

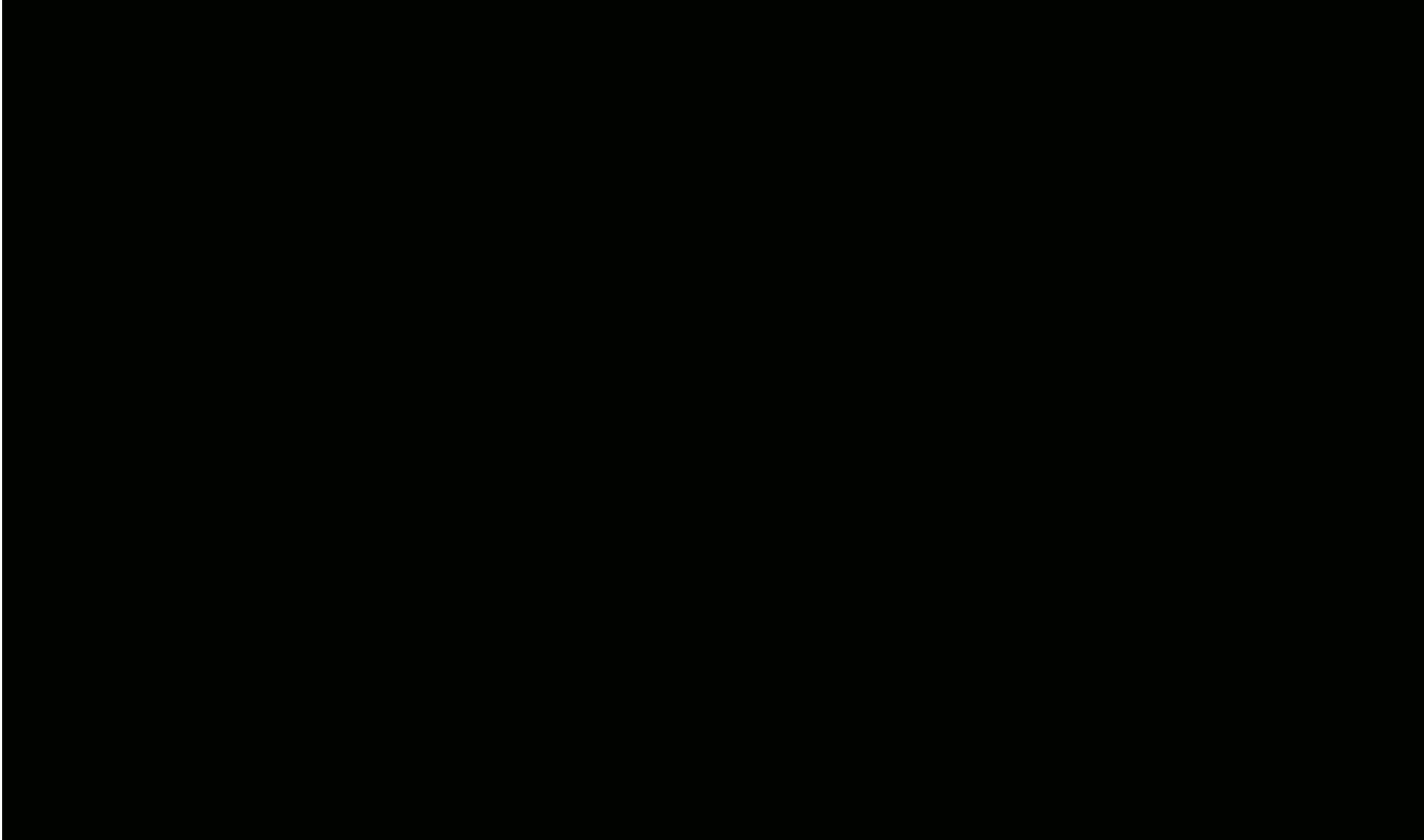


# COBIT as an IT Governance Mechanism

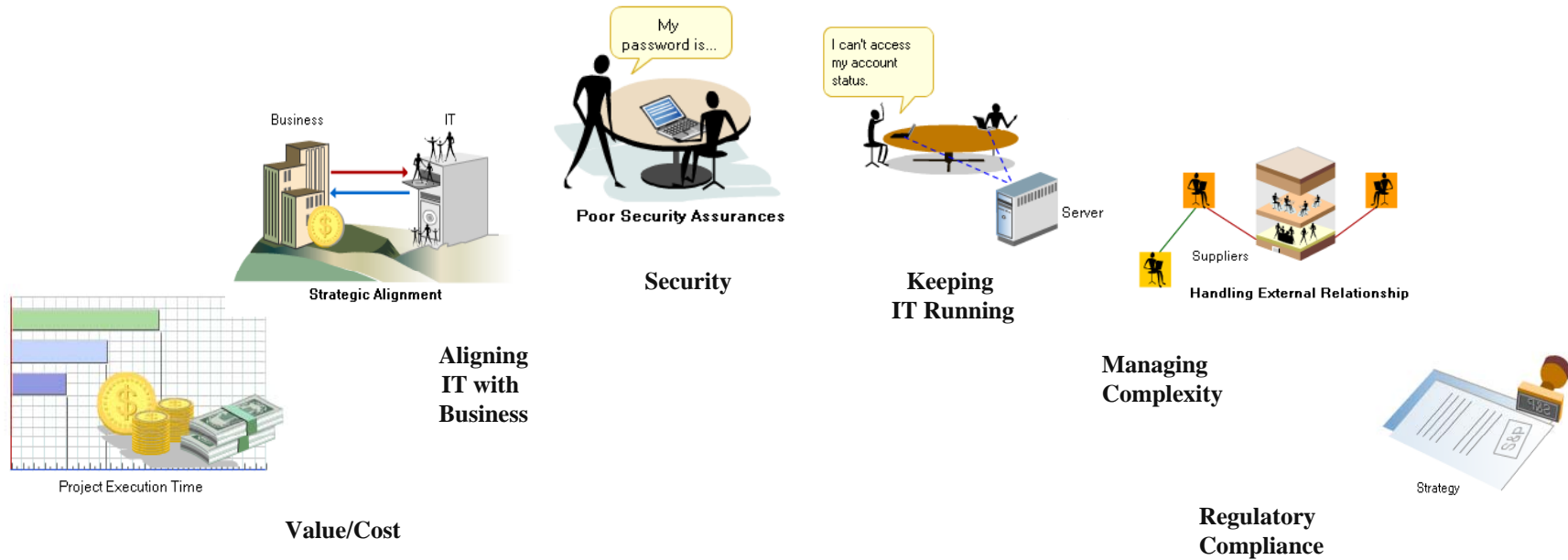
By: Kris SEEBURN

*Member ISACA Academic Relations Committee  
Chair EMEA Academic Relations Committee  
Chair – ISACA Mauritius Chapter in Formation  
President ISGMU*

*Lecturer / Programme Director MSc Computer Security & Forensics - University of Technology, Mauritius*

