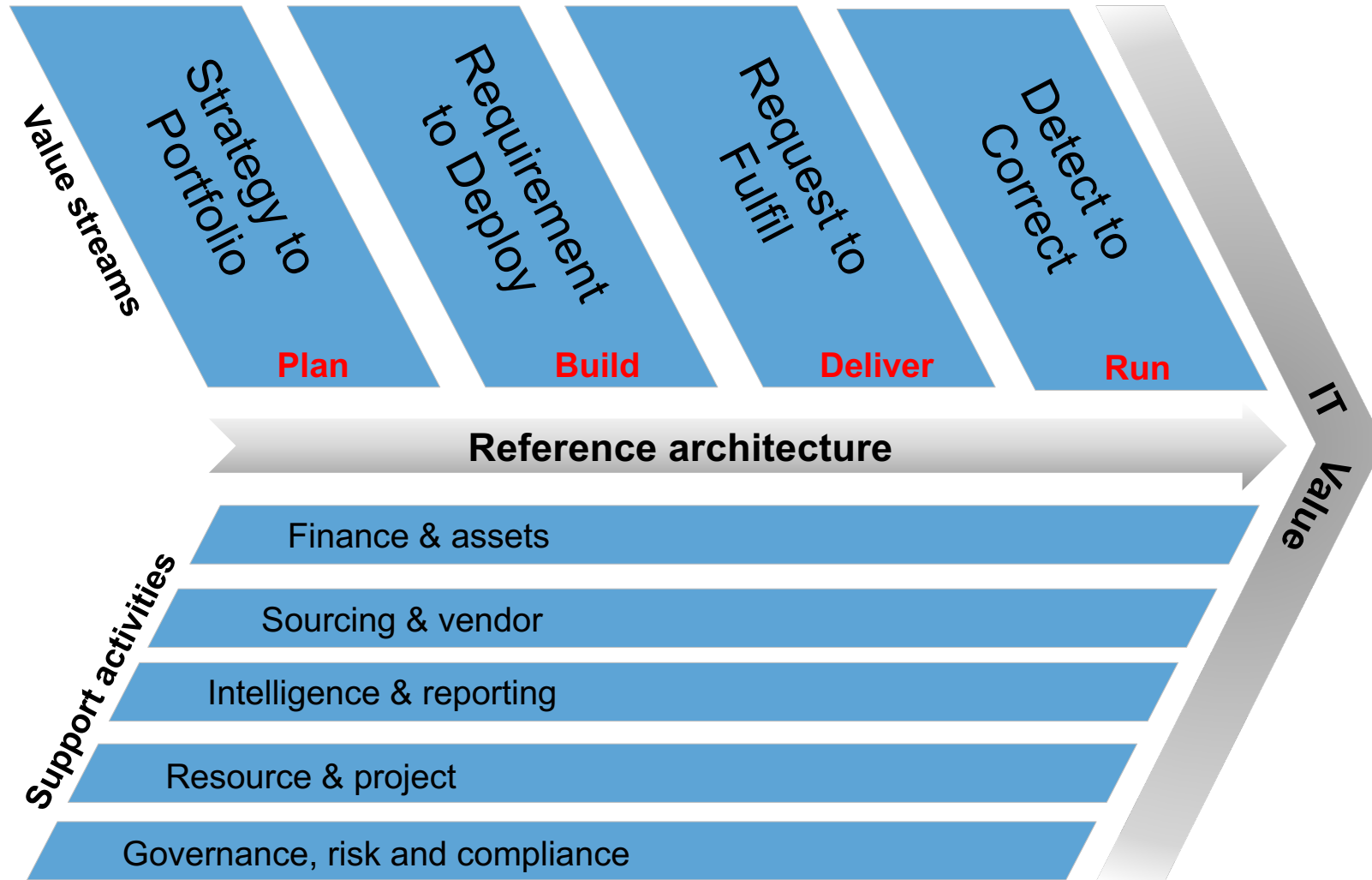
- COBIT = Framework created by ISACA for IT Management and Governance
- Toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- ISACA first released COBIT in 1996
- ISACA published the current version, COBIT 5, in 2012

