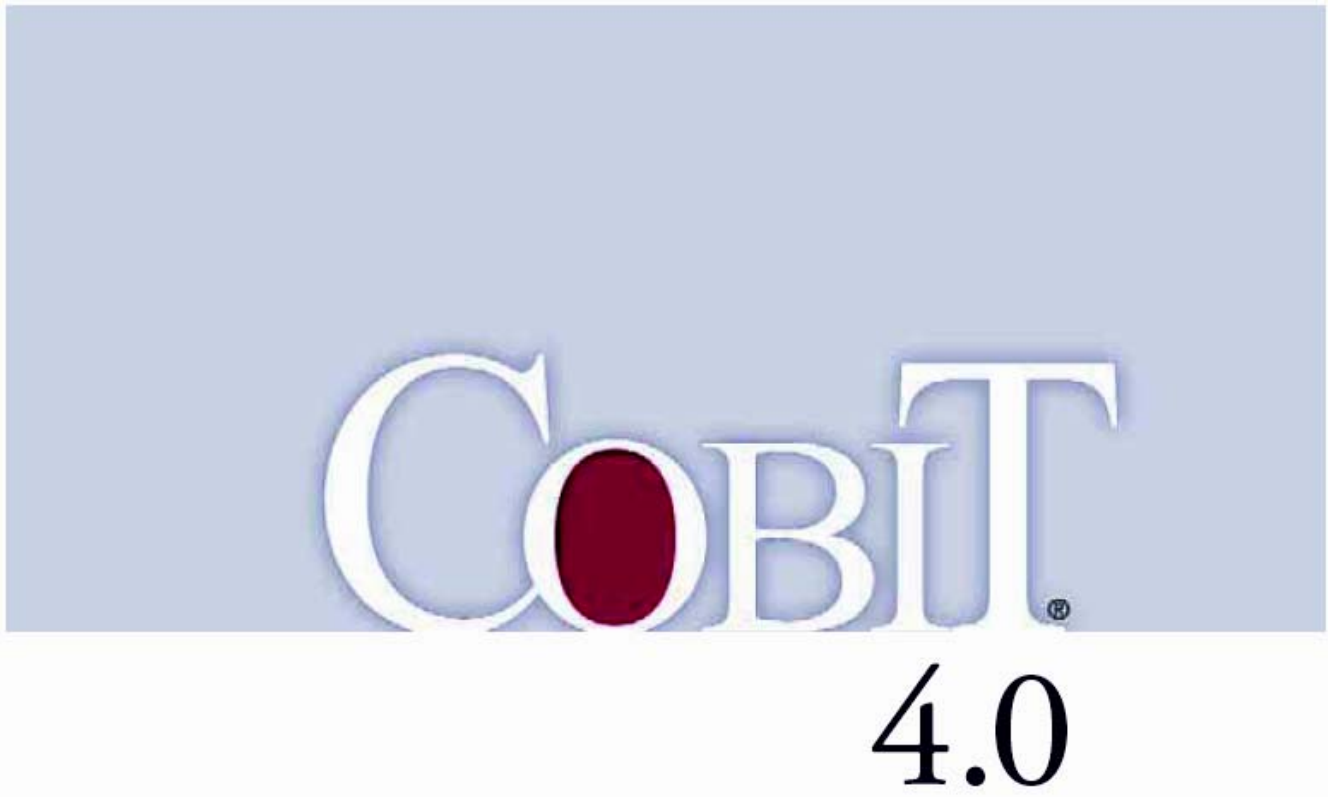
7. COBIT

Control Objectives for Information and related Technology

2006



GOVERNANCE INSTITUTE®

Objectives of implementing COBIT

- Supporting IT Governance
  - COBIT supports IT governance by providing a framework to ensure that:
    - IT is aligned with the business
    - IT enables the business and maximizes benefits
    - IT resources are used responsibly
    - IT risks are managed appropriately

COBIT Framework History

- The COBIT framework was defined in the first edition, copyrighted in April 1996 by the IT Governance Institute.
- The COBIT® 2nd Edition© released in 1998
- The COBIT® 3rd Edition© released in 2000
- The COBIT® 4.0 Edition© released in 2005

COBIT is Measurement-driven

COBIT provides:

- Maturity models to enable benchmarking and identification of necessary capability improvements
- Performance goals and metrics for the IT processes, demonstrating how processes meet business and IT goals and are used for measuring internal process performance based on balanced scorecard principles
- Activity goals for enabling effective process performance

The core content

- The core content is divided according to the 34 IT processes.
- Each process is covered in four sections of approximately one page each, combining to give a complete picture of how
  - to control,
  - manage and
  - measure the process.

The four sections for each process are:

1. The high-level control objective for the process
   (a) A process description summarizing the process objectives
   (b) A high-level control objective represented in a waterfall summarizing process goals, metrics and practices
   (c) The mapping of the process to the process domains, information criteria, IT resources and IT governance focus
2. The detailed control objectives for the process
3. Management guidelines:
   - the process inputs and outputs
   - RACI (Responsible, Accountable, Consulted and/or Informed)
4. The maturity model for the process

How Is COBIT 4.0 Different From COBIT 3rd Edition?

- COBIT 4.0 is an enhancement of COBIT 3rd Edition and in no way invalidates any implementation or execution activities based on COBIT 3rd Edition.
- The introduction of COBIT 4.0 provides the opportunity to further improve IT governance and control arrangements.

Executive Overview

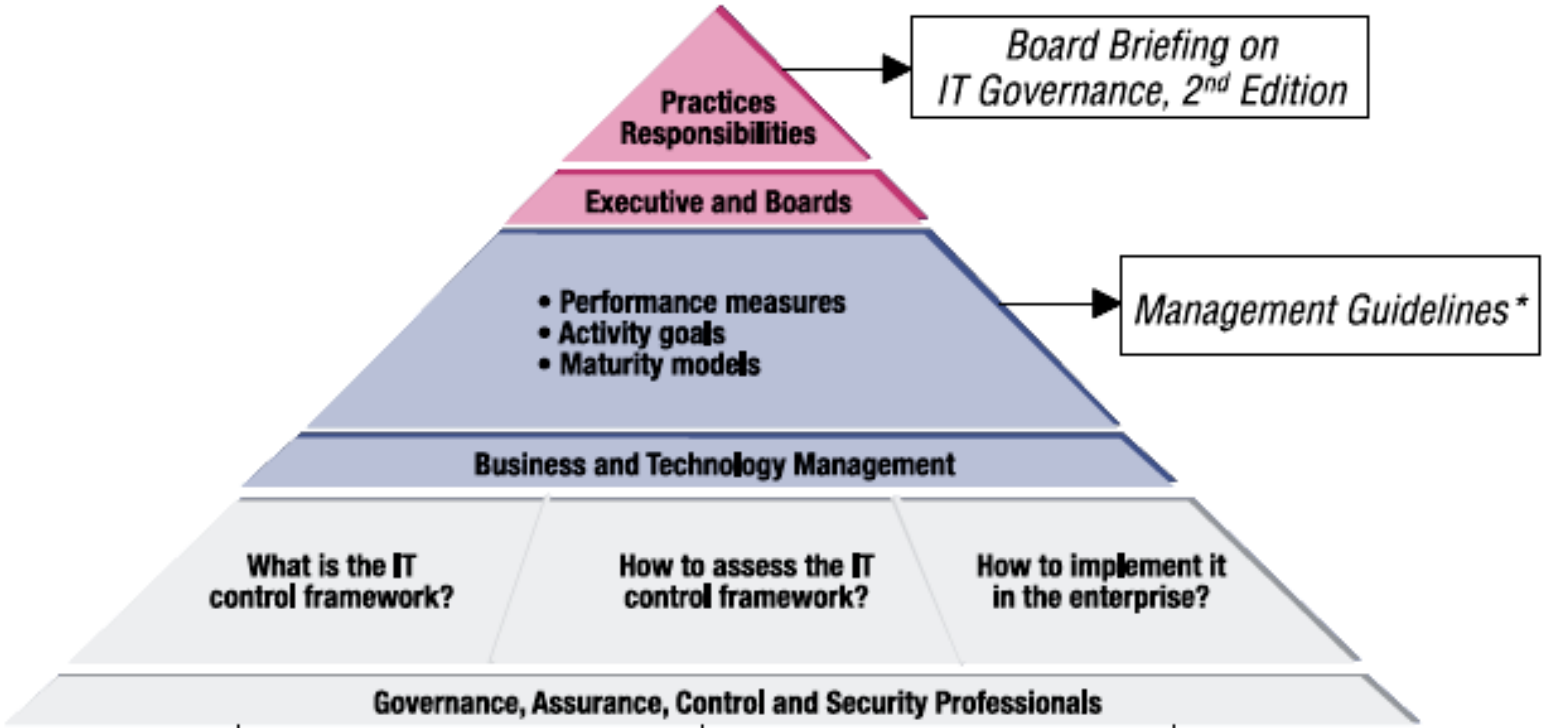
IT Governance Focus Areas

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organisation.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COBIT as the generally accepted internal control framework for IT

- COBIT is focused on what is required to achieve adequate management and control of IT.
- COBIT has been aligned and harmonised with other, more detailed, IT standards and best practices.
  - *Example:* COSO is generally accepted as the internal control framework for enterprises.
  - COBIT is the generally accepted internal control framework for IT.
- COBIT has become the integrator for IT best practices and the umbrella framework for IT governance that helps in understanding and managing the risks and benefits associated with IT.

COBIT Products



* Now integrated into CobiT 4.0

Framework

- Explaining how COBIT organises IT governance objectives and best practices by IT domains and processes, and links them to business requirements

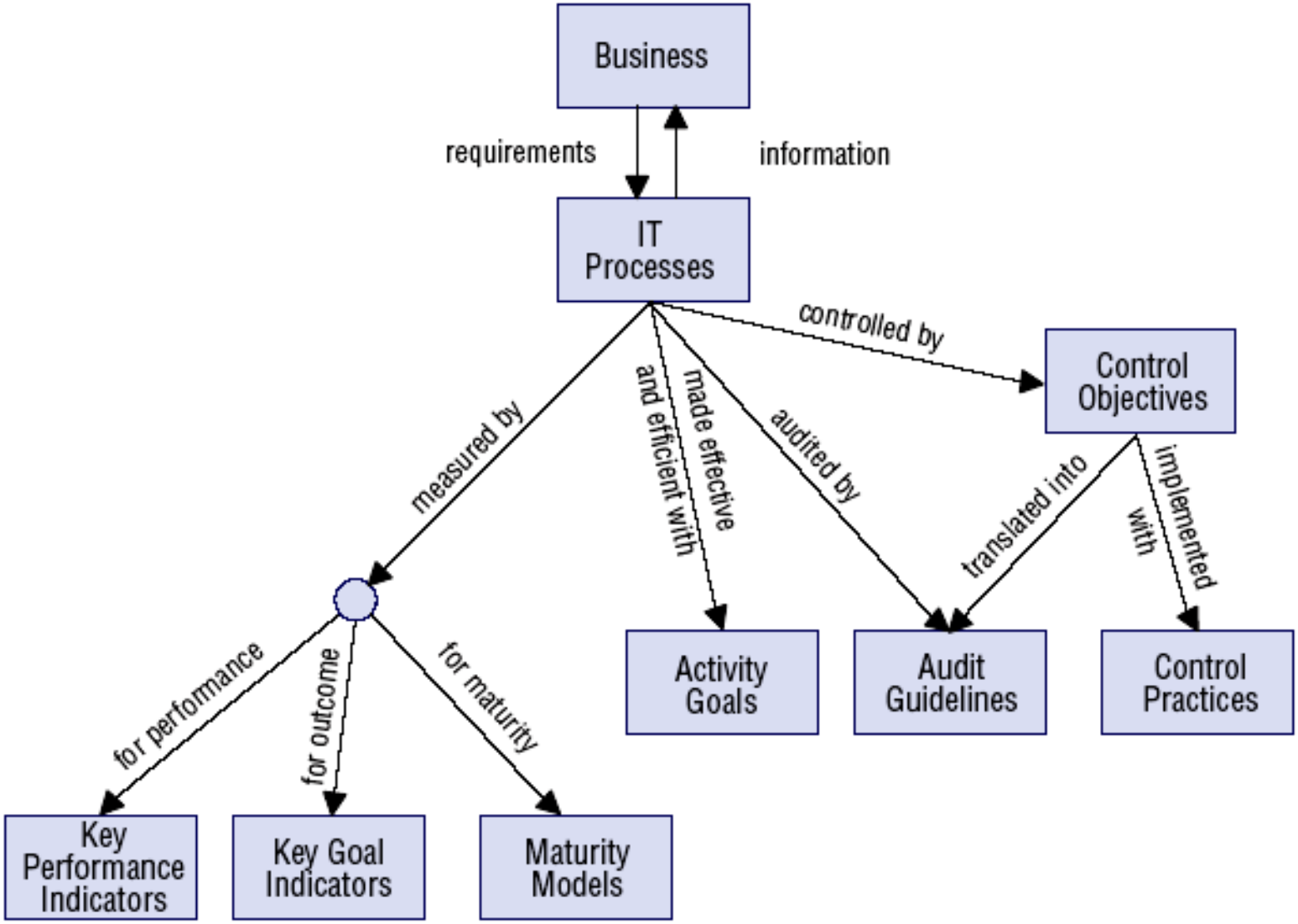
Control objectives

- Providing generic best practice management objectives for all IT activities

Control Practices

- Providing guidance on why controls are worth implementing and how to implement them

Interrelationships of COBIT Components

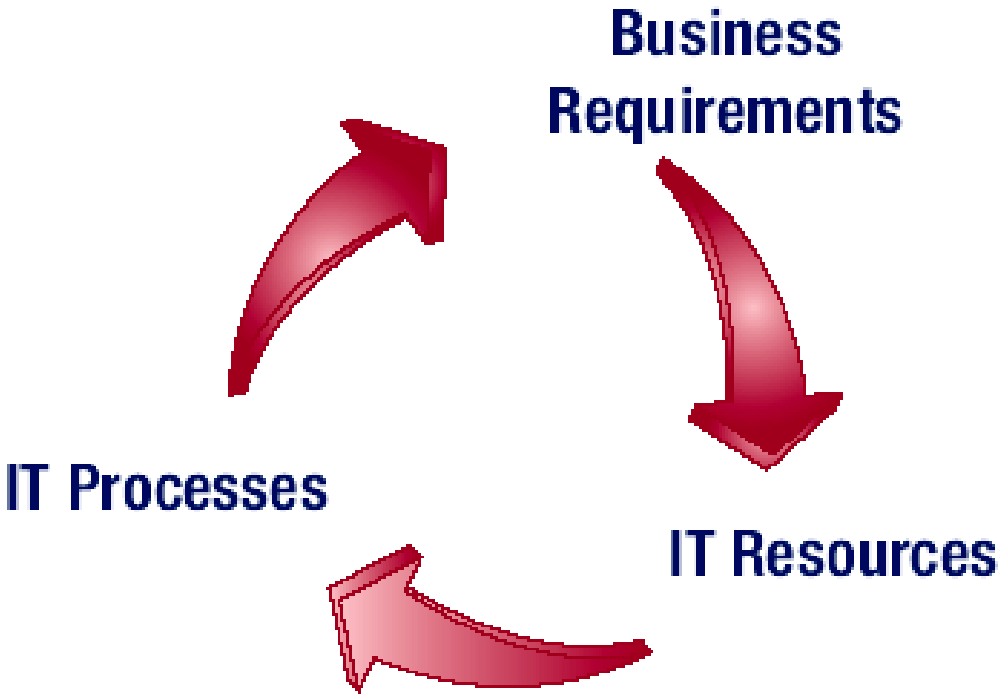


COBIT Framework

Basic COBIT Principle: *Business-focused*

- Business orientation is the main theme of COBIT.
- The COBIT framework is based on the following principle:
  - to provide the information that
    - the enterprise requires to achieve its objectives,
    - the enterprise needs to manage and control IT resources using a structured set of processes to deliver the required information services.
- The COBIT framework provides tools to help ensure alignment to business requirements.