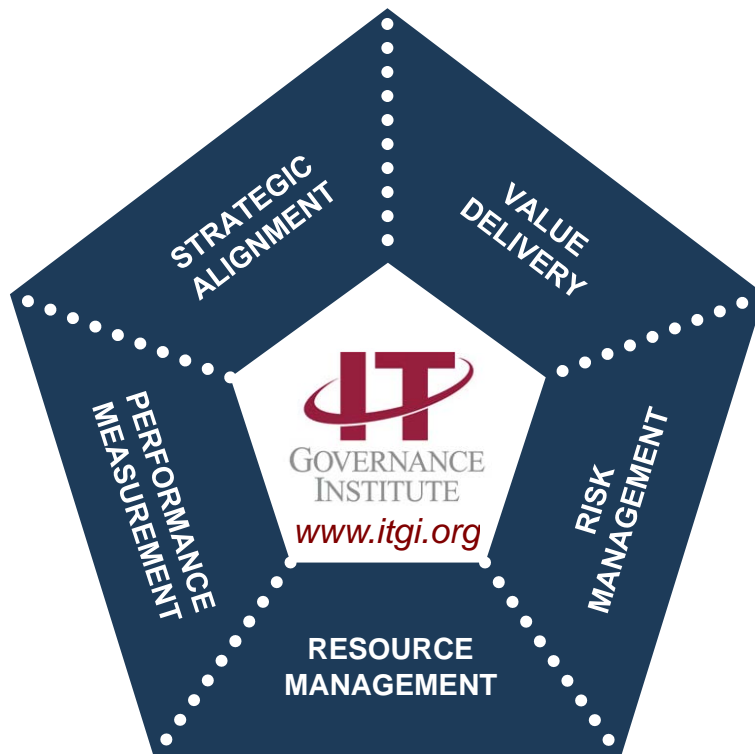


# The Need for IT Governance



**Organisations require a structured approach for managing these and other challenges.**

**This will ensure that there are agreed objectives for IT, good management controls in place and effective monitoring of performance to keep on track and avoid unexpected outcomes.**



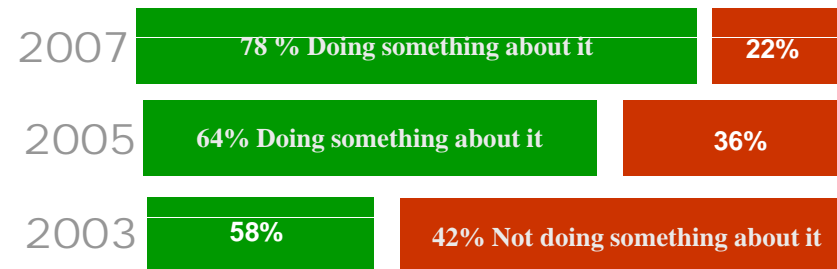
**Enterprise governance** is a set of responsibilities and practices exercised by the board and executive management with the goal of:

- Providing **strategic direction**
- Ensuring that **objectives** are achieved
- Ascertaining that **risks** are managed appropriately
- Verifying that the **enterprise's resources** are used responsibly



## IT governance is:

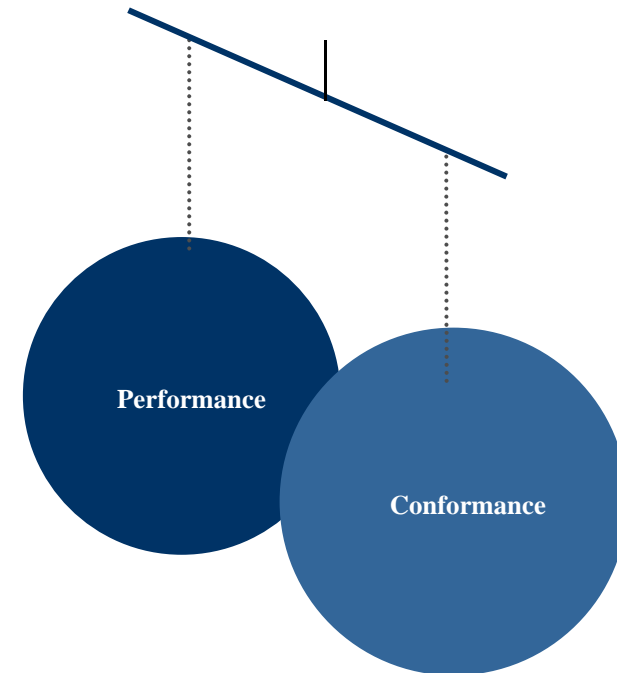
- The responsibility of the board of directors and executive management
- An **integral part** of enterprise governance, consisting of the leadership, organisational structures and processes that ensure that the **enterprise’s IT sustains and extends the organisation’s strategies and objectives**



Source: Surveys by PwC for the IT Governance Institute Sep-Oct 2003 and Sep-Oct 2005 and Sep-Oct 2007

## Enterprise governance is about:

- ⦿ **Conformance**
  - Adhering to legislation, internal policies, audit requirements, etc.
- ⦿ **Performance**
  - Improving profitability, efficiency, effectiveness, growth, etc.



**Enterprise governance and IT governance require a balance between conformance and performance goals directed by the board.**

## 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** in 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**

To make an IT governance implementation project successful:

- ⦿ Make IT governance a workable solution—able to deal with the challenges and pitfalls presented by IT.
- ⦿ Focus as much on improving performance and enabling competitive advantage as preventing problems.
- ⦿ Make IT governance a shared responsibility between the business (customer) and the IT service provider, with the **full commitment and direction of the board**.
- ⦿ Align IT governance within a wider enterprise governance scheme.
- ⦿ Boards and executive management need to extend enterprise governance to include IT, provide the necessary leadership and organisational structures, and insist on well-managed and properly controlled processes.