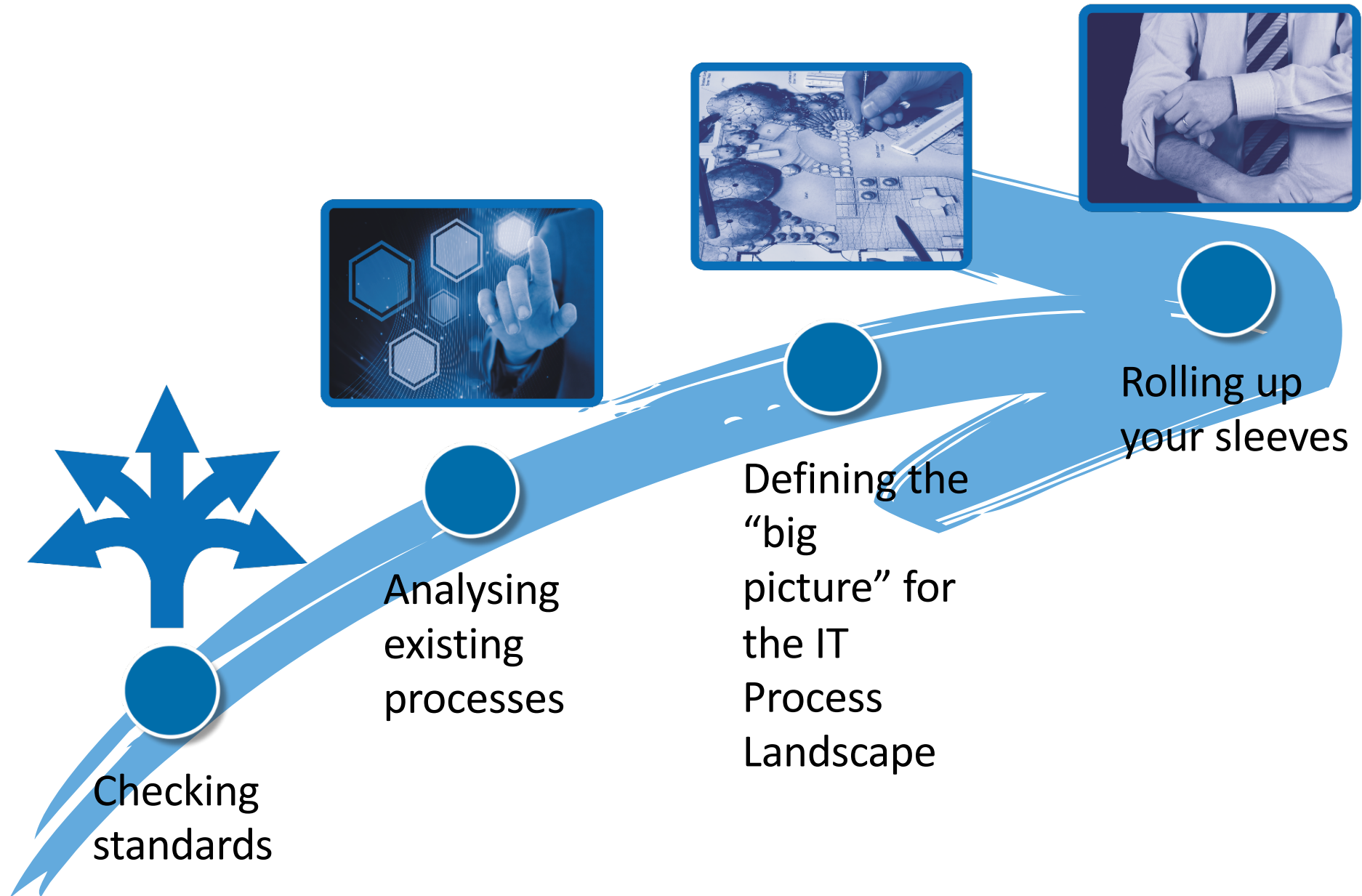






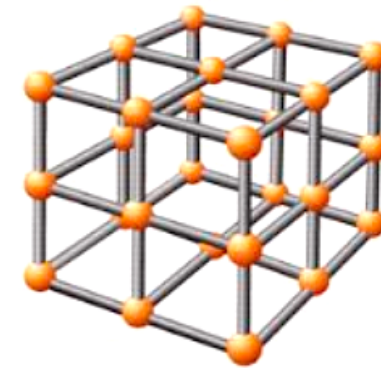
IT Value chain






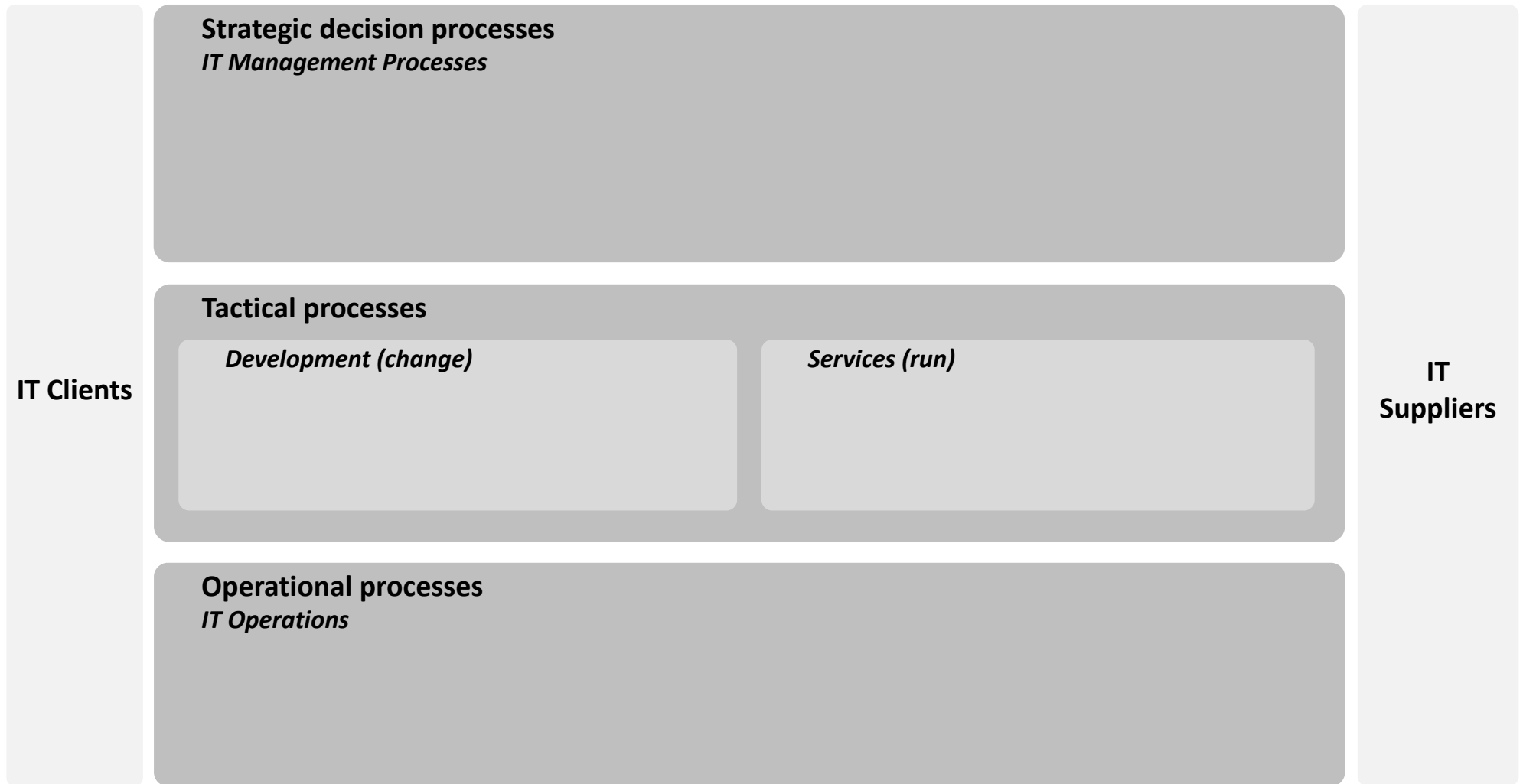




- Customers (as internal customer)
- Time frame
- Suppliers

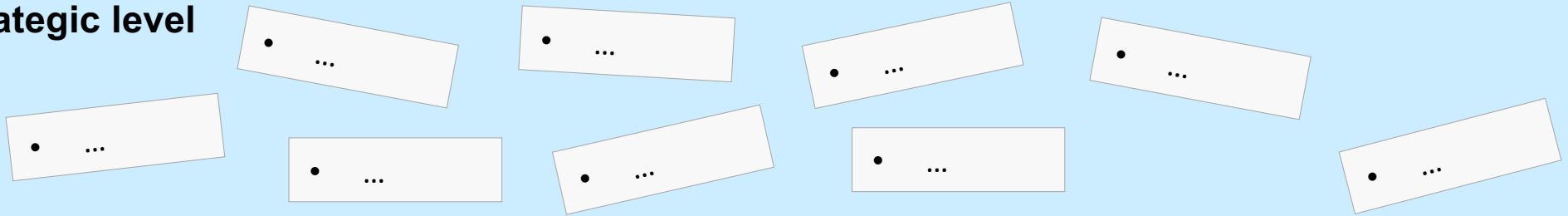


Customers	Time Frame	IT Suppliers
Upper management	strategic 	Partner
Middle management	tactical 	Provider
Employee	operational 	Seller