Basic COBIT Principle: *Business-focused*



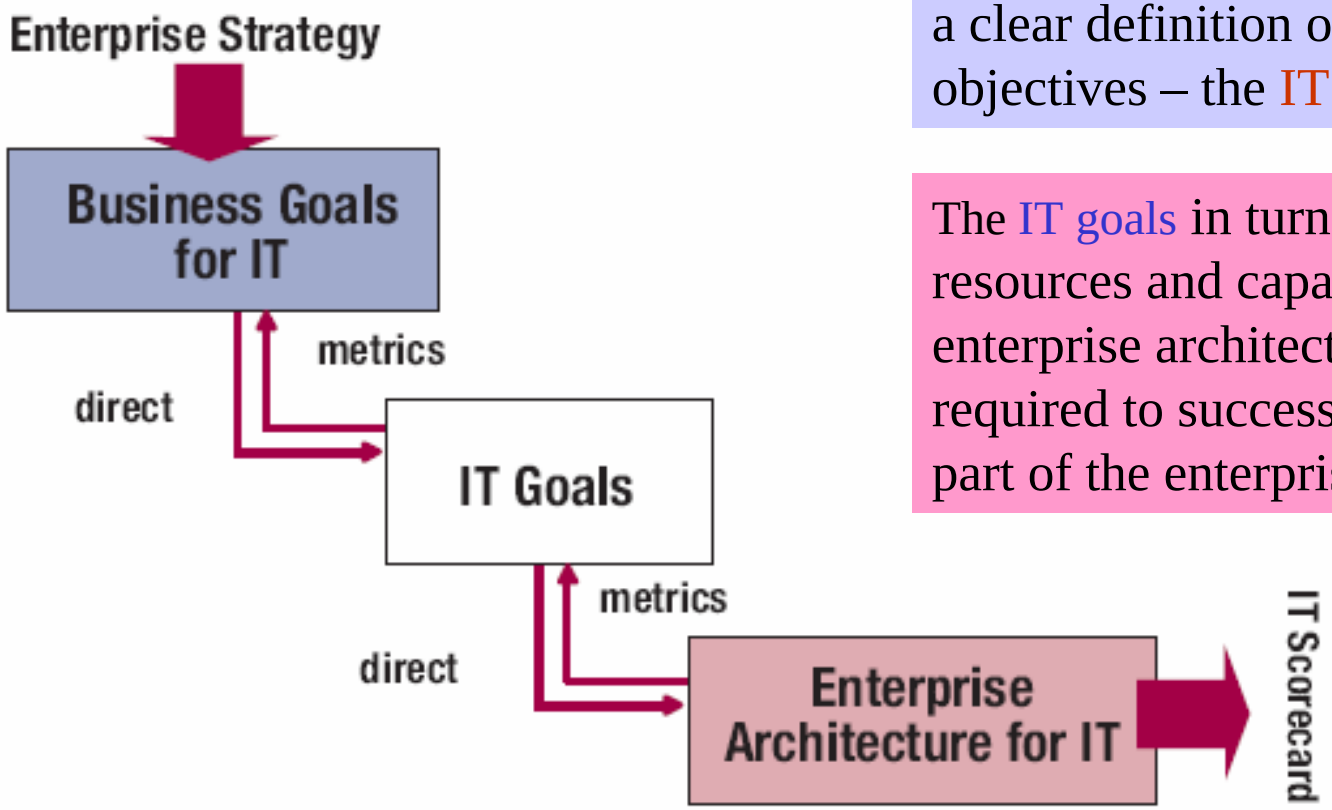
COBIT's information criteria

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorised disclosure.
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance** deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria, as well as internal policies.
- **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

- Effectiveness
- Efficiency
- Availability
- Integrity
- Confidentiality
- Reliability
- Compliance

- tõhusus
- efektiivsus
- ...

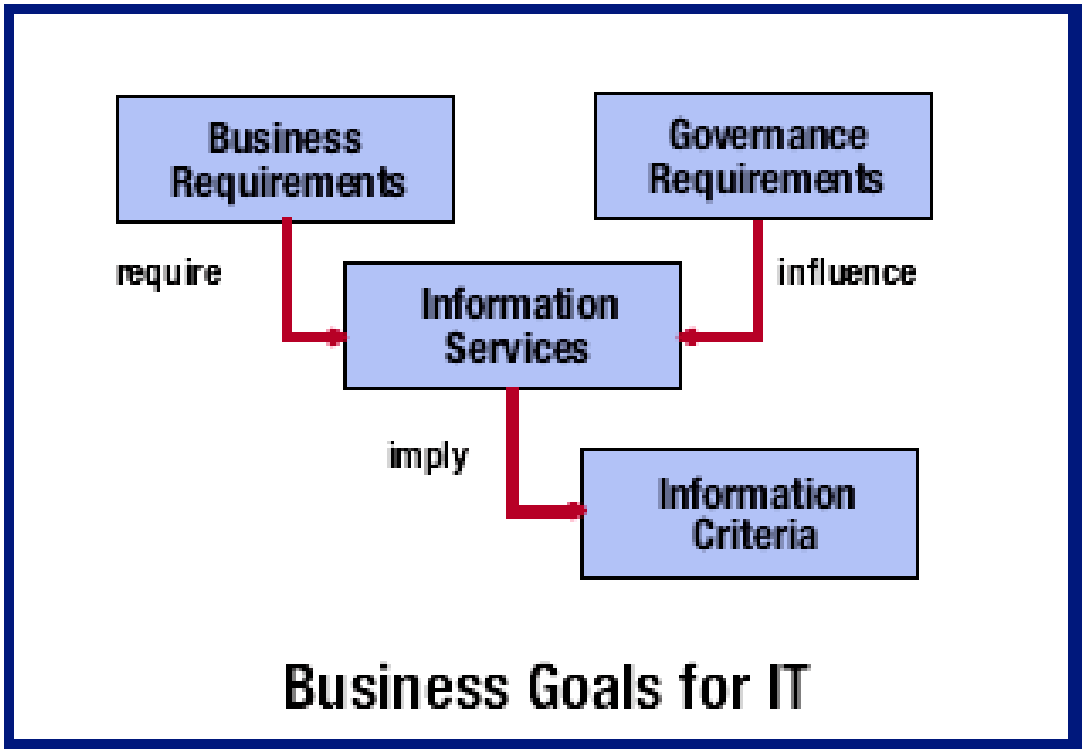
Defining IT Goals and Enterprise Architecture for IT



Business goals for IT should lead to a clear definition of IT's own objectives – the IT goals

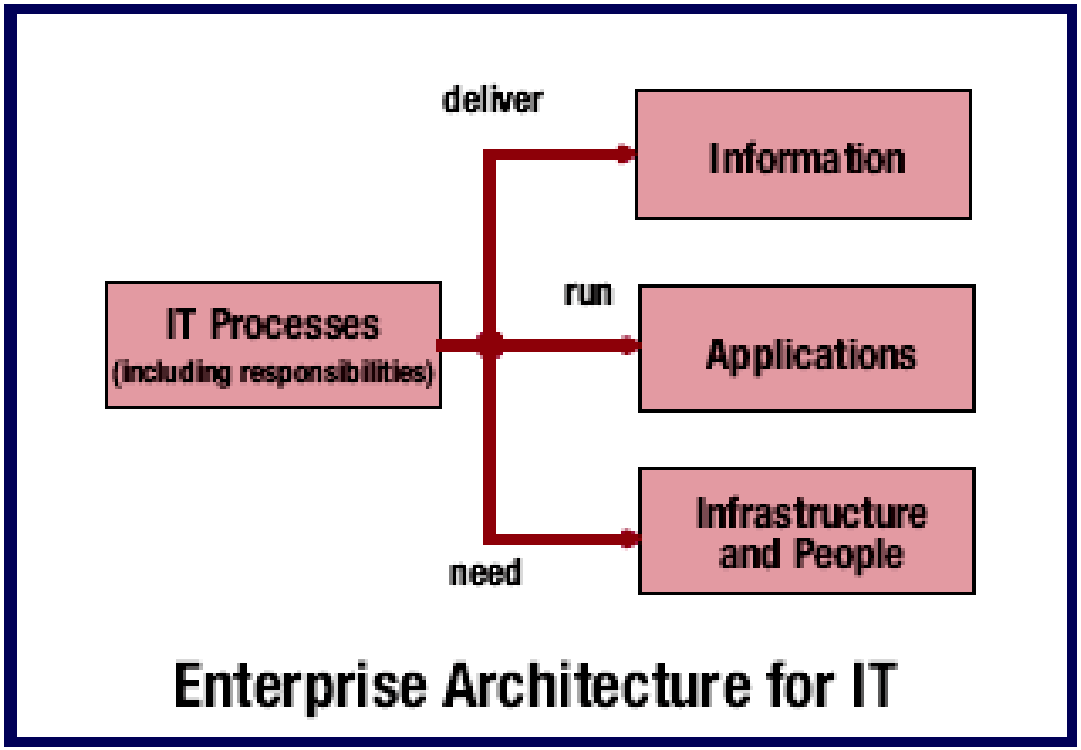
The IT goals in turn define the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the enterprise's strategy.

Business Goals for IT

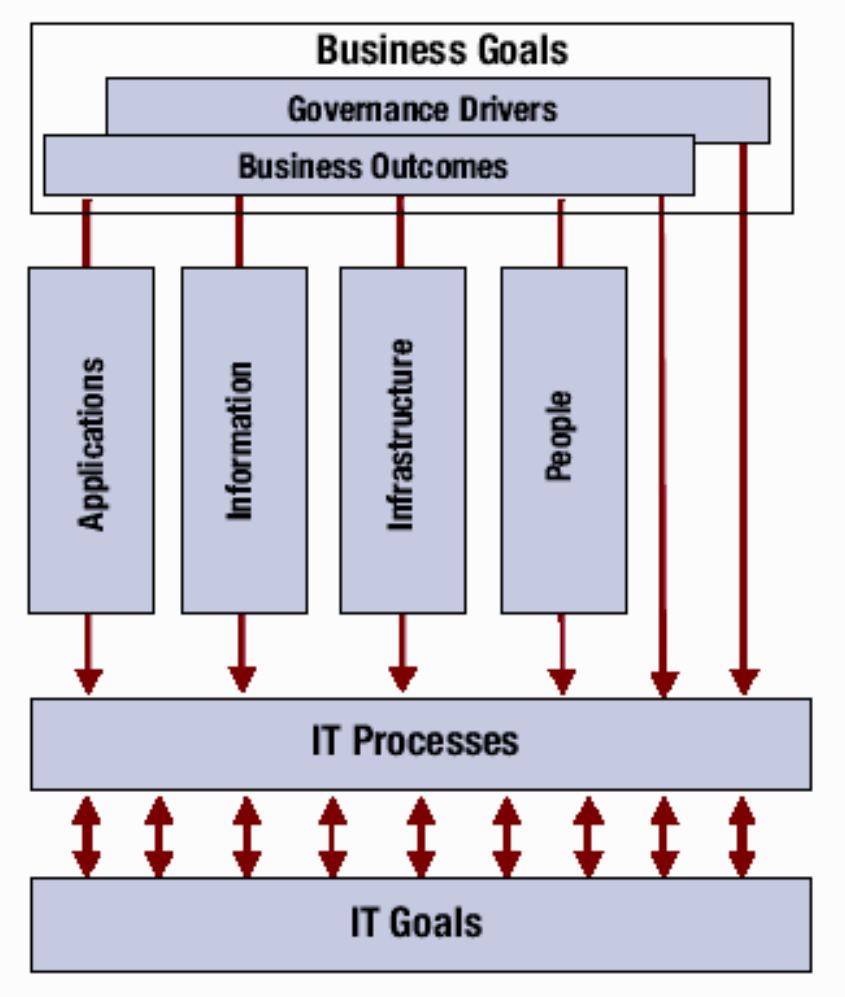


Every enterprise uses IT to enable business initiatives and these can be represented as business goals for IT.