**COBIT helps bridge the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure.**

## **COBIT:**

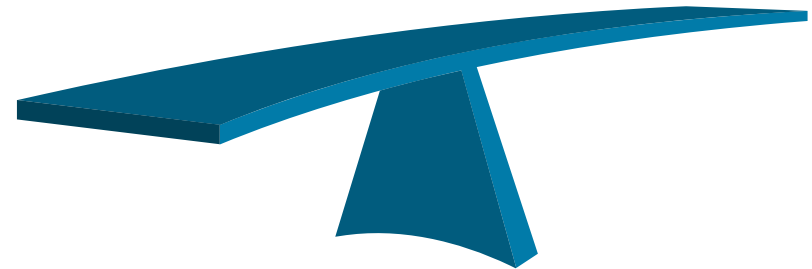
- ⦿ Starts from business requirements
- ⦿ Is process-oriented, organising IT activities into a generally accepted process model
- ⦿ Identifies the major IT resources to be leveraged
- ⦿ Defines the management control objectives to be considered
- ⦿ Incorporates major international standards
- ⦿ Has become the *de facto* standard for overall control of IT



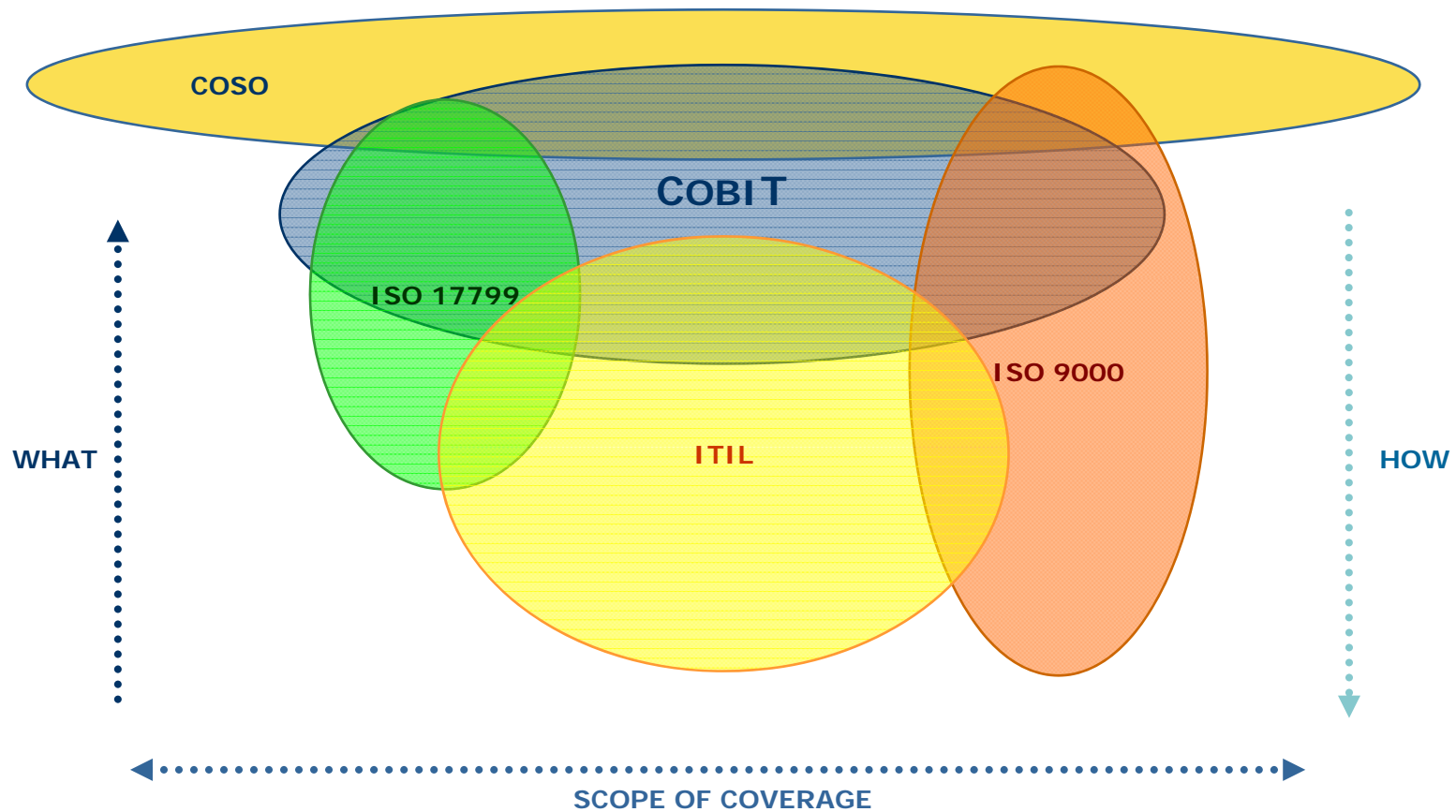
**IT resources need to be managed by a set of naturally grouped processes. COBIT provides a framework that achieves this objective.**