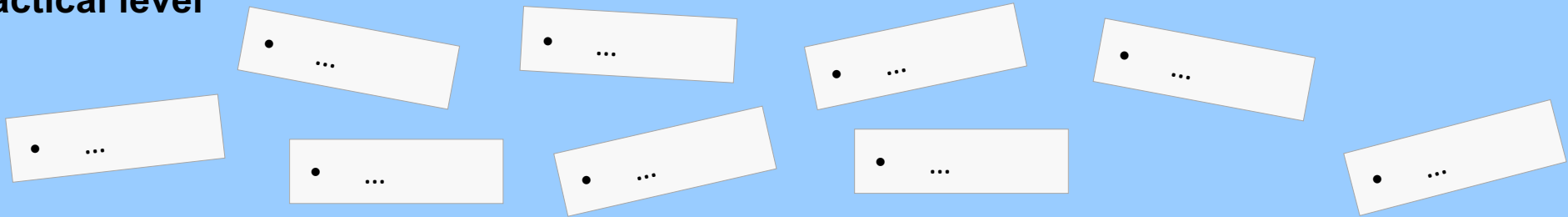




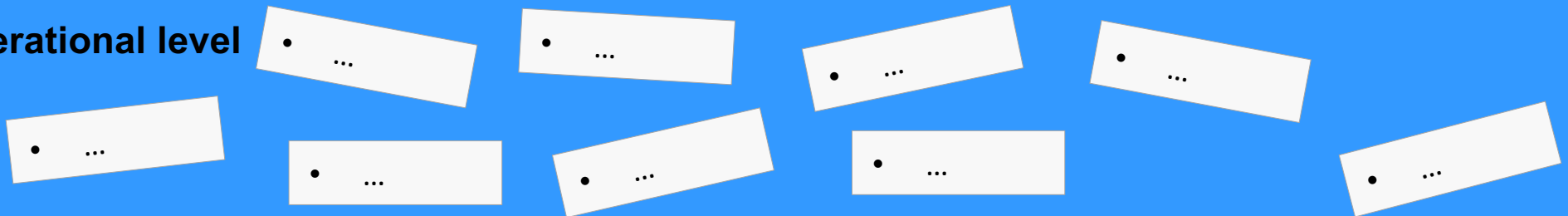
Strategic level



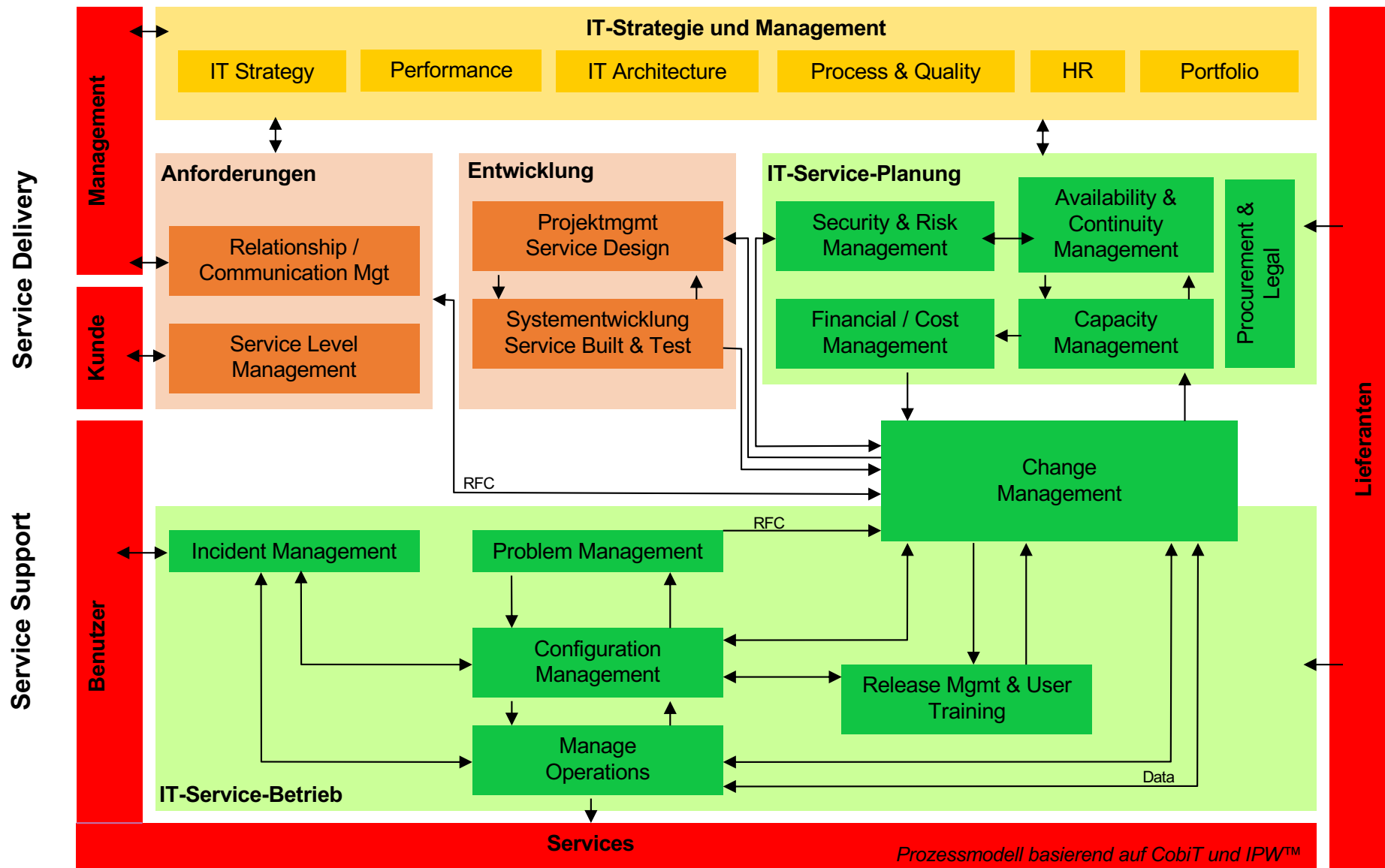
Tactical level



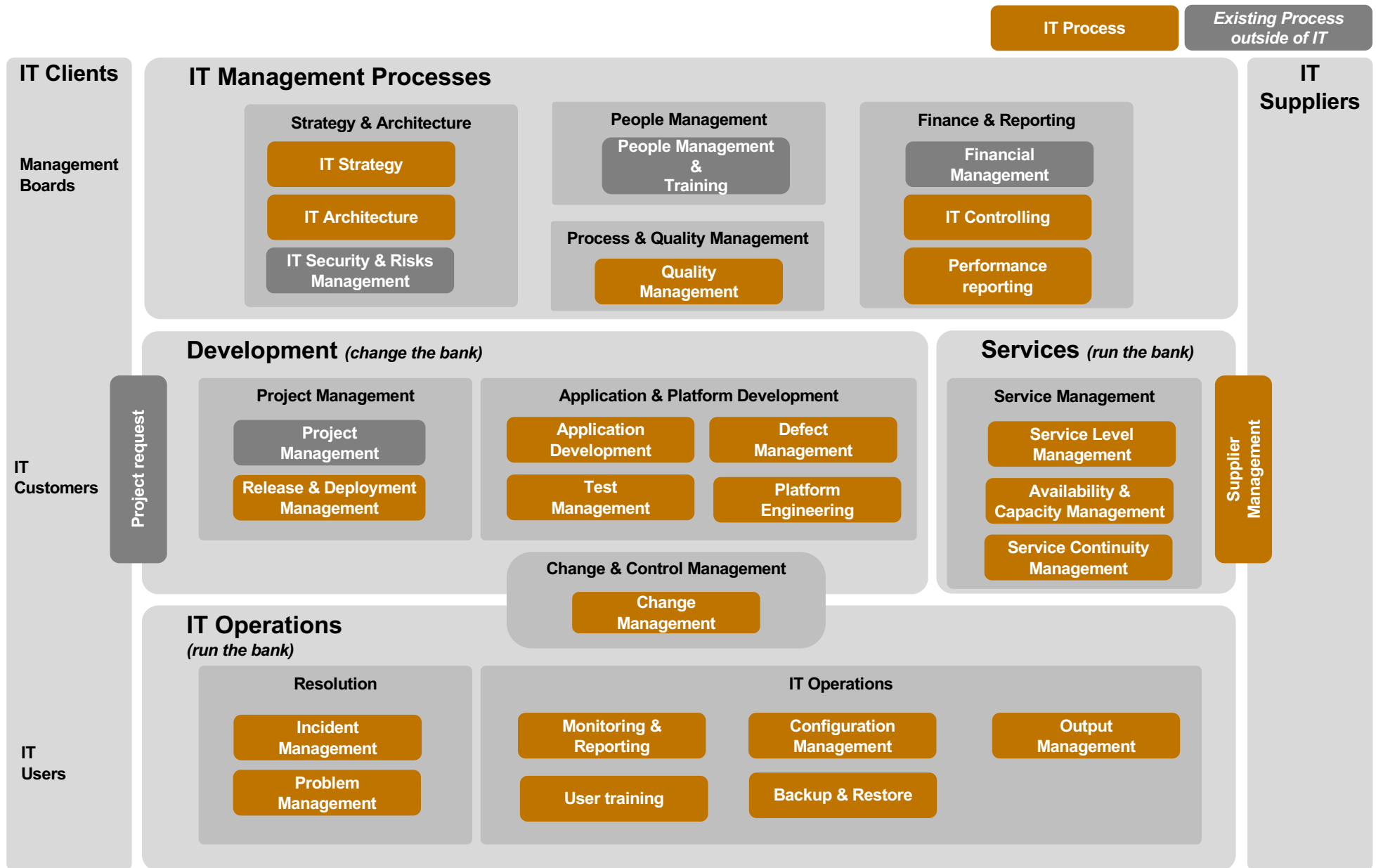
Operational level



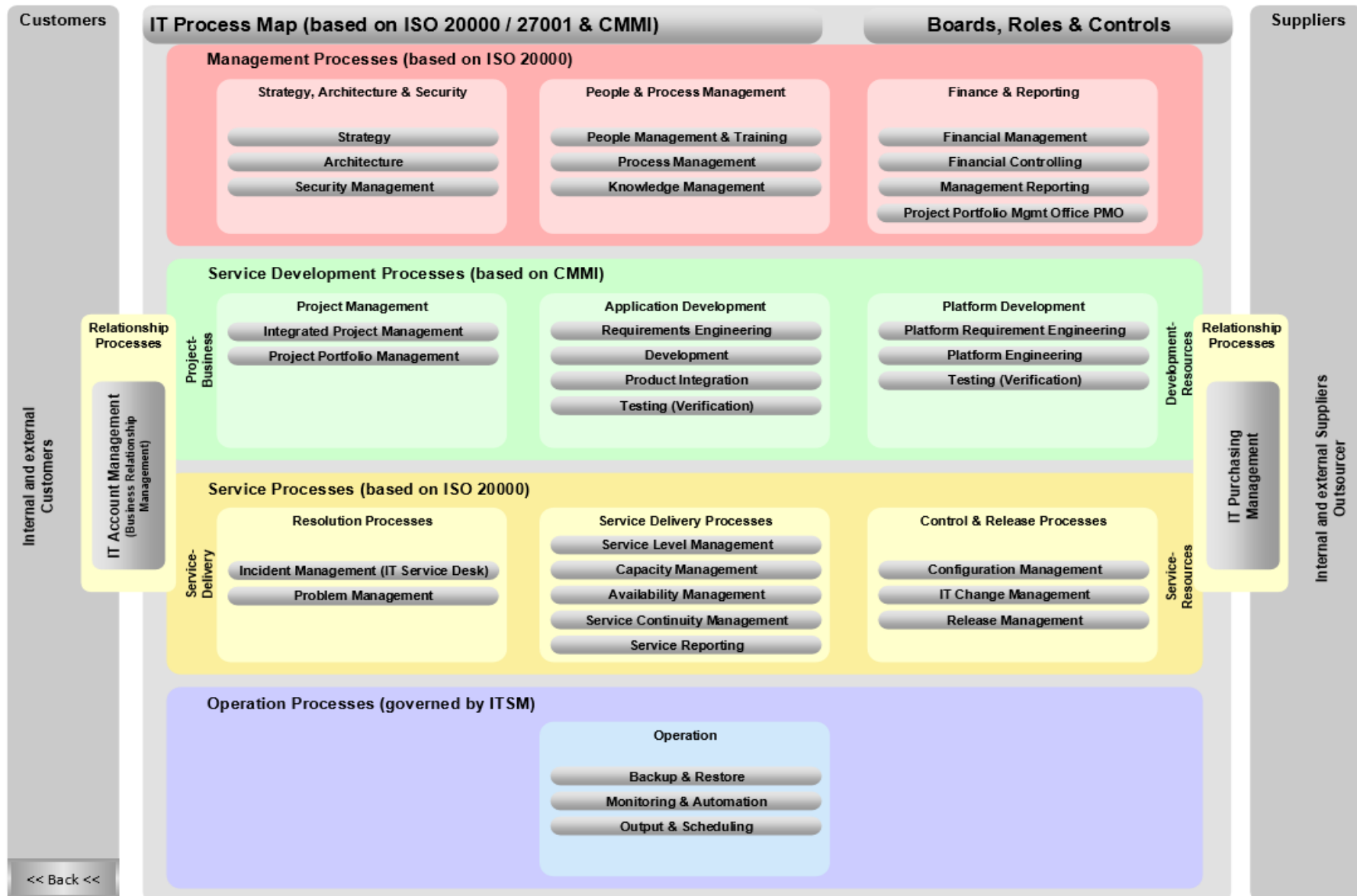
IT Process Landscape: 1st Example