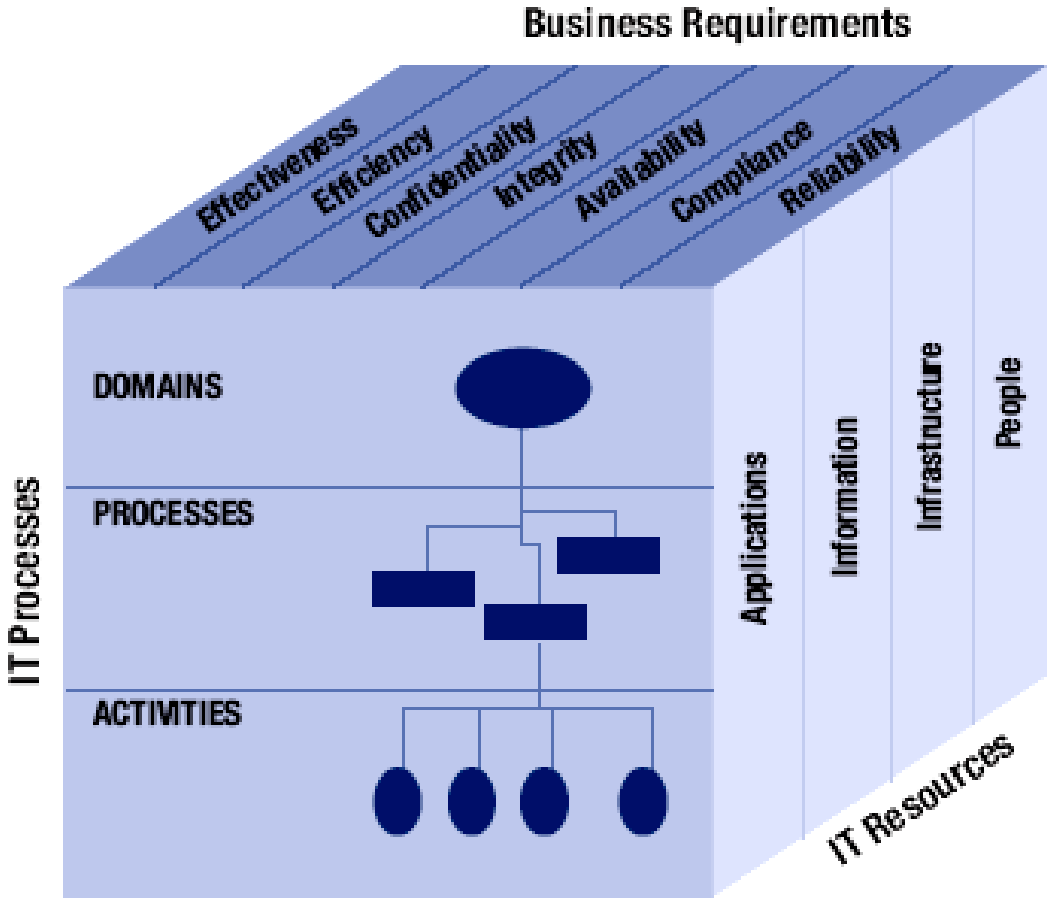
Enterprise Architecture for IT



Managing IT Resources to Deliver IT Goals



The COBIT Cube



Business Goals and IT Goals

Linking Business Goals to IT Goals

		Business Goals	IT Goals							
Financial Perspective	1	Expand market share.	25	28						
	2	Increase revenue.	25	28						
	3	Return on investment	24							
	4	Optimise asset utilisation.	14							
	5	Manage business risks.	2	14	17	18	19	20	21	22
Customer Perspective	6	Improve customer orientation and service.	3	23						
	7	Offer competitive products and services.	5	24						
	8	Service availability	10	16	22	23				
	9	Agility in responding to changing business requirements (time to market)	1	5	25					
	10	Cost optimisation of service delivery	7	8	10	24				
Internal Perspective	11	Automate and integrate the enterprise value chain.	6	7	8	11				
	12	Improve and maintain business process functionality.	6	7	11					
	13	Lower process costs.	7	8	13	15	24			
	14	Compliance with external laws and regulations	2	19	20	21	22	26	27	
	15	Transparency	2	18						
	16	Compliance with internal policies	2	13						
	17	Improve and maintain operational and staff productivity.	7	8	11	13				
Learning and Growth Perspective	18	Product/business innovation	5	25	28					
	19	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26			
	20	Acquire and maintain skilled and motivated personnel.	9							

IT Goals

1	Respond to business requirements in alignment with the business strategy.
2	Respond to governance requirements in line with board direction.
3	Ensure the satisfaction of end users with service offerings and service levels.
4	Optimise the use of information.
5	Create IT agility.
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.
7	Acquire and maintain integrated and standardised application systems.
8	Acquire and maintain an integrated and standardised IT infrastructure.
9	Acquire and maintain IT skills that respond to the IT strategy.
10	Ensure mutual satisfaction of third-party relationships.
11	Seamlessly integrate applications and technology solutions into business processes.
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.
13	Ensure proper use and performance of the applications and technology solutions.
14	Account for and protect all IT assets.

IT Goals

15	Optimise the IT infrastructure, resources and capabilities.
16	Reduce solution and service delivery defects and rework.
17	Protect the achievement of IT objectives.
18	Establish clarity of business impact of risks to IT objectives and resources.
19	Ensure critical and confidential information is withheld from those who should not have access to it.
20	Ensure automated business transactions and information exchanges can be trusted.
21	Ensure IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.
22	Ensure minimum business impact in the event of an IT service disruption or change.
23	Make sure that IT services are available as required.
24	Improve IT's cost-efficiency and its contribution to business profitability.
25	Deliver projects on time and on budget meeting quality standards.
26	Maintain the integrity of information and processing infrastructure.
27	Ensure IT compliance with laws and regulations.
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.

Management guidelines

Performance Measurement

Goals and metrics are defined in COBIT at three levels:

- IT goals and metrics that define what the business expects from IT (what the business would use to measure IT)
- Process goals and metrics that define what the IT process must deliver to support IT's objectives (how the IT process owner would be measured)
- Process performance metrics (to measure how well the process is performing to indicate if the goals are likely to be met)

CSF, KGI, KPI

- **Critical Success Factors -** for getting processes under control
- **Key Goal Indicators -** for monitoring achievement of IT process goals
- **Key Performance Indicators -** for monitoring performance within each IT process

Key goal indicators

Key goal indicators (KGI) define measures that tell management—after the fact—whether an IT process has achieved its business requirements, usually expressed in terms of information criteria:

- Availability of information needed to support the business needs
- Absence of integrity and confidentiality risks
- Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance

Key performance indicators

- Key performance indicators (KPI) define measures that determine how well the IT process is performing in enabling the goal to be reached.
- They are lead indicators of whether a goal will likely be reached or not, and are good indicators of capabilities, practices and skills.
- They measure the activity goals, which are the actions the process owner must take to achieve effective process performance.

How Well Enterprise is Currently Performing

- For effective IT governance to be implemented, enterprises need to assess how well they are currently performing and be able to identify where and how improvements can be made.
- This applies to both the IT governance process itself and all the processes that need to be managed within IT.
- The use of **maturity models** greatly simplifies this task and provides a pragmatic and structured approach for measuring how well developed an enterprise's processes are against a consistent and easy-to-understand scale.

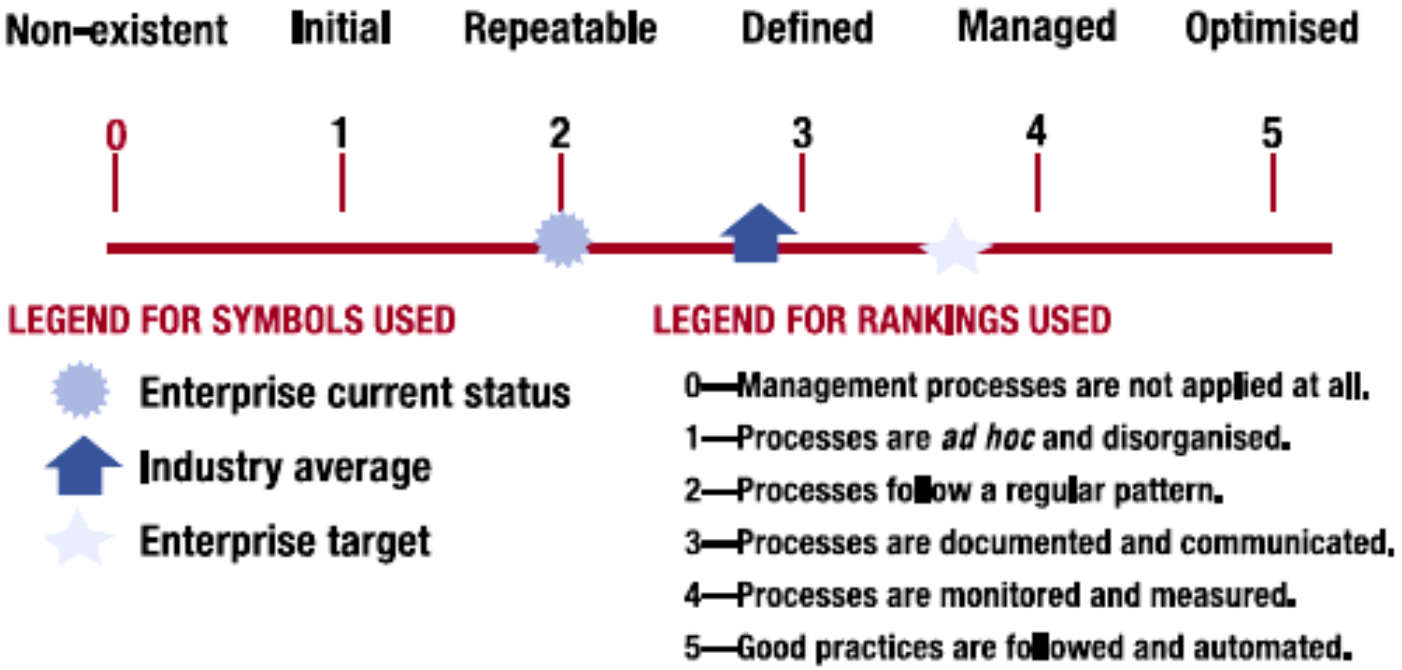
Maturity Models

- Maturity models are techniques enabling the enterprise:
  - Build a view of current practices by discussing them in workshops and comparing to example models
  - Set targets for future development by considering model descriptions higher up the scale and comparing to best practices
  - Plan projects to reach the targets by defining the specific changes required to improve management
  - Prioritise project work by identifying where the greatest impact will be made and where it is easiest to implement

Maturity models

- Maturity modelling for management and control over IT processes is based on a method of evaluating the organisation, so it can evaluate itself from a level of non-existent (0) to optimised (5).
- Using the maturity models developed for each of COBIT's 34 IT processes, management can identify:
  - The actual performance of the enterprise—Where the enterprise is today
  - The current status of the industry—The comparison
  - The enterprise's target for improvement—Where the enterprise wants to be

Maturity models



Generic Maturity Model

0 Non-Existent. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.

2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.

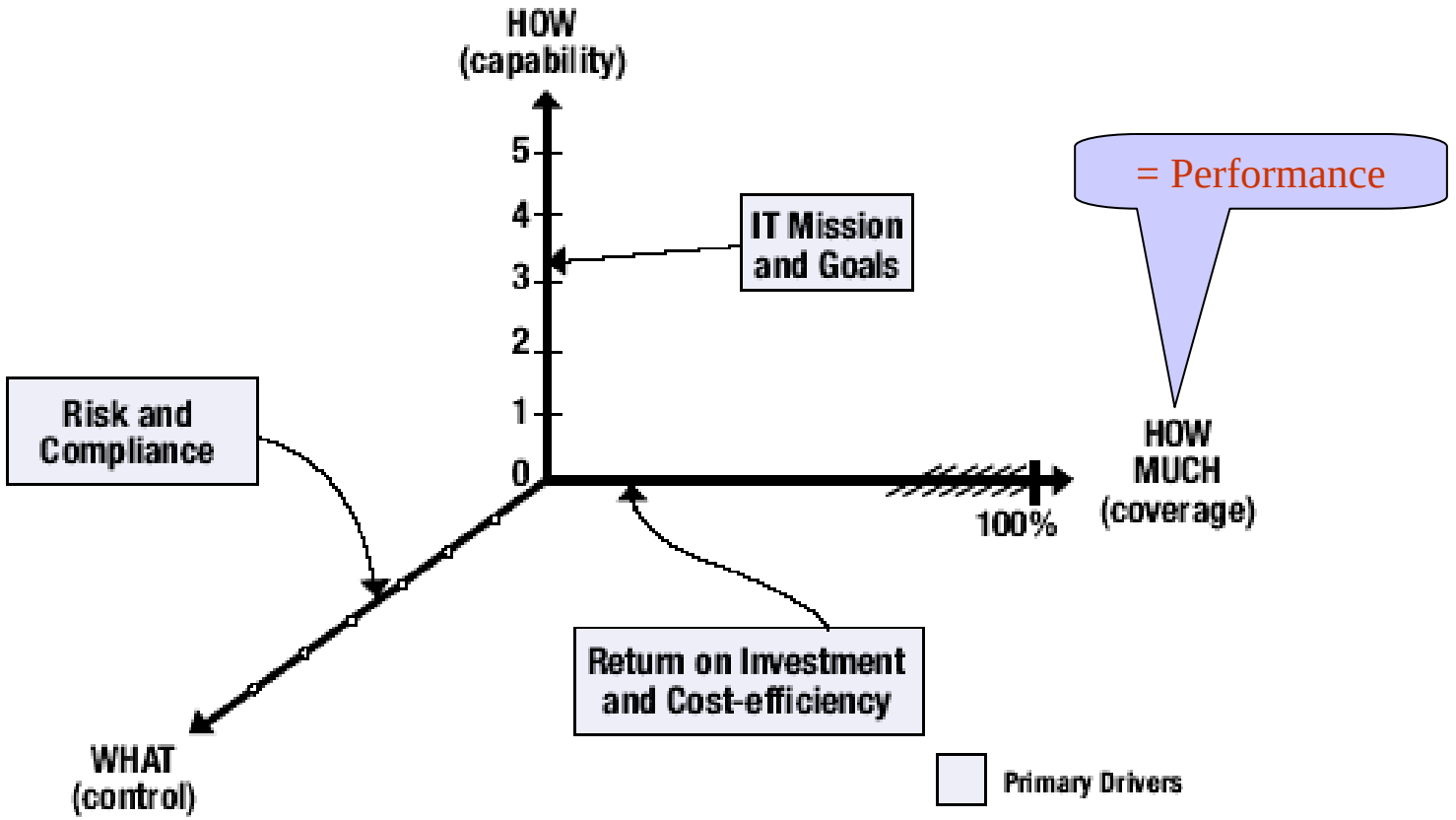
3 Defined. Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