COBIT brings the following advantages to an IT governance implementation effort:

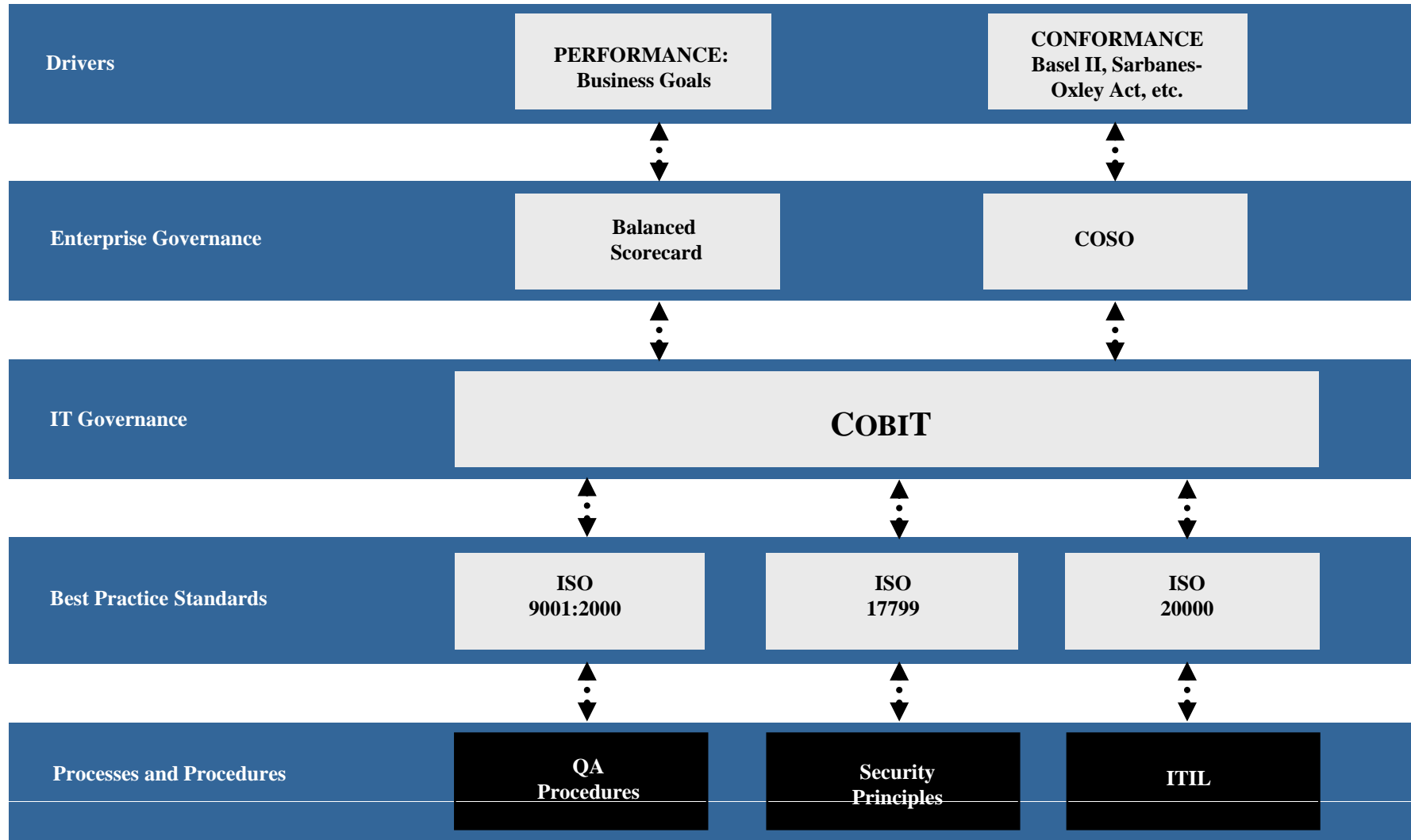
- ⦿ Enables mapping of IT goals to business goals and *vice versa*
- ⦿ Better alignment, based on a business focus
- ⦿ A view of what IT does that is understandable to management
- ⦿ Clear ownership and responsibilities based on process orientation
- ⦿ General acceptability with third parties and regulators
- ⦿ Shared understanding amongst all stakeholders, based on a common language
- ⦿ Fulfilment of the COSO requirements for the IT control environment