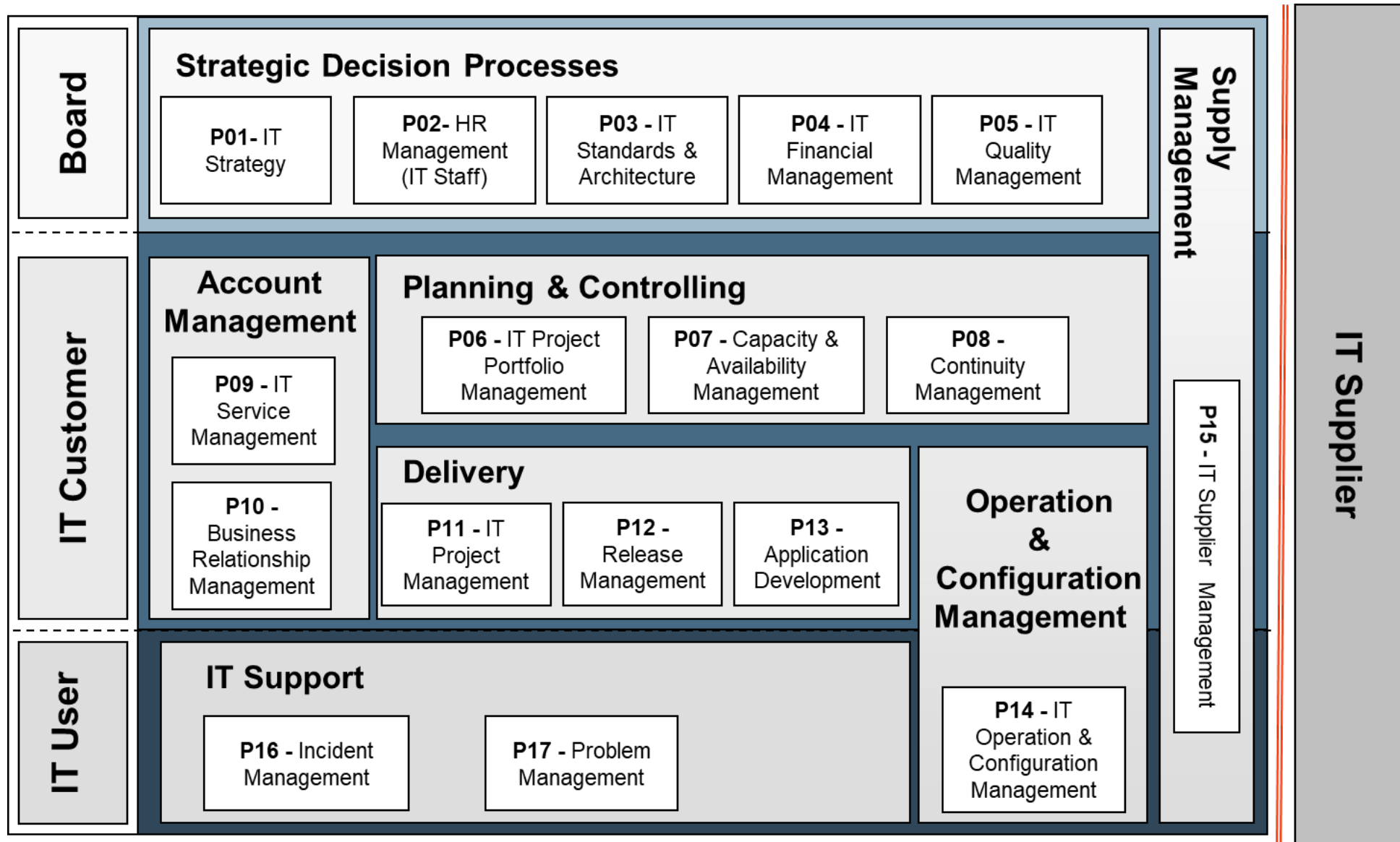


IT Process Landscape: 2nd Example



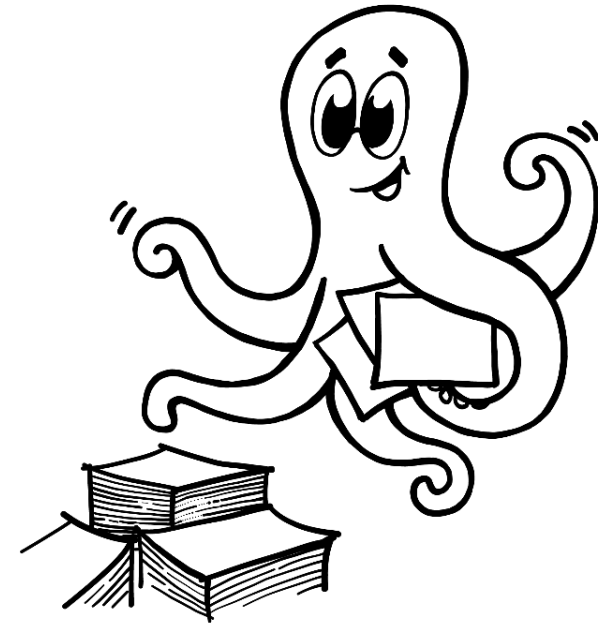
IT Process Landscape: 3rd Example







- Process design (objective, trigger, steps, roles, input, output, process dependency, CSFs)
- 5 Techniques for process modelling