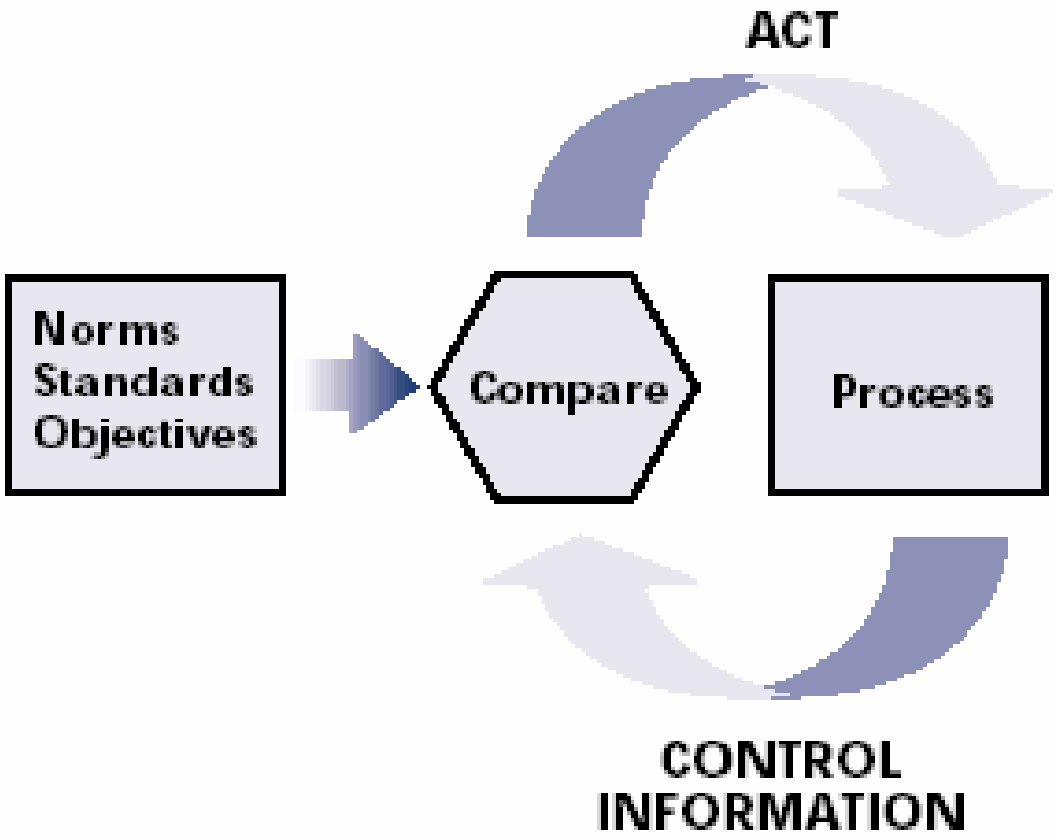
5 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

This approach is derived from the maturity model that the Software Engineering Institute defined for the maturity of software development capability.

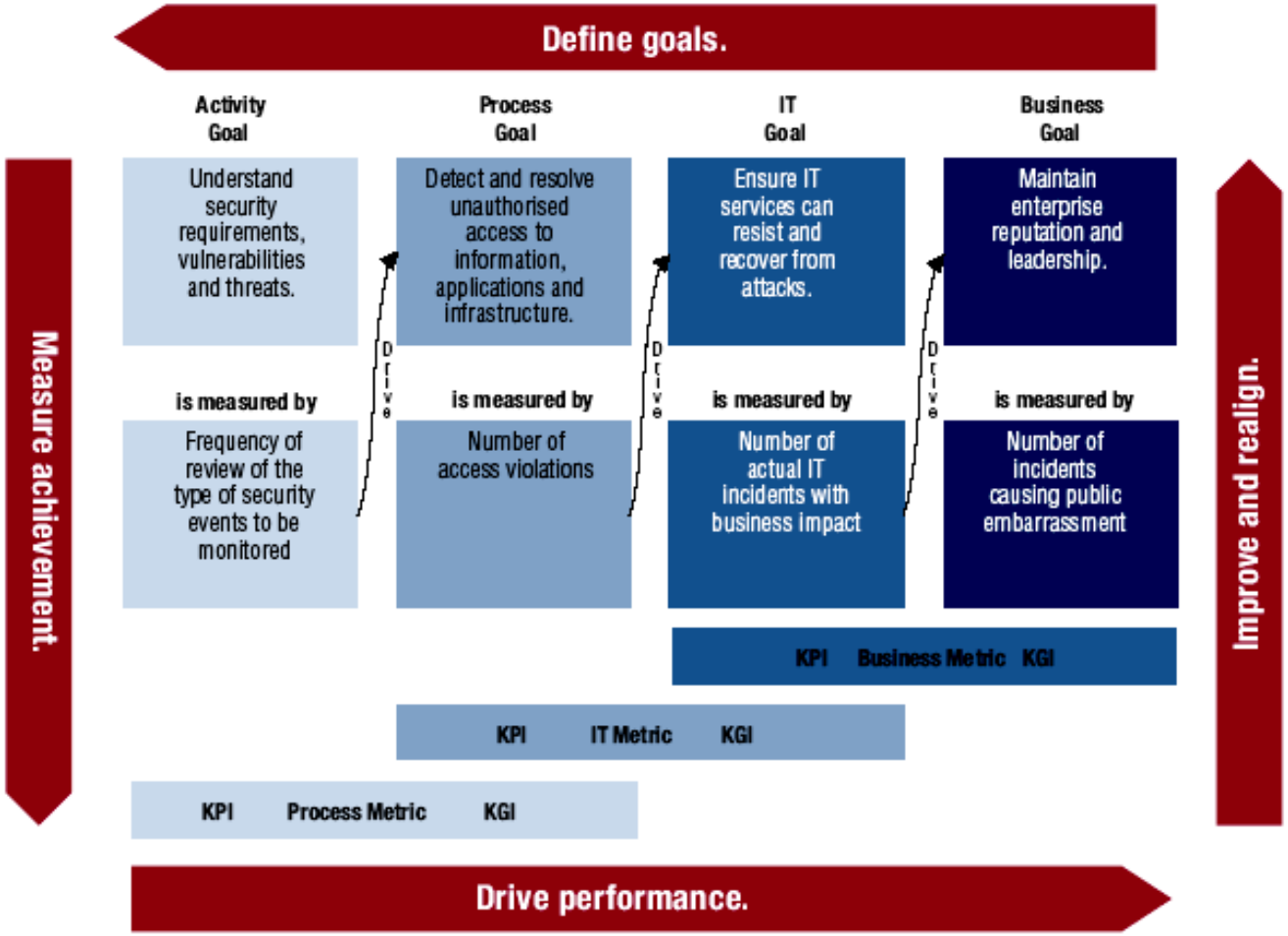
The Three Dimensions of Maturity



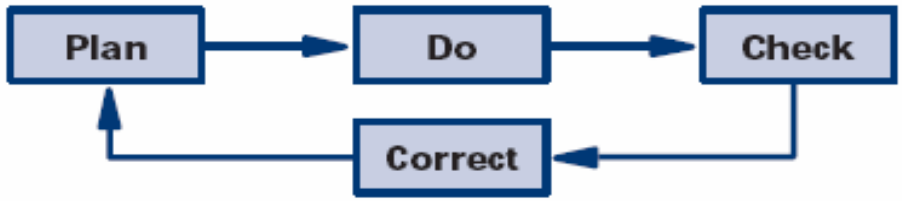
Critical Success Factors



Example: Relationship Among Process, Goals and Metrics (DS5 – Ensure systems security)



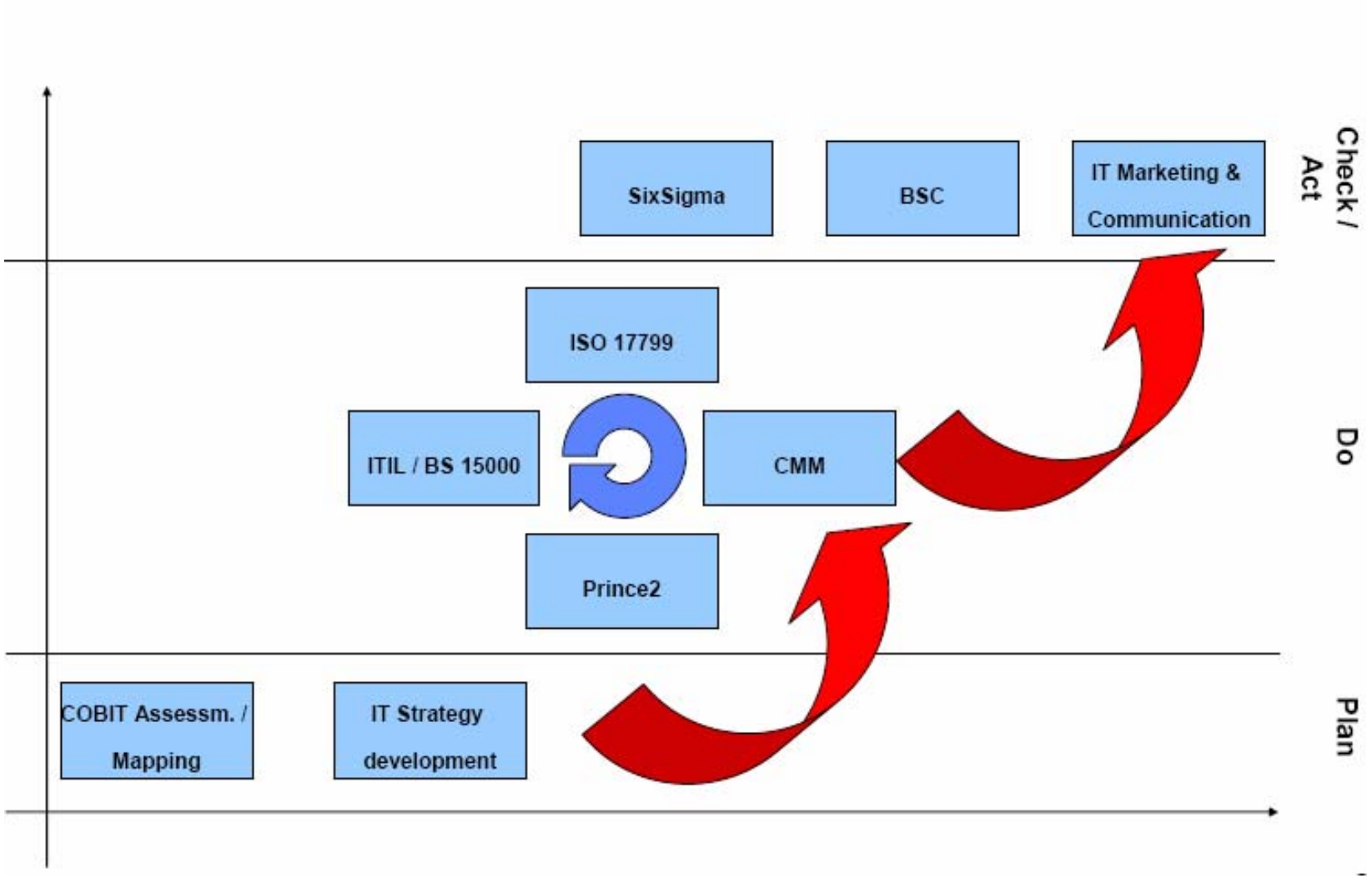
Four Types of Activities

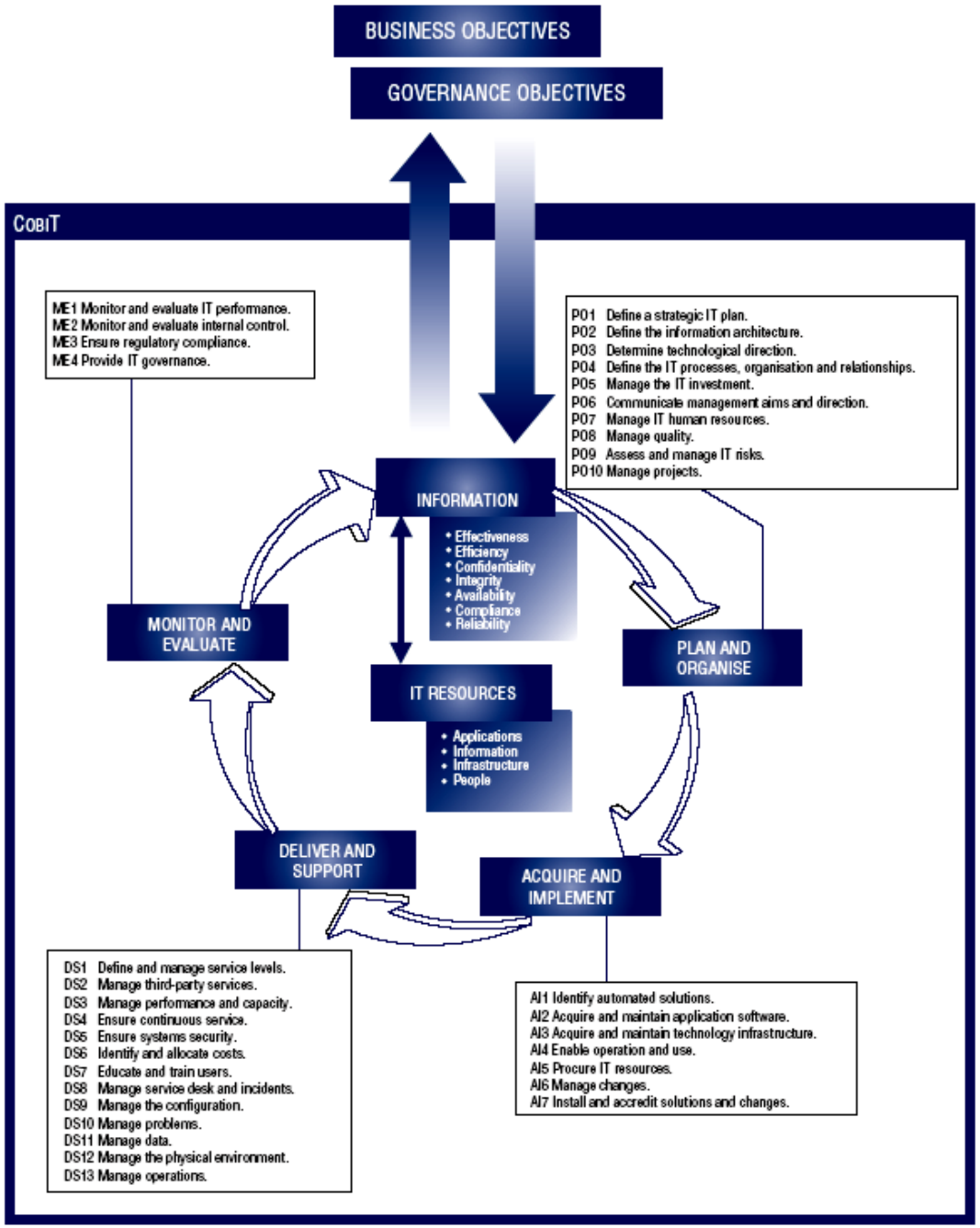


These control principles are needed at different levels, at
- strategic
- tactical
- administrative level

- There are usually four types of activities at each level that logically follow each other:
  - planning
  - doing
  - checking
  - correcting
- The feedback and control loop mechanisms between the levels should be considered.