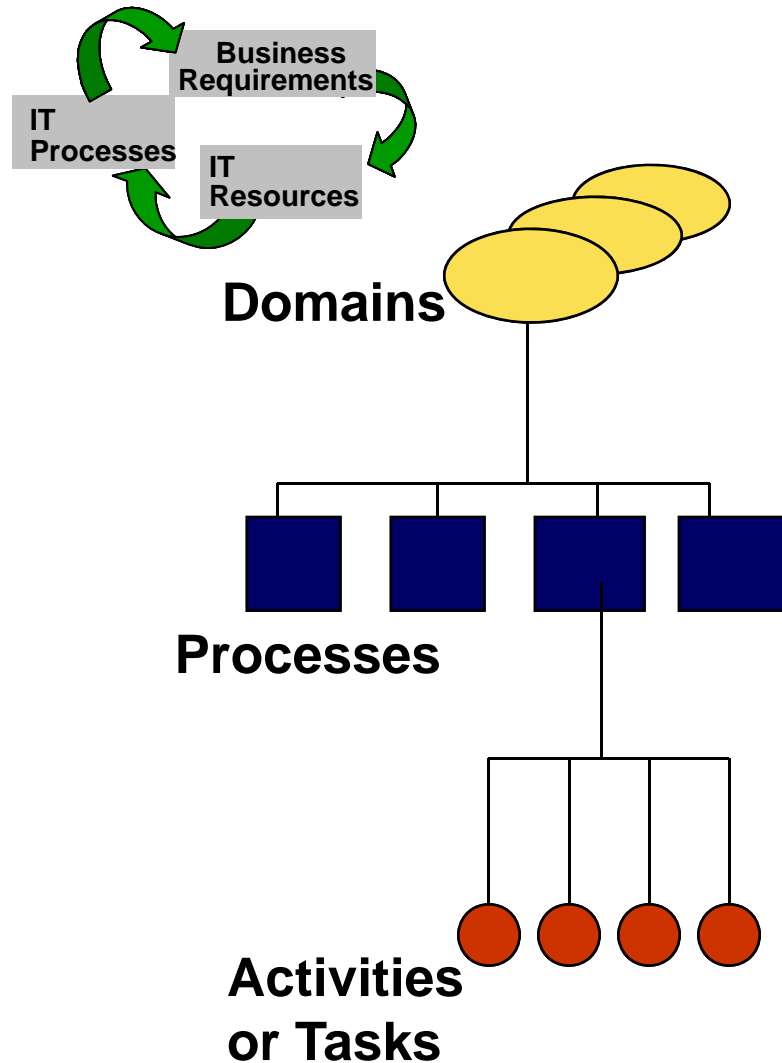


Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with COBIT acting as the consolidator ('umbrella').