- Acronyms for ITIL and COBIT
- Strategic, tactical and operational levels of a process landscape





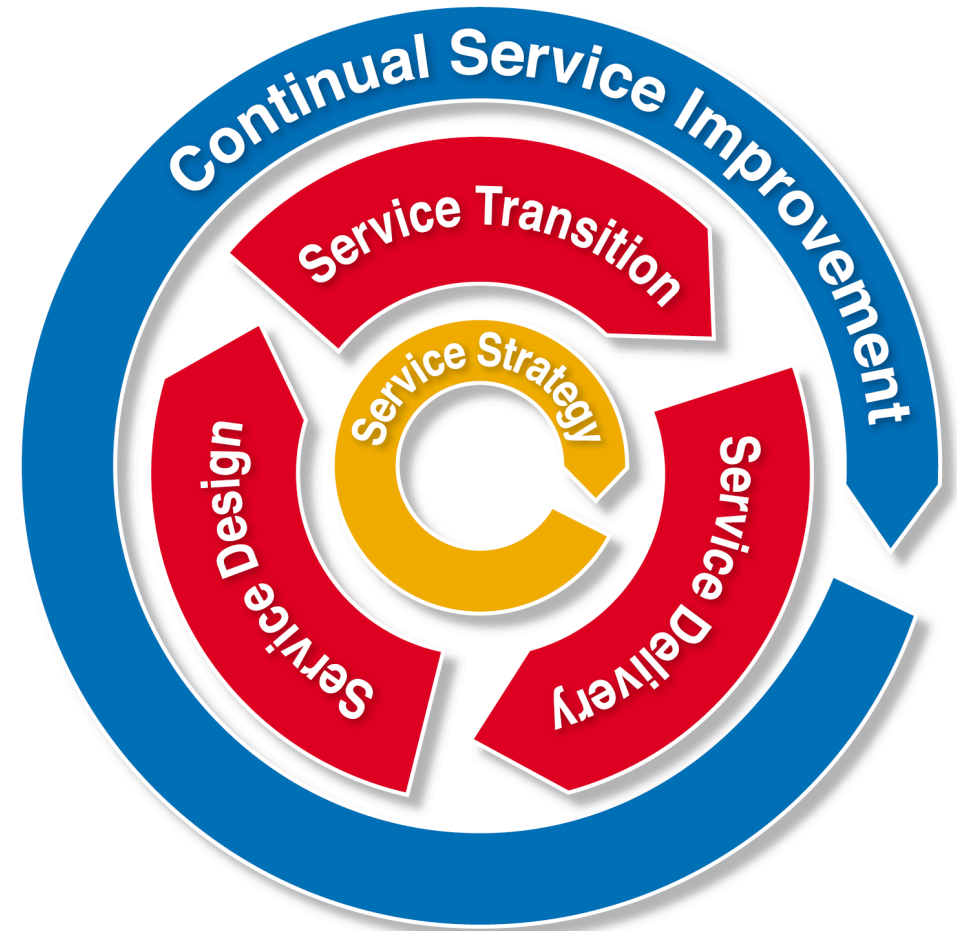
- Pilorget L (2015) Implementing IT Processes. Springer, Wiesbaden
- Pilorget L, Schell T (2018) IT Management. Springer, Wiesbaden