Plan-Do-Check-Correct





Overall COBIT Framework

PLAN AND ORGANISE

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation 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 IT risks.
PO10 Manage projects.

ACQUIRE AND IMPLEMENT

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.

DELIVER 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.

COBIT Framework and IT Governance Focus Areas

	Goals	Metrics	Practices	Maturity Models
Strategic alignment	P	P		
Value delivery		P	S	P
Risk management		S	P	S
Resource management		S	P	P
Performance measurement	P	P		S

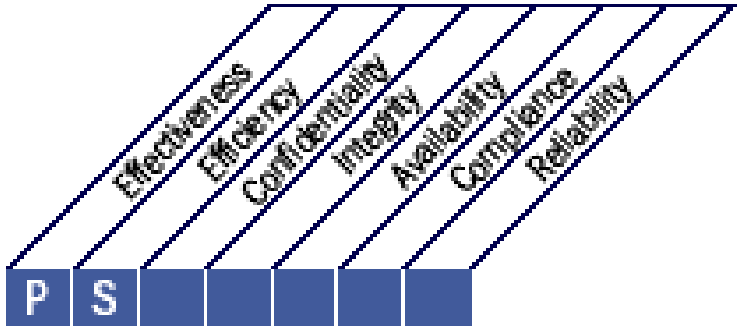
P=Primary enabler S=Secondary enabler

Plan and Organise

PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organisation 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 IT Risks
PO10	Manage Projects

PO1 Define a Strategic IT Plan

- IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities.
- The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios.
- The strategic plan should improve key stakeholders' understanding of IT opportunities and limitations, assess current performance and clarify the level of investment required.
- The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which establishes concise objectives, plans and tasks understood and accepted by both business and IT.



PO1 Define a Strategic IT Plan

Control over the IT process of

Define a strategic IT plan

that satisfies the business requirement for IT of

sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks

by focusing on

incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

is achieved by

- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

and is measured by

- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plan
- Delay between updates of IT strategic plan and updates of IT tactical plans

Detailed Control Objectives

PO1 Define a Strategic IT Plan

PO1.1 IT Value Management

- Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases.
- Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds.
- IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes.
- IT services should be executed against equitable and enforceable service level agreements.
- Accountability for achieving the benefits and controlling the costs is clearly assigned and monitored.
- Establish fair, transparent, repeatable and comparable evaluation of business cases including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.

PO1.2 Business-IT Alignment

- Educate executives on current technology capabilities and future directions, the opportunities that IT provides, and what the business has to do to capitalise on those opportunities.
- Make sure the business direction to which IT is aligned is understood.
- The business and IT strategies should be integrated, clearly linking enterprise goals and IT goals and recognising opportunities as well as current capability limitations, and broadly communicated.
- Identify where the business (strategy) is critically dependent on IT and mediate between imperatives of the business and the technology, so agreed priorities can be established.

PO1.3 Assessment of Current Performance

- Assess the performance of the existing plans and information systems in terms of
  - contribution to business objectives,
  - functionality,
  - stability,
  - complexity,
  - costs,
  - strengths and weaknesses.

PO1.4 IT Strategic Plan

- Create a strategic plan that defines, in co-operation with the relevant stakeholders, how IT will contribute to the enterprise's strategic objectives (goals) and related costs and risks.
- It includes how IT will support IT-enabled investment programmes and operational service delivery.
- It defines how the objectives will be met and measured and will receive formal sign-off from the stakeholders.
- The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements.
- The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans.

PO1.5 IT Tactical Plans

- Create a portfolio of tactical IT plans that are derived from the IT strategic plan.
- These tactical plans describe
  - required IT initiatives,
  - resource requirements, and
  - how the use of resources and achievement of benefits will be monitored and managed.
- The tactical plans should be sufficiently detailed to allow the definition of project plans.
- Actively manage the set tactical IT plans and initiatives through analysis of project and service portfolios.
- This encompasses balancing requirements and resources on a regular basis, comparing them to achievement of strategic and tactical goals and the expected benefits, and taking appropriate action on deviations.

PO1.6 IT Portfolio Management

- Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by
  - identifying,
  - defining,
  - evaluating,
  - prioritising,
  - selecting,
  - initiating,
  - managing and
  - controlling programmes.
- This includes
  - clarifying desired business outcomes,
  - ensuring that programme objectives support achievement of the outcomes,
  - understanding the full scope of effort required to achieve the outcomes,
  - assigning clear accountability with supporting measures,
  - defining projects within the programme,
  - allocating resources and funding, delegating authority, and
  - commissioning required projects at programme launch.

PO1 Define a Strategic IT Plan – Inputs and Outputs

From	Inputs
PO5	Cost/benefits reports
PO9	Risk assessment
PO10	Updated project portfolio
DS1	New/updated service requirements; updated service portfolio
*	Business strategy and priorities
*	Programme portfolio
ME1	Performance input to IT planning
ME4	Report on IT governance status; enterprise strategic direction for IT

* Inputs from outside CobiT

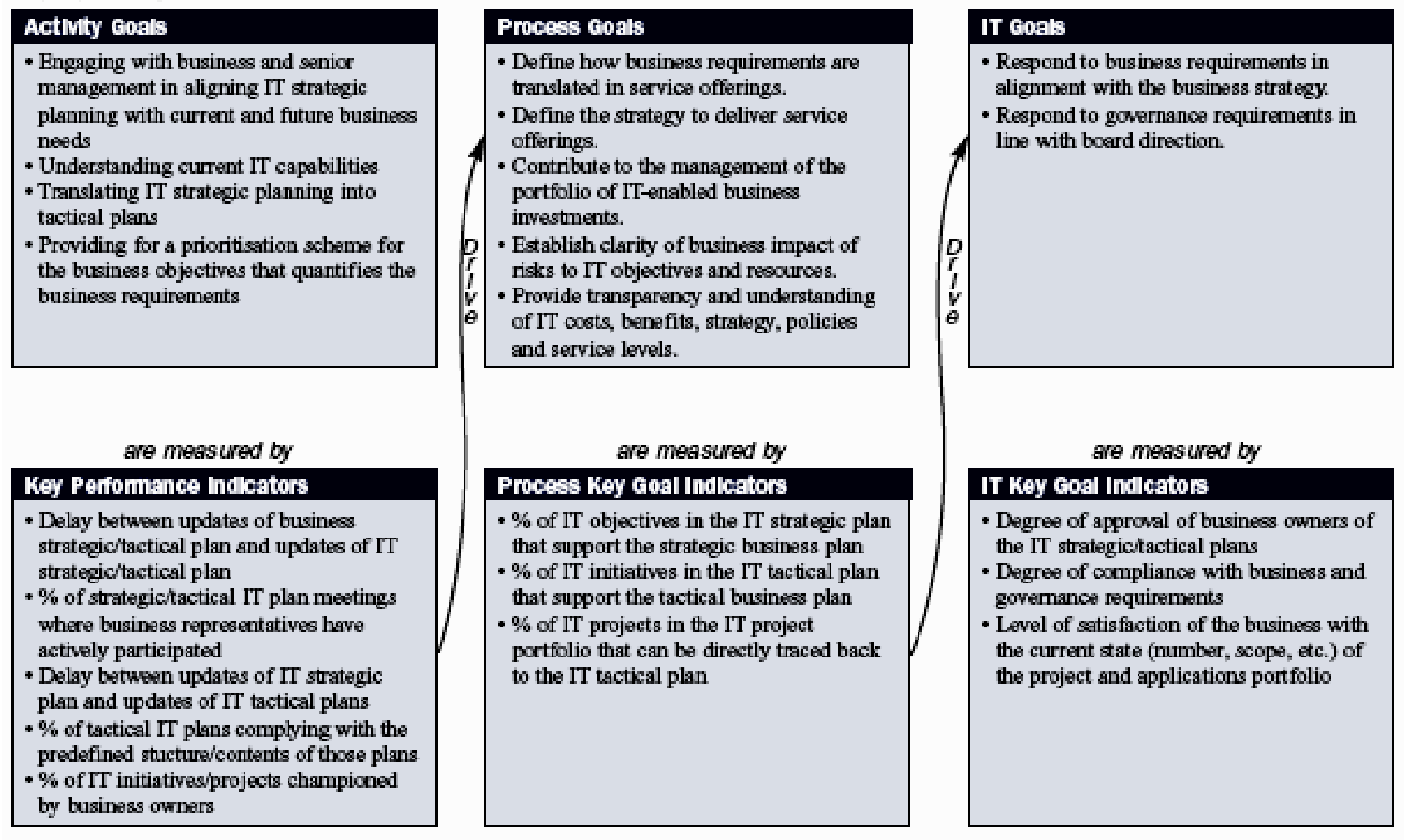
Outputs	To						
Strategic IT plan	PO2...PO6	PO8	PO9	AI1	DS1		
Tactical IT plan	PO2...PO6	PO9	AI1	DS1			
IT project portfolio	PO5	PO6	PO10	AI6			
IT service portfolio	PO5	PO6	PO9	DS1			
IT sourcing strategy	DS2						
IT acquisition strategy	AI5						

PO1 Define a Strategic IT Plan – RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
	Functions										
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

PO1 Define a Strategic IT Plan – Goals and Metrics



PO1 Define a Strategic IT Plan – Maturity Model

Management of the process of Define a strategic IT plan that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks is either:

- 0 Non-existent
- 1 Initial/ Ad Hoc
- 2 Repeatable but Intuitive
- 3 Defined Process
- 4 Managed and Measurable
- 5 Optimised

0 Non-existent when

- IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/ Ad Hoc when

- The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement.
- IT strategic planning is occasionally discussed at IT management meetings.
- The alignment of business requirements, applications and technology takes place reactively rather than by an organisationwide strategy.
- The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive when

- IT strategic planning is shared with business management on an as-needed basis.
- Updating of the IT plans occurs in response to requests by management.
- Strategic decisions are driven on a project-by-project basis, without consistency with an overall organisation strategy.
- The risks and user benefits of major strategic decisions are being recognised in an intuitive way.

3 Defined Process when

- A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which is documented and known to all staff.
- The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed.
- However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process.
- The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower.
- The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies.
- IT strategic planning is discussed at business management meetings.

4 Managed and Measurable when

- IT strategic planning is standard practice and exceptions would be noticed by management.
- IT strategic planning is a defined management function with senior-level responsibilities.
- Management is able to monitor the IT strategic planning process, make informed decisions based on it and measure its effectiveness.
- Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed.
- The IT strategy and organisationwide strategy are increasingly becoming more co-ordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process reengineering.
- There is a well-defined process for determining the usage of internal and external resources required in system development and operations.

5 Optimised when

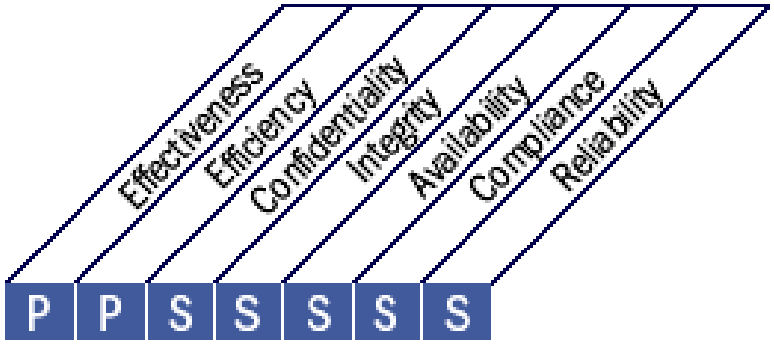
- IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernable business value through investments in IT.
- Risk and value-added considerations are continuously updated in the IT strategic planning process.
- Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments.
- Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process.
- The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Monitor and Evaluate

ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

ME4 Provide IT Governance

- Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.



ME4 Provide IT Governance

Control over the IT process of

Provide IT governance

that satisfies the business requirement for IT of

integrating IT governance with corporate governance objectives and complying with laws and regulations

by focusing on

preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions

is achieved by

- Establishing an IT governance framework integrated into corporate governance
- Obtaining independent assurance over the IT governance status

and is measured by

- Frequency of board reporting on IT to stakeholders (including maturity)
- Frequency of reporting from IT to board (including maturity)
- Frequency of independent reviews of IT compliance

Detailed Control Objectives

ME4 Provide IT Governance

ME4.1 Establishment of an IT Governance Framework

- Work with the board to define and establish an IT governance framework including leadership, processes, roles and responsibilities, information requirements, and organisational structures to ensure that the enterprise's IT-enabled investment programmes are aligned with and deliver on the enterprise's strategies and objectives.
- The framework should provide clear linkage among
  - the enterprise strategy,
  - the portfolio of IT-enabled investment programmes that execute the strategy,
  - the individual investment programmes, and
  - the business and IT projects that make up the programmes.
- The framework should provide for unambiguous accountabilities and practices to avoid breakdown in internal control and oversight.
- The framework should be consistent with the overall enterprise control environment and generally accepted control principles, and be based on the IT process and control framework.

ME4.2 Strategic Alignment

- Enable board and executive understanding of strategic IT issues such as the role of IT, technology insights and capabilities.
- Make sure there is a shared understanding between the business and IT of the potential contribution of IT to the business strategy.
- Make sure that there is a clear understanding that value is achieved from IT only when IT-enabled investments are managed as a portfolio of programmes that include the full scope of changes that the business has to make to optimise the value from IT capabilities in delivering on the strategy.
- Work with the board to define and implement governance bodies, such as an IT strategy committee, to provide strategic direction to management relative to IT, ensuring that the strategy and objectives are cascaded down into business units and IT functions, and that confidence and trust are developed between the business and IT.
- Enable the alignment of IT to the business in strategy and operations, encouraging co-responsibility between business and IT for making strategic decisions and obtaining benefits from IT-enabled investments.