# Where Does COBIT Fit?





**Natural grouping of processes, often matching an organisational domain of responsibility**

**A series of joined activities with natural control breaks**

**Actions needed to achieve a measurable result—activities have a life cycle, whereas tasks are discrete**

## IT Domains

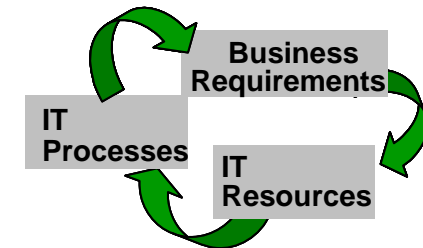
- Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Natural grouping of processes, often matching an organisational domain of responsibility

## IT Processes

- IT strategy
- Computer operations
- Incident handling
- Acceptance testing
- Change management
- Contingency planning
- Problem management

A series of joined activities with natural (control) breaks



## Activities

- Record new problem.
- Analyse.
- Propose solution.
- Monitor solution.
- Record known problem.
- Etc. ...

Actions needed to achieve a measurable result—activities have a life cycle, whereas tasks are discrete

- Description

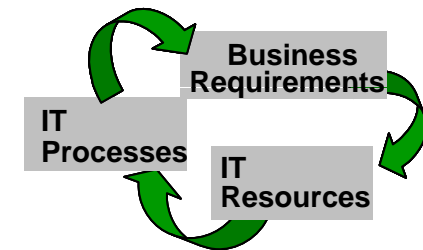
- This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Proper organisation and technological infrastructure must be put in place.

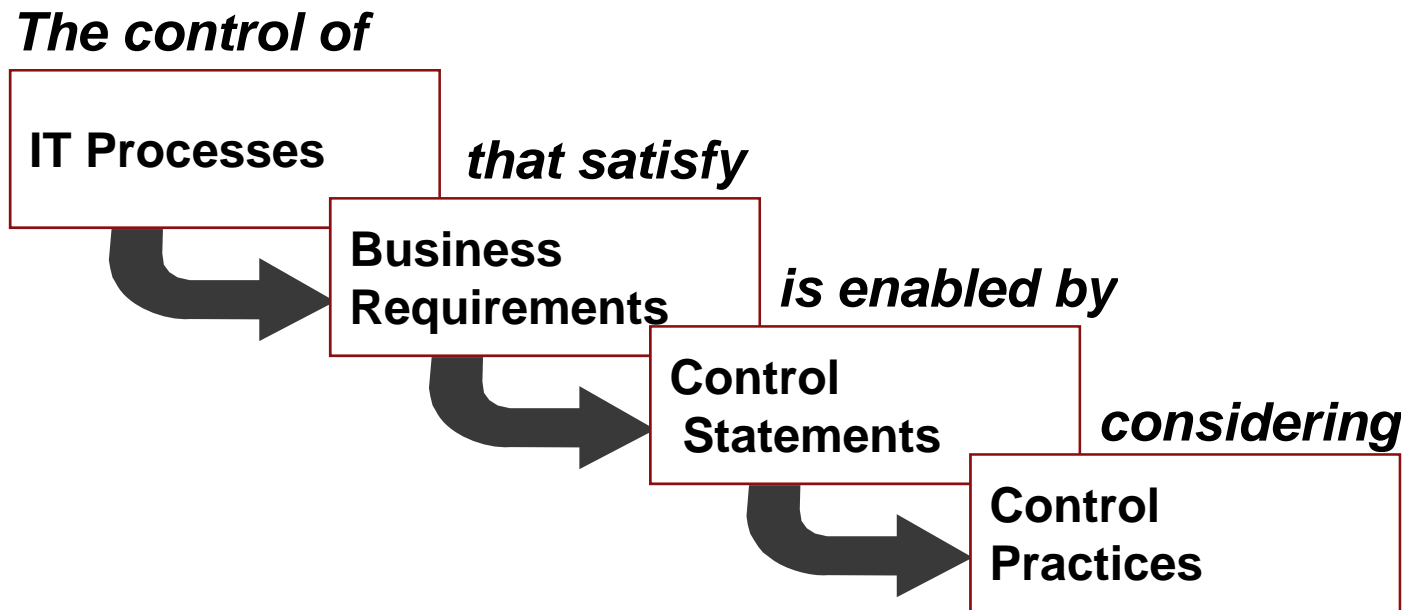
#### Topics

- Strategy and tactics
- Vision planned
- Organisation and infrastructure

- Questions

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?