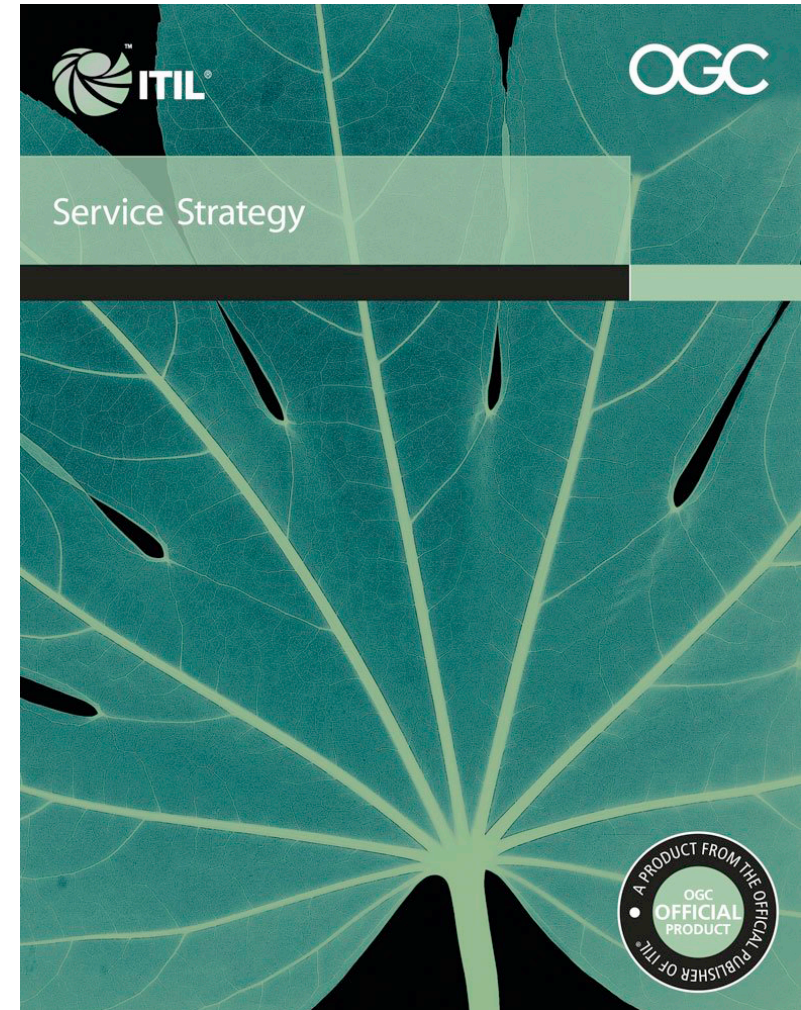


- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement





- What IT Services should we provide?
- Who should we provide these services too?
- How do we genuinely differentiate from competitors?
- How do we create lasting business value for our customers?
- How can we make a case for ROI and other investments?
- How should we best define and measure service quality?
- How do we choose between different paths for improving service quality?
- How do we efficiently (re)allocate resources across a portfolio of services?
- How do we resolve conflicting demands for shared resources?



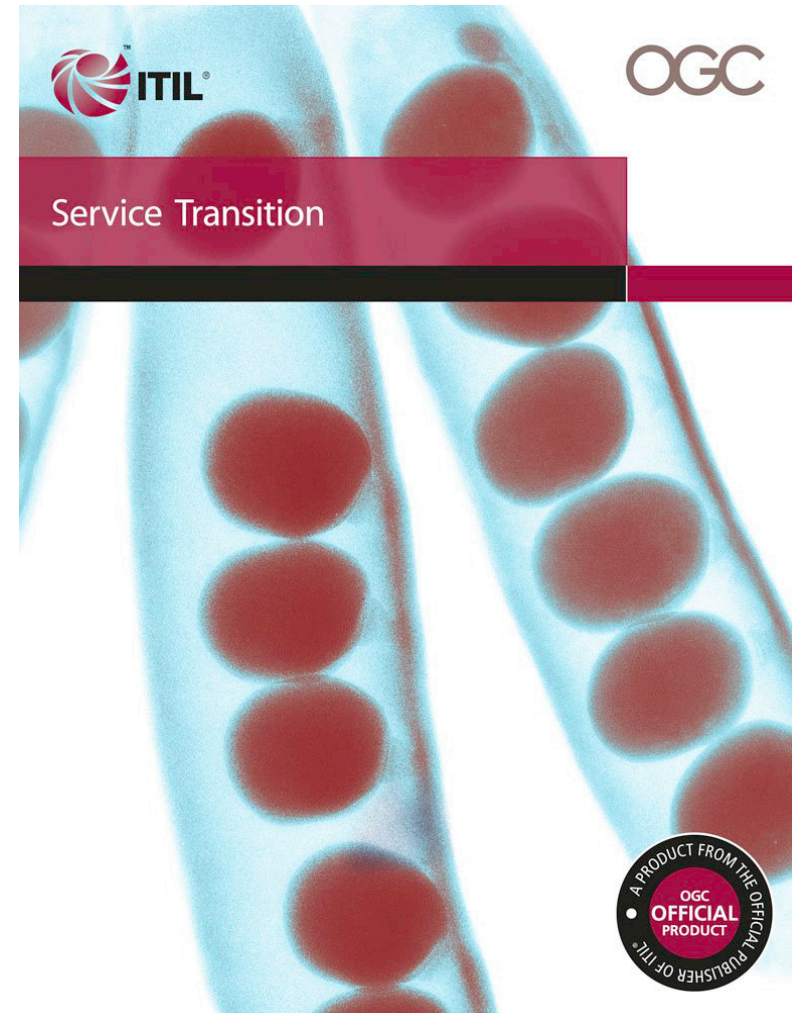


- Design coordination
- Service catalogue management
- Service level management
- Availability management
- Capacity management
- IT service continuity management
- Information security management
- Supplier management





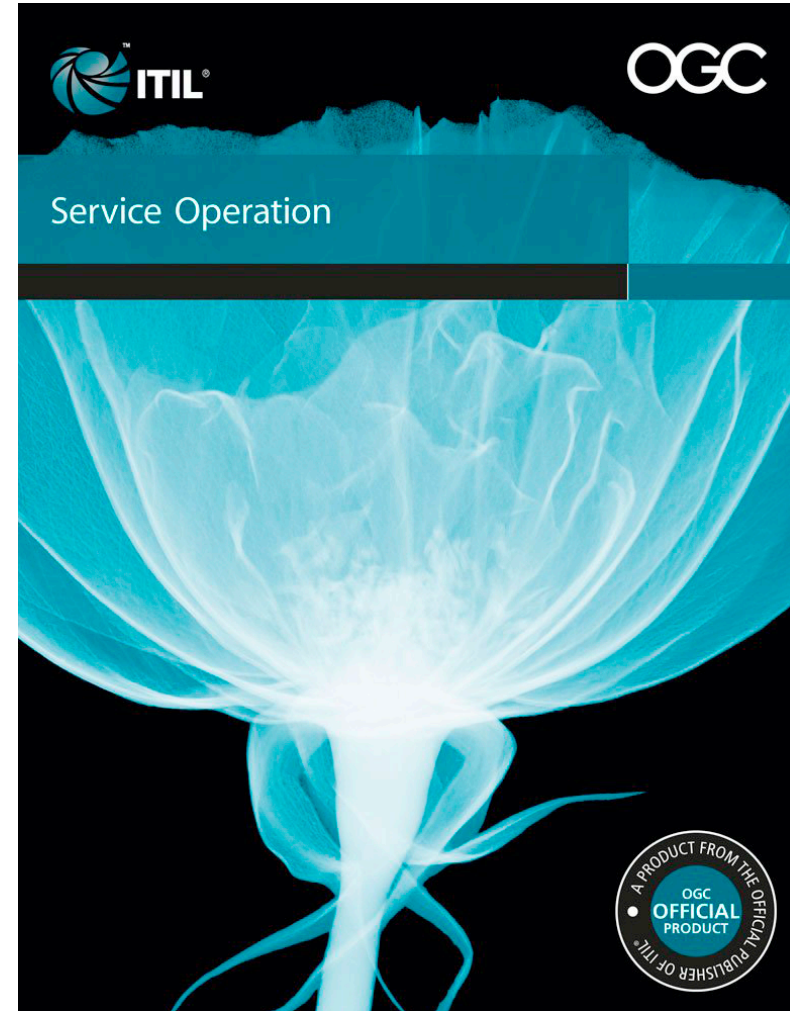
- Knowledge management
- Transition planning and support
- Change management
- Availability management
- Service asset and configuration management (SACM)
- Release and deployment management
- Evaluation