ME4.3 Value Delivery

- Manage IT-enabled investment programmes and other IT assets and services to ensure that they deliver the greatest possible value in supporting the enterprise's strategy and objectives.
- Ensure that the expected business outcomes of IT-enabled investments and the full scope of effort required to achieve those outcomes is understood, that comprehensive and consistent business cases are created and approved by stakeholders, that assets and investments are managed throughout their economic life cycle, and that there is active management of the realisation of benefits, such as contribution to new services, efficiency gains and improved responsiveness to customer demands.
- Enforce a disciplined approach to portfolio, programme and project management, insisting that the business takes ownership of all IT-enabled investments and IT ensures optimisation of the costs of delivering IT capabilities and services.
- Ensure that technology investments are standardised to the greatest extent possible to avoid the increased cost and complexity of a proliferation of technical solutions.

ME4.4 Resource Management

- Optimise the investment, use and allocation of IT assets through regular assessment, making sure that IT has sufficient, competent and capable resources to execute the current and future strategic objectives and keep up with business demands.
- Management should put clear, consistent and enforced human resources policies and procurement policies in place to ensure that resource requirements are fulfilled effectively and to conform to architecture policies and standards.
- The IT infrastructure should be assessed on a periodic basis to ensure that it is standardised wherever possible and interoperability exists where required.

ME4.5 Risk Management

- Work with the board to define the enterprise's appetite for IT risk.
- Communicate IT risk appetite into the enterprise and agree on an IT risk management plan.
- Embed risk management responsibilities into the organisation, ensuring that the business and IT regularly assess and report IT-related risks and the impact on the business.
- Make sure IT management follows up on risk exposures, paying special attention to IT control failures and weaknesses in internal control and oversight, and their actual and potential business impact.
- The enterprise's IT risk position should be transparent to all stakeholders.

ME4.6 Performance Measurement

- Report relevant portfolio, programme and IT performance to the board and executives in a timely and accurate manner.
- Management reports should be provided for senior management's review of the enterprise's progress toward identified goals.
- Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated.
- Integrate reporting with similar output from other business functions.
- The performance measures should be approved by key stakeholders.
- The board and executive should challenge these performance reports and IT management should be given an opportunity to explain deviations and performance problems.
- Upon review, appropriate management action should be initiated and controlled.

ME4.7 Independent Assurance

- Ensure that the organisation establishes and maintains a function that is competent and adequately staffed and/or seeks external assurance services to provide the board—this will occur most likely through an audit committee—with timely independent assurance about the compliance of IT with its policies, standards and procedures, as well as with generally accepted practices.

ME4 Provide IT Governance – Inputs and Outputs

From	Inputs
PO4	IT process framework
PO5	Cost/benefit reports
PO9	Risk assessment and reporting
ME2	Report on effectiveness of IT controls
ME3	Catalogue of legal and regulatory requirements related to IT service delivery

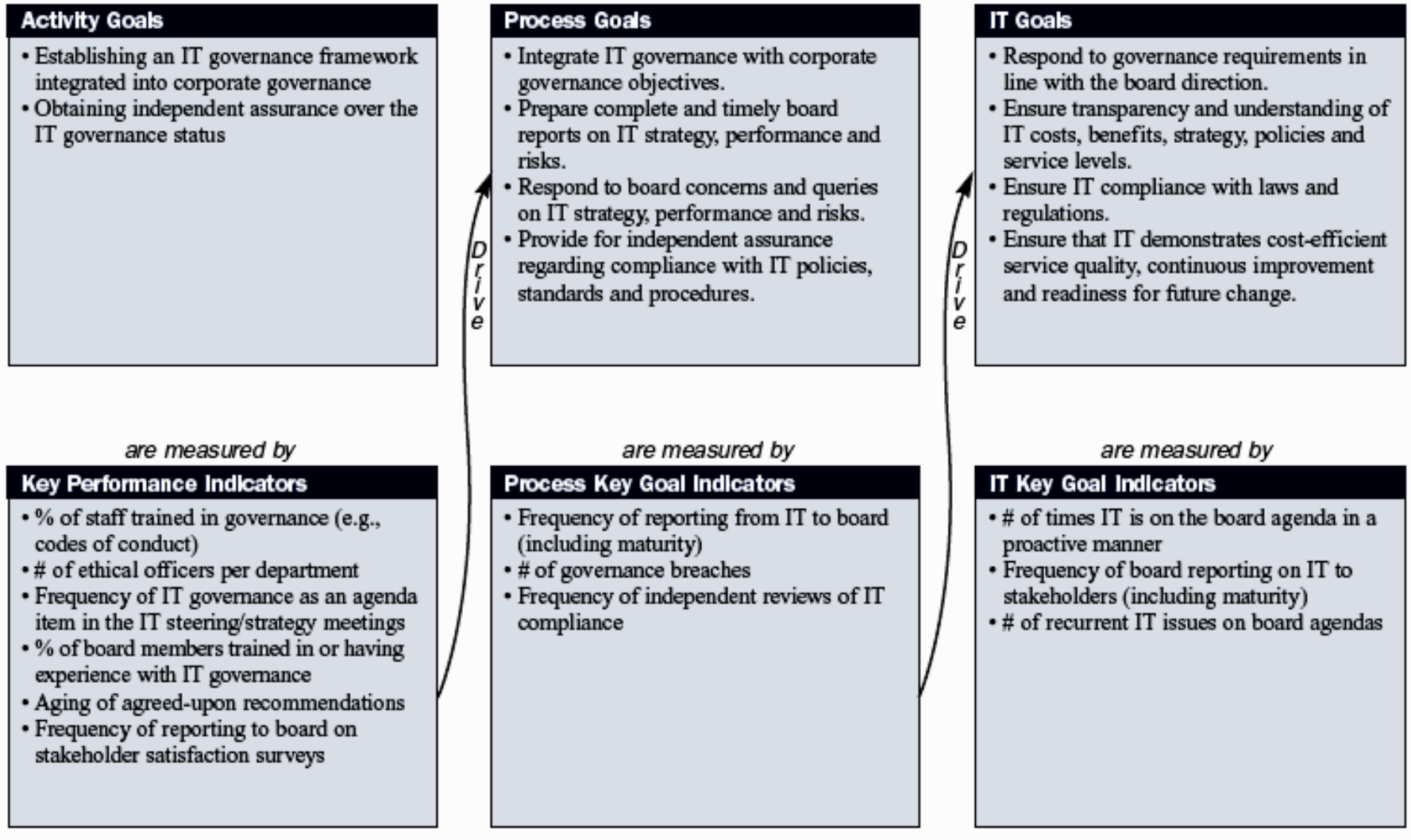
Outputs	To						
Process framework improvements	PO4						
Report on IT governance status	PO1	ME1					
Expected business outcome of IT-enabled business investments	PO5						
Enterprise strategic direction for IT	PO1						
Enterprise appetite for IT risks	PO9						

ME4 Provide IT Governance – RACI Chart

Activities	Board	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
	Functions											
Establish executive and board oversight and facilitation over IT activities.	A	R	C	C	C							C
Review, endorse, align and communicate IT performance, IT strategy, resource and risk management with business strategy.	A	R	I	I	R							C
Obtain periodic independent assessment of performance and compliance with policies, standards and procedures.	A	R	C	I	C		I	I	I	I	I	R
Resolve findings of independent assessments and ensure management's implementation of agreed-upon recommendations.	A	R	C	I	C		I	I	I	I	I	R
Generate an IT governance report.	A	C	C	C	R	C	I	I	I	I	I	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

ME4 Provide IT Governance – Goals and Metrics



ME4 Provide IT Governance – Maturity Model

- Management of the process of Provide IT governance that satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws and regulations is either:
  - 0 Non-existent
  - 1 Initial/ Ad Hoc
  - 2 Repeatable but Intuitive
  - 3 Defined Process
  - 4 Managed and Measurable
  - 5 Optimised

0 Non-existent when

- There is a complete lack of any recognisable IT governance process.
- The organisation has not even recognised that there is an issue to be addressed;
  - hence, there is no communication about the issue.

1 Initial/ Ad Hoc when

- There is recognition that IT governance issues exist and need to be addressed.
- There are ad hoc approaches applied on an individual or case-by-case basis.
- Management's approach is reactive and there is only sporadic, inconsistent communication on issues and approaches to address them.
- Management has only an approximate indication of how IT contributes to business performance.
- Management only reactively responds to an incident that has caused some loss or embarrassment to the organisation.

2 Repeatable but Intuitive when

- There is awareness of IT governance issues.
- IT governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development.
- Selected IT processes are identified for improvement based on individuals' decisions.
- Management has identified basic IT governance measurements and assessment methods and techniques; however, the process has not been adopted across the organisation.
- Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance processes within various IT projects and processes.
- The processes, tools and metrics to measure IT governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined Process when

- The importance of and need for IT governance are understood by management and communicated to the organisation.
- A baseline set of IT governance indicators is developed where linkages between outcome measures and performance drivers are defined and documented.
- Procedures have been standardised and documented.
- Management has communicated standardised procedures and training is established.
- Tools have been identified to assist with overseeing IT governance.
- Processes may be monitored, but deviations, while mostly being acted upon by individual initiative, would unlikely be detected by management.

4 Managed and Measurable when

- There is full understanding of IT governance issues at all levels.
- There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements.
- Responsibilities are clear and process ownership is established.
- IT processes and IT governance are aligned with and integrated into the business and the IT strategy.
- Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics.

4 Managed and Measurable when

- All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer.
- Management has defined tolerances under which processes must operate. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools.
- IT governance has been integrated into strategic and operational planning and monitoring processes.
- Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprisewide improvements.
- Overall accountability of key process performance is clear and management is rewarded based on key performance measures.

5 Optimised when

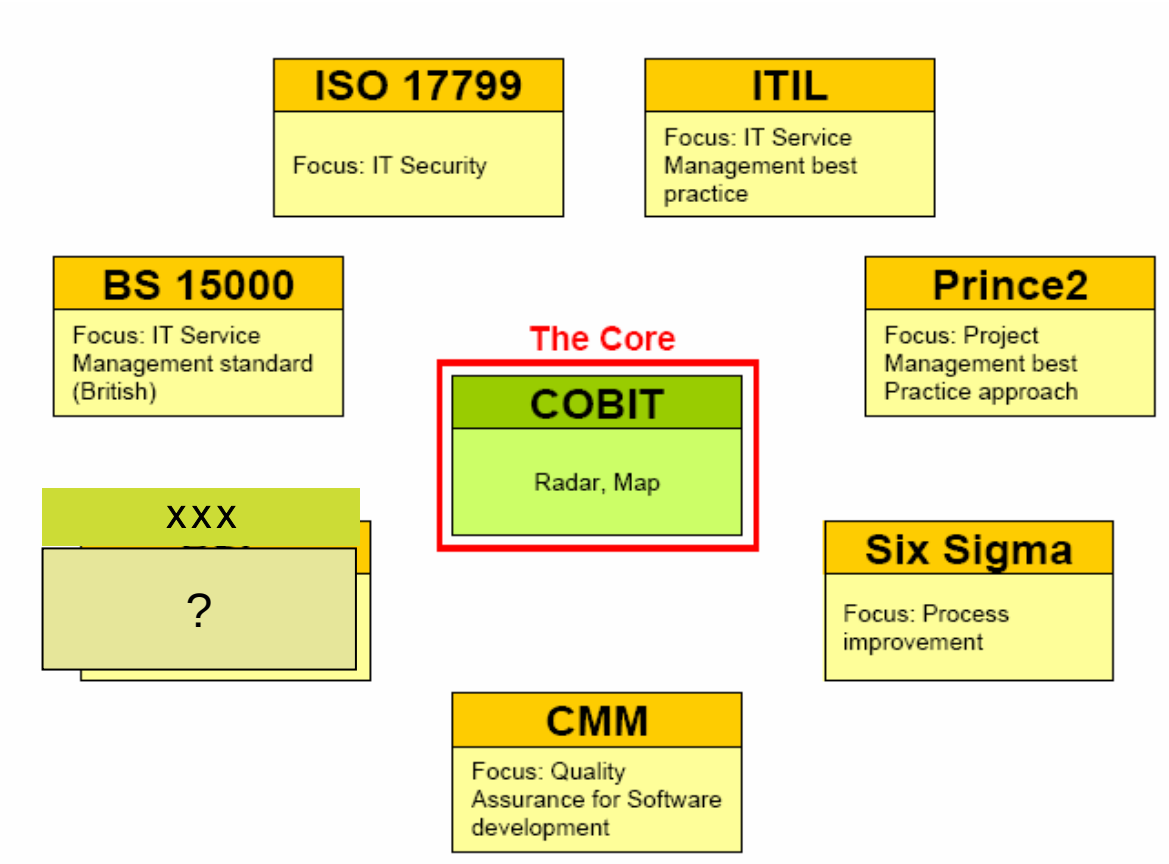
- There is advanced and forward-looking understanding of IT governance issues and solutions.
- Training and communication are supported by leading-edge concepts and techniques.
- Processes have been refined to a level of industry best practice, based on results of continuous improvement and maturity modelling with other organisations.
- The implementation of IT policies has led to an organisation, people and processes that are quick to adapt and fully support IT governance requirements.
- All problems and deviations are root cause analysed and efficient action is expediently identified and initiated.