4 main Functions of Service Operation



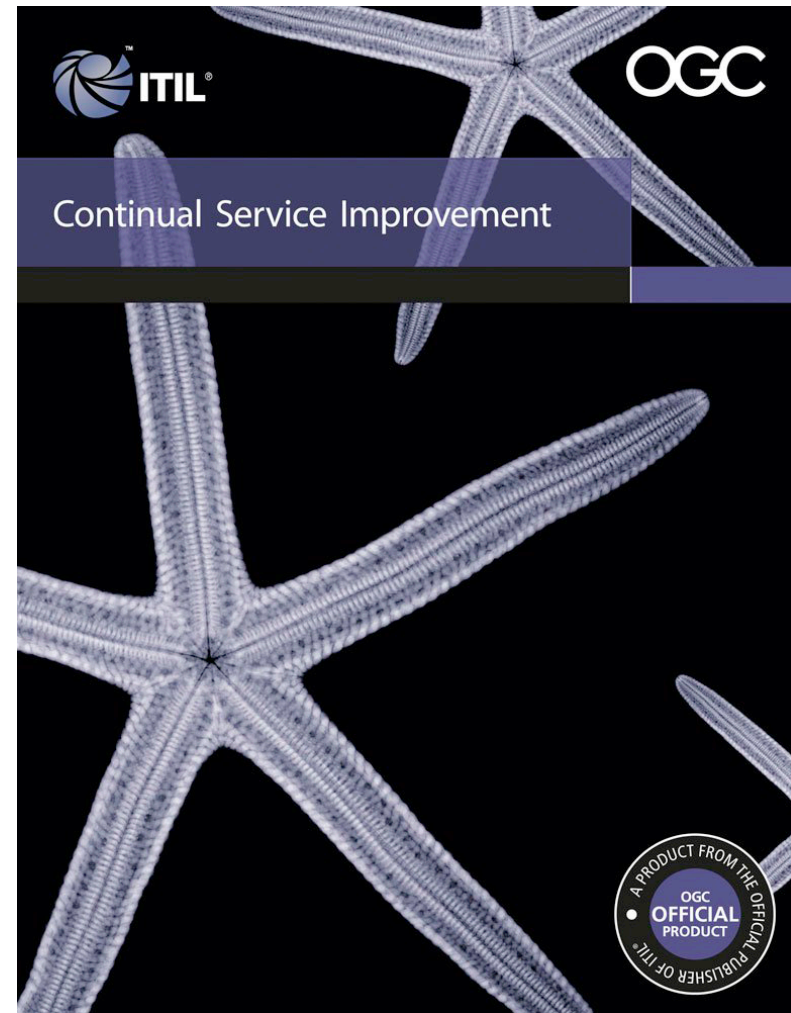
- **Technical management**
 - Manage the IT infrastructure
 - Provide skilled staff and support operations staff members
- **Application management**
 - Manage the IT applications
 - Ensure knowledge and provide training to technical staff
- **Operations management**
 - Conduct day-to-day activities to ensure that SLAs are met
 - Ensure availability and stability of IT systems
 - Schedule and monitor batch-jobs
- **Service desk**
 - SPOC (Single Point of Contact) for users of IT services
 - Prioritize issues and escalates if necessary
 - Solves as far as possible incidents

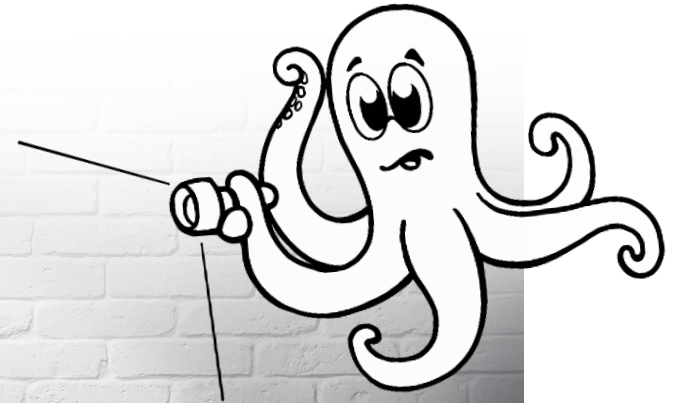


Continual Service Improvement (CSI) in seven steps



- 1) Identify the strategy for improvement
- 2) Define what you will measure
- 3) Gather the data
- 4) Process the data
- 5) Analyse the information and data
- 6) Present and use the information
- 7) Implement improvement





COBIT 4

COBIT 4, Plan and Organise (PO)



PO1	Define a strategic IT plan	PO5	Manage the IT investment	PO10	Manage projects
PO1.1	IT value management	PO5.1	Financial management framework	PO10.1	Programme management framework
PO1.2	Business-IT alignment	PO5.2	Priorisation within IT budget	PO10.2	Project management framework
PO1.3	Assessment of current performance	PO5.3	IT budgeting process	PO10.3	Project management approach
PO1.4	IT strategic plan	PO5.4	Cost management	PO10.4	Stakeholder commitment
PO1.5	IT tactical plans	PO5.5	Benefit management	PO10.5	Project scope statement
PO1.6	IT portfolio management	PO6	Communicate management aims and direction	PO10.6	Project phase initiation
PO2	Define the information architecture	P6.1	IT policy and control environment	PO10.7	Integrated project plan
PO2.1	Information architecture model	P6.2	Enterprise IT risk and internal control framework	PO10.8	Project resources
PO2.2	Enterprise data dictionary and data syntax rules	P6.3	IT policies management	PO10.9	Project risk management
PO2.3	Data classification scheme	P6.4	Policy rollout	PO10.10	Project quality plan
PO2.4	Integrity Management	P6.5	Communication of IT objectives and direction	PO10.11	Project change control
PO3	Determine technological direction	PO7	Manage IT human resources	PO10.12	Project planning of assurance methods
PO3.1	Technological direction planning	PO7.1	Personnel recruitment and retention	PO10.13	Project performance measurement, reporting and monitoring
PO3.2	Technical infrastructure plan - scope and coverage	PO7.2	Personnel competencies	PO10.14	Project closure
PO3.3	Monitoring of future trends and regulations	PO7.3	Staffing of roles		
PO3.4	Technology standards	PO7.4	Personnel training		
PO3.5	IT architecture board	PO7.5	Dependence upon individuals		
PO4	Define the IT processes, organization and relationships	PO7.6	Personnel clearance procedures		
PO4.1	IT process framework	PO7.7	Employee job performance evaluation		
PO4.2	IT strategy committee	PO7.8	Job change and termination		
PO4.3	IT steering committee	PO8	Manage quality		
PO4.4	Organisational placement of the IT function	PO8.1	Quality management system		
PO4.5	IT organisational structure	PO8.2	IT standards and quality practices		
PO4.6	Roles and responsibilities	PO8.3	Development and acquisition standards		
PO4.7	Responsibility for IT quality assurance	PO8.4	Customer focus		
PO4.8	Responsibility for risk, security and compliance	PO8.5	Continuous improvement		
PO4.9	Data and system ownership	PO8.6	Quality measurement, monitoring and review		
PO4.10	Supervision	PO9	Assess and manage IT risks		
PO4.11	Segregation of duties	PO9.1	IT and business risk management alignment		
PO4.12	IT staffing	PO9.2	Establishment of risk context		
PO4.13	Key IT personnel	PO9.3	Event identification		
PO4.14	Contracted staff policies and procedures	PO9.4	Risk assessment		
PO4.15	Relationships	PO9.5	Risk response		
		PO9.6	Maintenance and monitoring of a risk action plan		