5 Optimised when

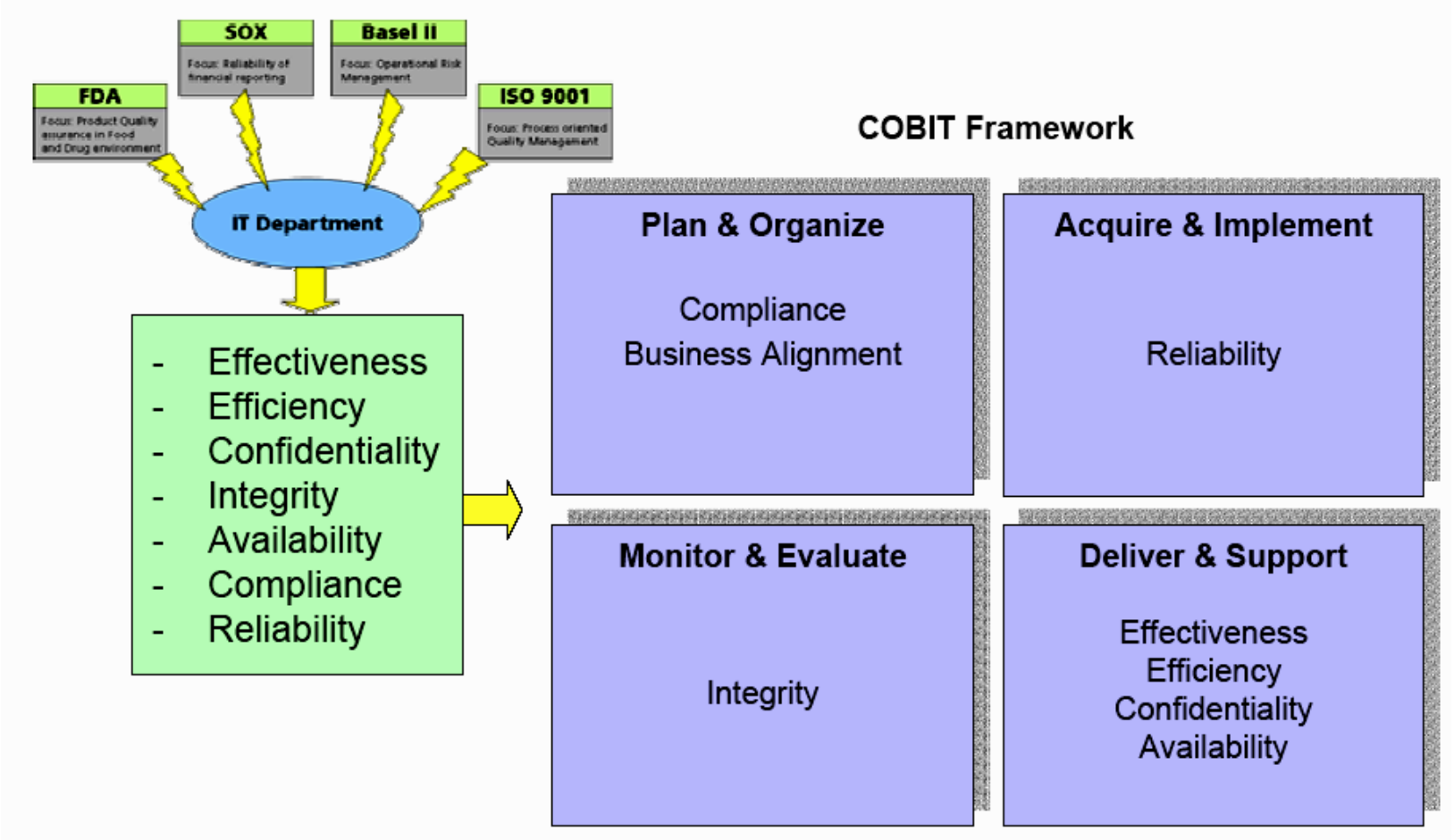
- IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness.
- The risks and returns of the IT processes are defined, balanced and communicated across the enterprise.
- External experts are leveraged and benchmarks are used for guidance.
- Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training.
- Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise. IT governance activities are integrated with the enterprise governance process.

COBIT Related Standards

COBIT Related Standards



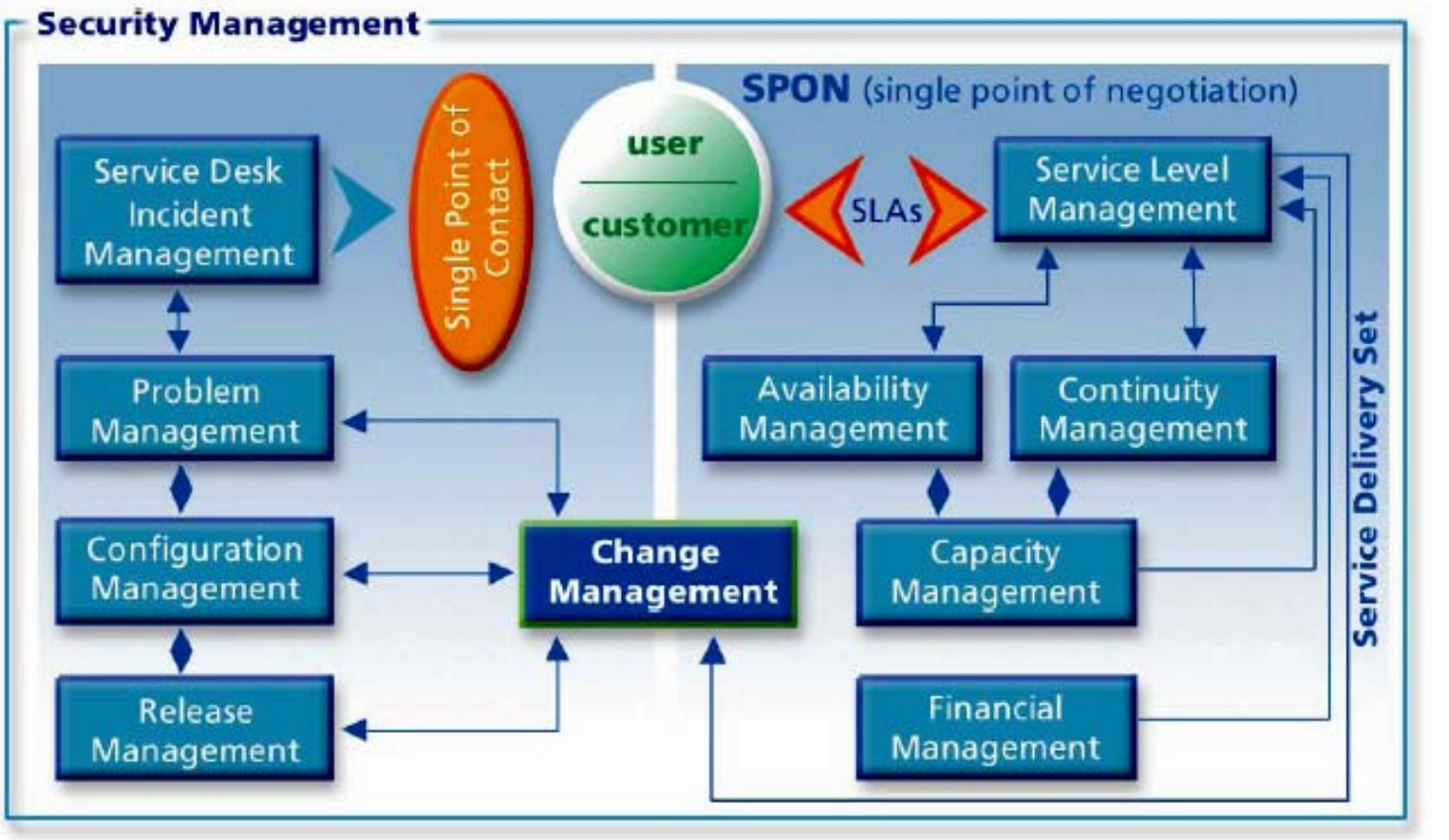
Regulations for the IT Department



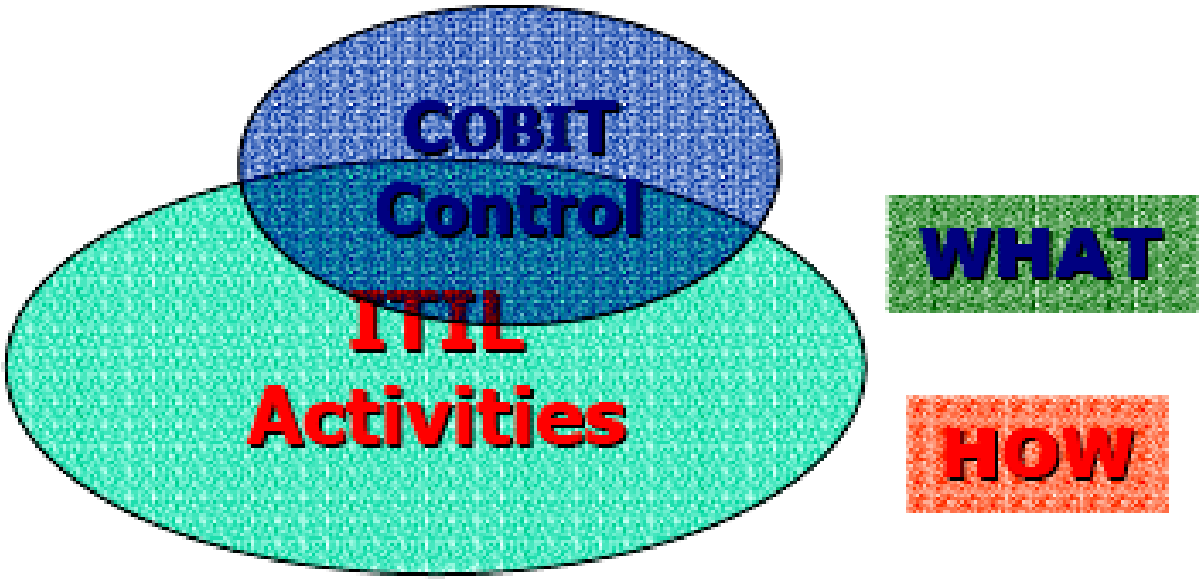
ITIL

- ITIL – The IT Infrastructure Library is a collection of best practices in IT service management. It is focused on the service processes of the IT and considers the central role of the user.

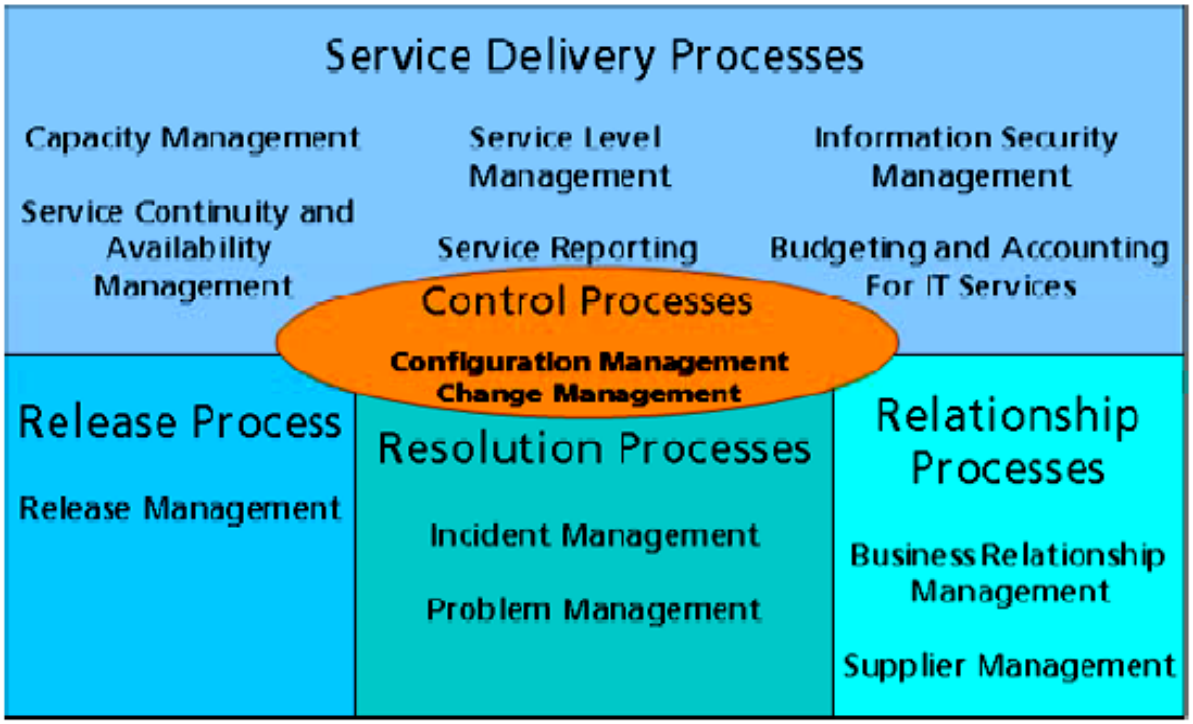
ITIL Framework



COBIT and other Standards / Positioning

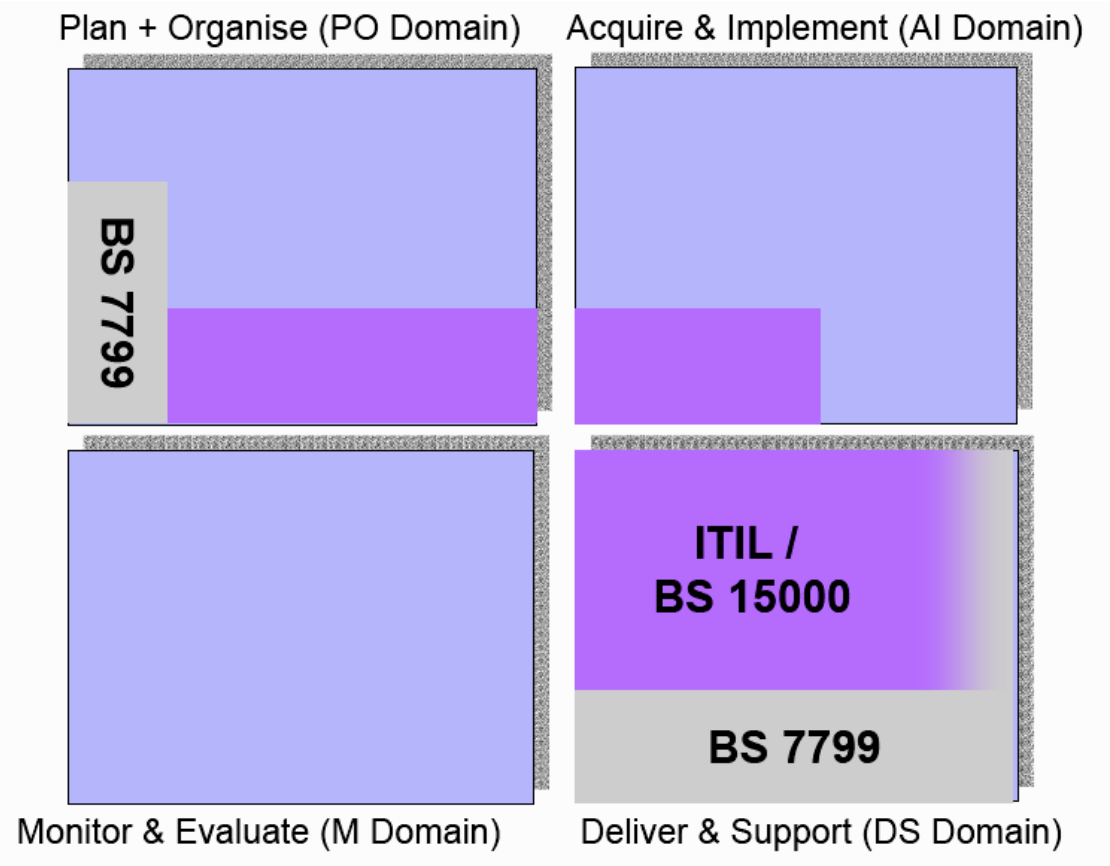


BS 15000 Framework



- Almost 100% ITIL
- Organizations can be certified (British Standard)

Example: ITIL / BS 15000 / BS 7799



ISO/IEC 17799:2000

- ISO/IEC 17799:2000 – The Code of Practice for Information Security Management is an international standard, based on BS 7799-1. It is presented as best practice for implementing information security management.