AI1	Identify automated solutions
AI1.1	Definition and maintenance of business functional and technical requirements
AI1.2	Risk analysis report
AI1.3	Feasibility study and formulation of alternative courses of action
AI1.4	Requirements and feasibility decision and approval
AI2	Acquire and maintain application software
AI2.1	High-level design
AI2.2	Detailed design
AI2.3	Application control and auditability
AI2.4	Application security and availability
AI2.5	Configuration and implementation of acquired application software
AI2.6	Major upgrades to existing systems
AI2.7	Development of application software
AI2.8	Software quality assurance
AI2.9	Application requirements management
AI2.10	Application software maintenance
AI3	Acquire and maintain technology infrastructure
AI3.1	Technological infrastructure acquisition plan
AI3.2	Infrastructure resource protection and availability
AI3.3	Infrastructure maintenance
AI3.4	Feasibility test environment
AI4	Enable operation and use
AI4.1	Planning for operational solutions
AI4.2	Knowledge transfer to business management
AI4.3	Knowledge transfer to end users
AI4.4	Knowledge transfer to operations and support staff

AI5	Procure IT resources
AI5.1	Procurement control
AI5.2	Supplier contract management
AI5.3	Supplier selection
AI5.4	Software acquisition
AI5.5	Acquisition of development resources
AI5.6	Acquisition of infrastructure, facilities and related services
AI6	Manage changes
AI6.1	Change standards and procedures
AI6.2	Impact assessment, prioritisation and authorisation
AI6.3	Emergency changes
AI6.4	Change status tracking and reporting
AI6.5	Change closure and documentation
AI7	Install and accredit solutions and changes
AI7.1	Training
AI7.2	Test plan
AI7.3	Implementation plan
AI7.4	Test environment
AI7.5	System and data conversion
AI7.6	Testing of changes
AI7.7	Final acceptance test
AI7.8	Promotion to production
AI7.9	Software release
AI7.10	System distribution
AI7.11	Recording and tracking of changes
AI7.12	Post-implementation review

COBIT 4, Deliver and Support (DS)



DS1	Define and manage service levels	DS6	Identify and allocate costs
DS1.1	Service level agreement framework	DS6.1	Definition of services
DS1.2	Definition of services	DS6.2	IT accounting
DS1.3	Service level agreements	DS6.3	Cost modelling and charging
DS1.4	Operating level agreements	DS6.4	Cost model maintenance
DS1.5	Monitoring and reporting of service level achievements	DS7	Educate and train users
DS1.6	Review of service level agreements and contracts	DS7.1	Identification of education and training needs
DS2	Manage third-party services	DS7.2	Delivery of training and education
DS2.1	Identification of all supplier relationships	DS7.3	Evaluation of training received
DS2.2	Supplier relationship management	DS8	Manage service desk and incidents
DS2.3	Supplier risk management	DS8.1	Service desk
DS2.4	Supplier performance monitoring	DS8.2	Registration of customer queries
DS3	Manage performance and capacity	DS8.3	Incident escalation
DS3.1	Performance and capacity planning	DS8.4	Incident closure
DS3.2	Current capacity and performance	DS8.5	Trend analysis
DS3.3	Future capacity and performance	DS9	Manage the configuration
DS3.4	IT resources availability	DS9.1	Configuration Repository and Baseline
DS3.5	Monitoring and reporting	DS9.2	Identification and maintenance of configuration items
DS4	Ensure continuous service	DS9.3	Configuration Integrity Review
DS4.1	IT continuity framework	DS10	Manage problems
DS4.2	IT continuity plans	DS10.1	Identification and classification of problems
DS4.3	Critical IT resources	DS10.2	Problem tracking and resolution
DS4.4	Maintenance of the IT continuity plan	DS10.3	Problem closure
DS4.5	Testing of the IT continuity plan	DS10.4	Integration of change, configuration and problem management
DS4.6	IT continuity plan training	DS11	Manage data
DS4.7	Distribution of the IT continuity plan	DS11.1	Business requirements for data management
DS4.8	IT-Services recovery and resumption	DS11.2	Storage and retention arrangements
DS4.9	Offsite backup storage	DS11.3	Media library management system
DS4.10	Post-resumption review	DS11.4	Disposal
DS5	Ensure systems security	DS11.5	Backup and Restoration
DS5.1	Management of IT security	DS11.6	Security requirements for data management
DS5.2	IT security plan	DS12	Manage the physical environment
DS5.3	Identity management	DS12.1	Site selection and layout
DS5.4	User account management	DS12.2	Physical security measures
DS5.5	Security testing, surveillance and monitoring	DS12.3	Physical access
DS5.6	Security incident definition	DS12.4	Protection against environmental factors
DS5.7	Protection of security technology	DS12.5	Physical facility management
DS5.8	Cryptographic key management	DS13	Manage operations
DS5.9	Malicious software prevention, detection and correction	DS13.1	Operations procedures and instructions
DS5.10	Network security	DS13.2	Job scheduling
DS5.11	Exchange of sensitive data	DS13.3	IT infrastructure monitoring
		DS13.4	Sensitive documents and output devices
		DS13.5	Preventive maintenance for hardware



ME1	Monitor and evaluate IT performance
ME1.1	Monitoring approach
ME1.2	Definition and collection of monitoring data
ME1.3	Monitoring method
ME1.4	Performance assessment
ME1.5	Board and executive reporting
ME1.6	Remedial actions
ME2	Monitor and evaluate internal control
ME2.1	Monitoring of internal control framework
ME2.2	Supervisory review
ME2.3	Control exceptions
ME2.4	Control self-assessment
ME2.5	Assurance of internal control
ME2.6	Internal control at third parties
ME2.7	Remedial Actions
ME3	Ensure regulatory compliance
ME3.1	Identification of laws and regulations having potential impact on IT
ME3.2	Optimisation of response to regulatory requirements
ME3.3	Evaluation of compliance with regulatory requirements
ME3.4	Positive assurance of compliance
ME3.5	Integrated Reporting
ME4	Provide IT-governance
ME4.1	Establishment of an IT governance framework
ME4.2	Strategic alignment
ME4.3	Value delivery
ME4.4	Ressource management
ME4.5	Risk management
ME4.6	Performance measurement
ME4.7	Independent assurance



KNOWLEDGE

www.know-ledge.ch