ISO/IEC TR 13335

- ISO/IEC TR 13335 – The technical report Guidelines for the Management of IT Security contains information on IT security management not only from the planning perspective, but also from the implementation and maintenance perspectives.

ISO/IEC 15408

- ISO/IEC 15408 – Security Techniques—Evaluation Criteria for IT Security is used as a reference to evaluate and certify the security of IT products and services.

Example: SOX

SOX requires management to:

- Certify the financial statements and internal control over financial reporting in periodic reports filed with the SEC (=S 302)
- Annually assess and report on internal controls.

SOX requires auditors to:

- Provide an attestation report on management's annual assessment (=S 404).

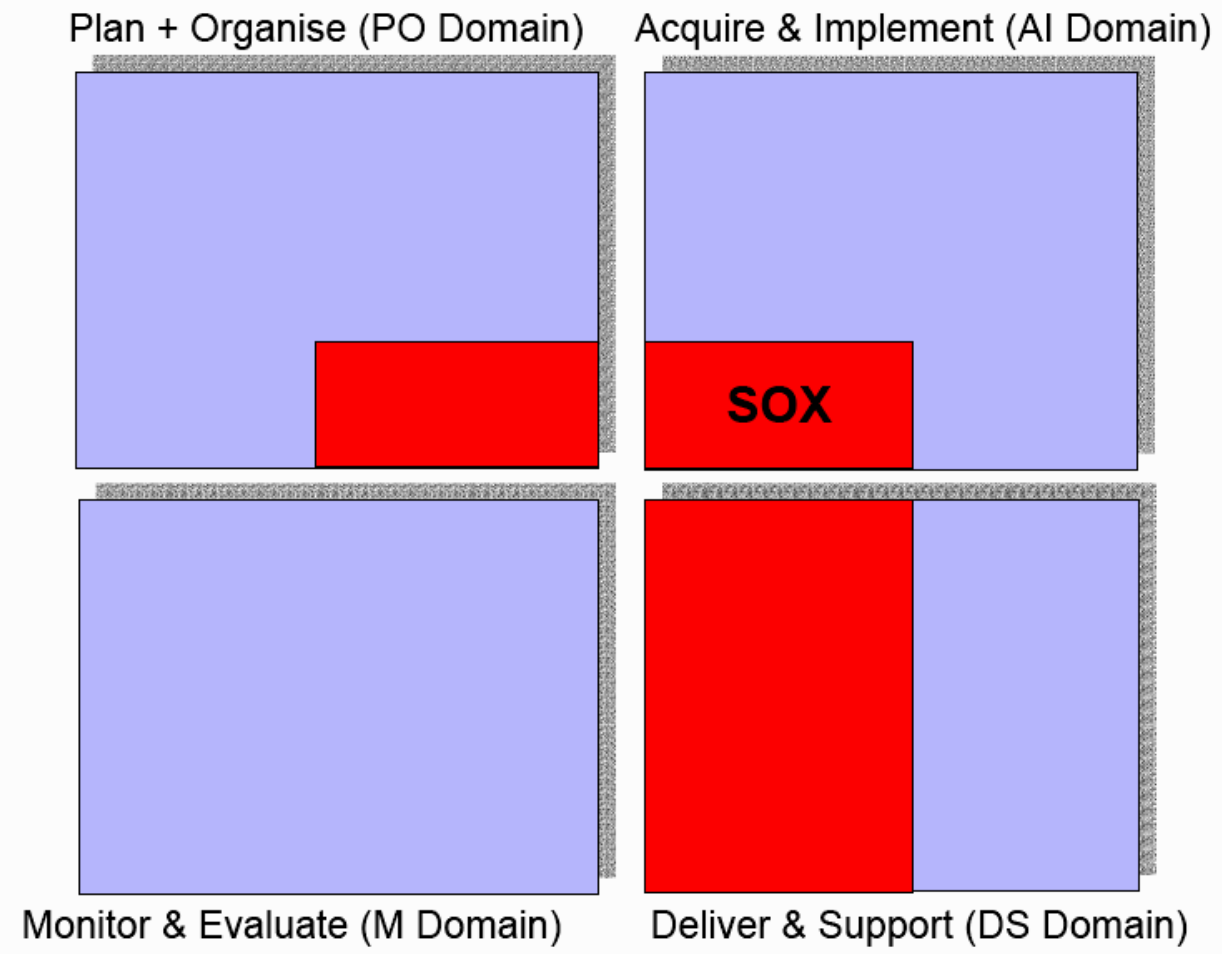
IT relevant Sections

- **S 302:** Corporate Responsibility For Financial Reports
- **S 404:** Management Assessment Of Internal Controls
- **S 409:** Real Time Disclosure

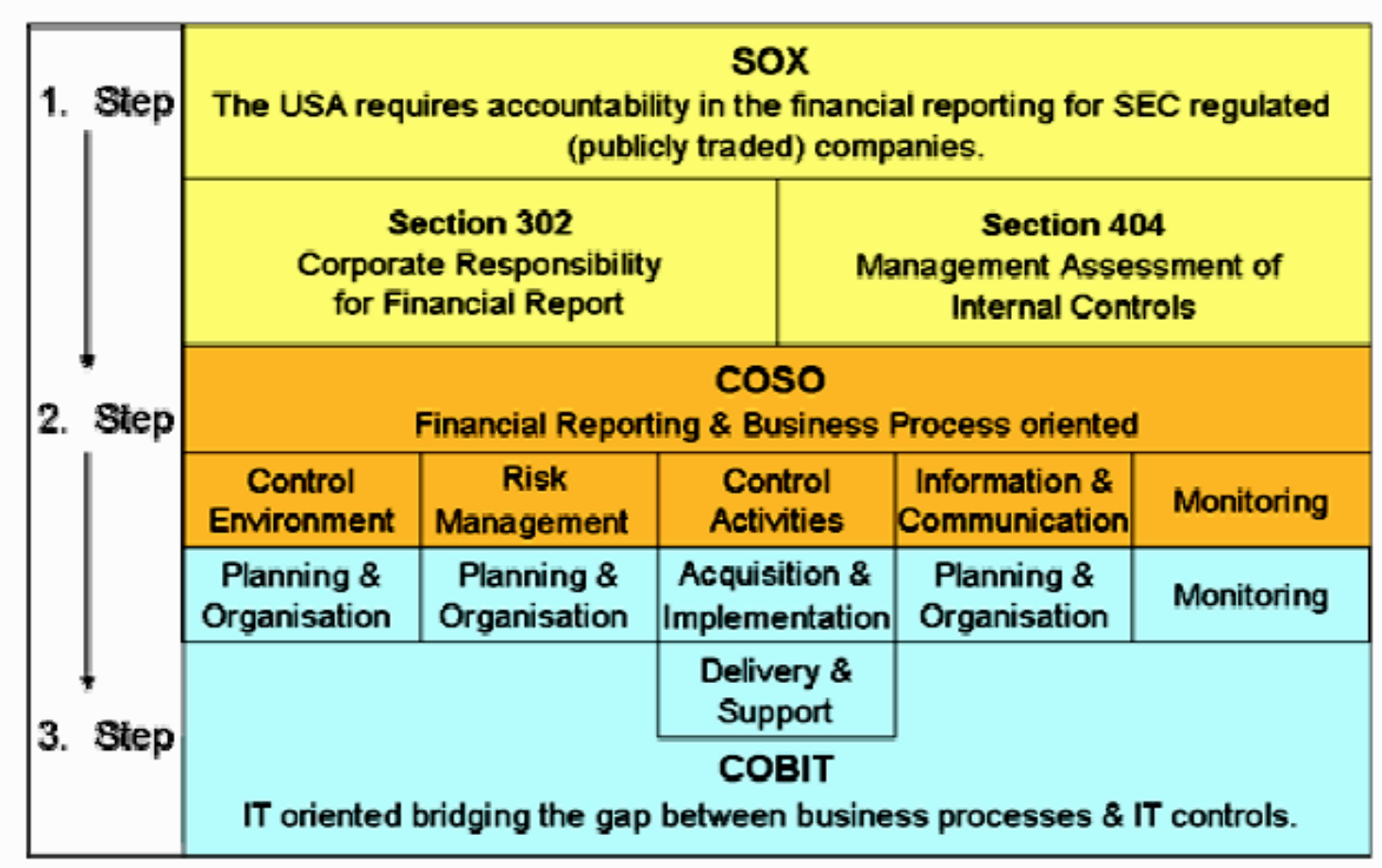
Generally relevant Sections

- **S 101:** Establishment, Board Membership & Duties Of The Board
- **S 103:** Auditing, Quality Control, Independence Standards & Rules
- **S 106:** Foreign Public Accounting Firms
- **S 401:** Disclosures In Periodic Reports & Study and Report on Special Purpose Entities
- .....

Example: SOX


Plan + Organise (PO Domain)
Acquire & Implement (AI Domain)
SOX
Monitor & Evaluate (M Domain)
Deliver & Support (DS Domain)

Example: SOX compliance



TickIT

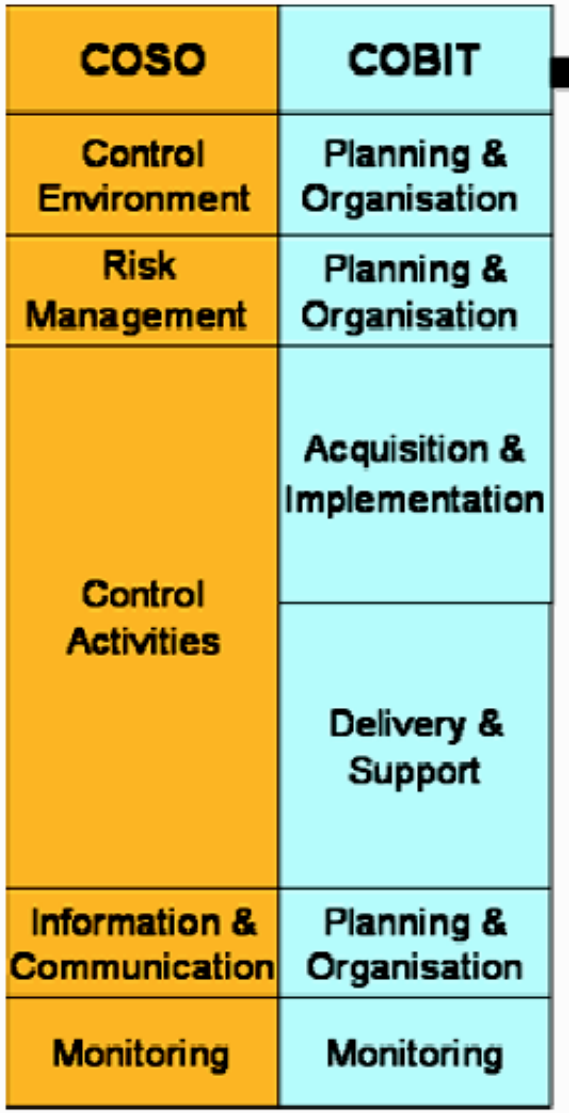
- TickIT – TickIT provides a scheme for the certification of the software quality management system.It intends to improve the effectiveness of the quality management system and targets customers, suppliers and assurance professionals.

NIST 800-14

- NIST 800-14 – The special publication Generally Accepted Principles and Practices for Securing Information Technology Systems contains information for establishing a comprehensive IT security program.

COSO
(Committee of Sponsoring Organisations of the Treadway Commission)

- COSO Integrated Framework defines a framework that initiates an integrated process of internal control.

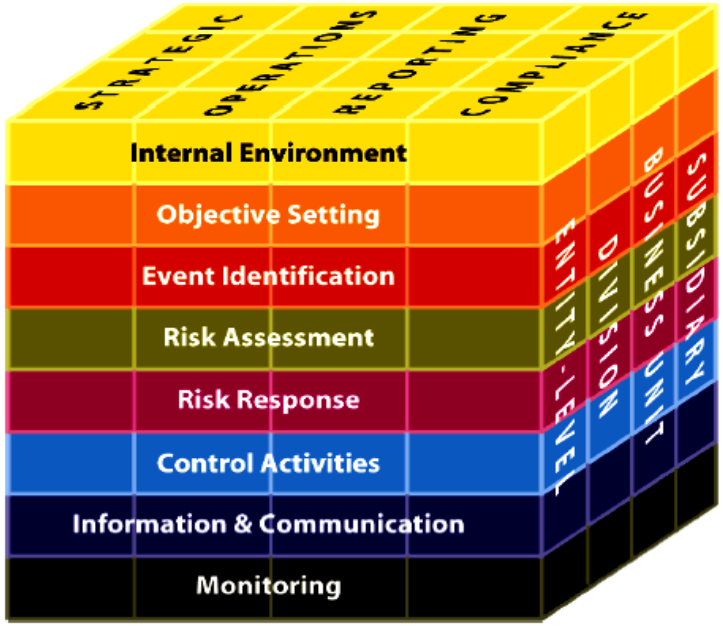


Relationship of Objectives and Components

- There is a direct relationship between **objectives**, which are what an entity strives to achieve, and the enterprise **risk management components**, which represent what is needed to achieve them.
- The four **objectives categories** –
  - strategic,
  - operations,
  - reporting and
  - compliance –

are represented by the vertical columns.

- The eight components are represented by horizontal rows.
- The entity and its organizational units are depicted by the third dimension of the matrix.



COSO cube

COBIT as Radar Map

CobiT is the Framework (Radar, Map) that:

- Helps you to map business requirements and standards to IT organisation (e.g. SOX, Basel II, FDA etc.)
- Allows to assess an IT organisation based on a international accepted standard

But!

It does not provide concrete information on the how-to:

- ITIL
- BS15000
- BS7799 / ISO17799
- Prince2
- …