**4 Domains - 34 Processes - 210 Control Objectives**

## Business Objectives

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

## IT Resources

- Data
- Application systems
- Technology
- Facilities
- People

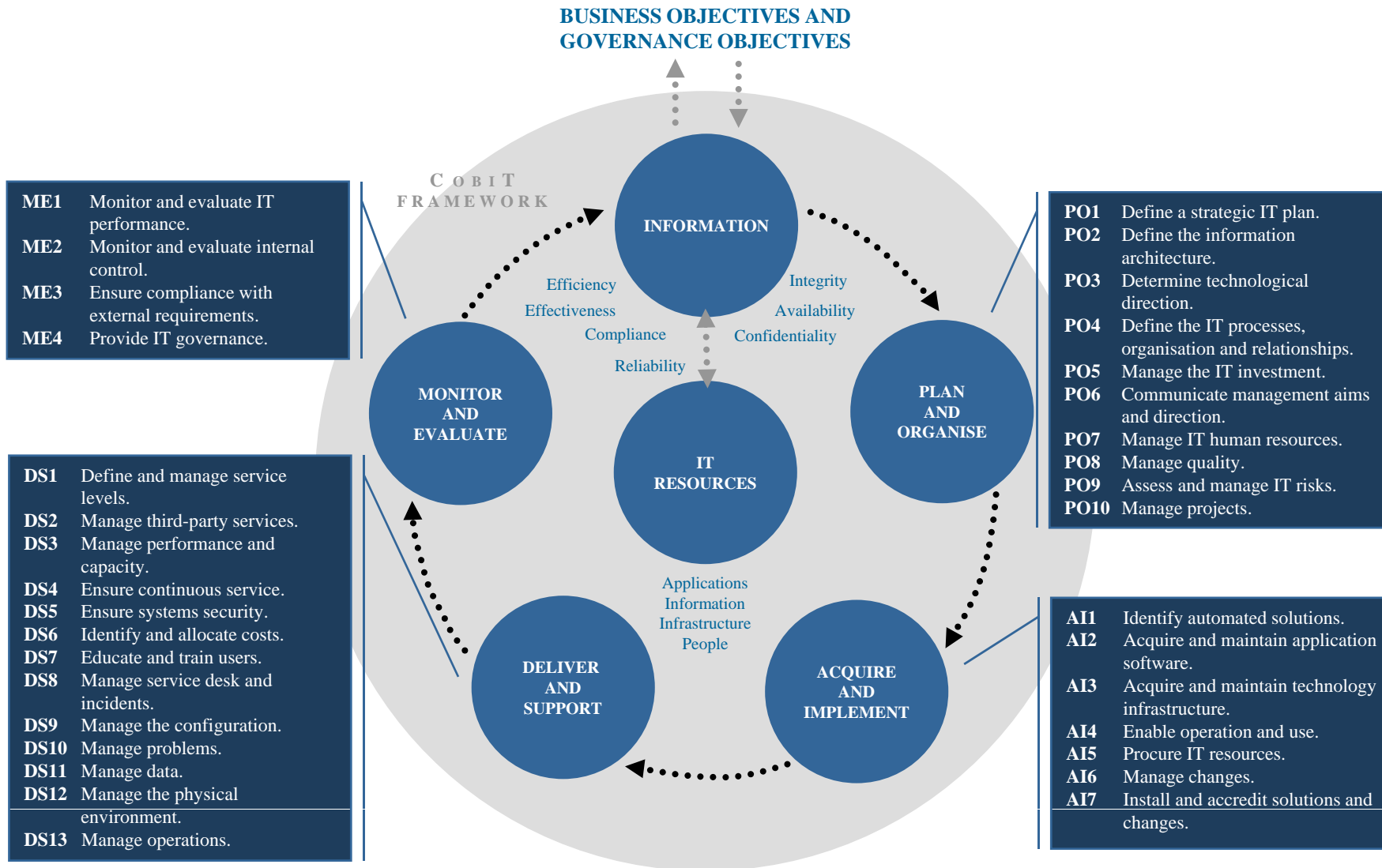
Monitor and Evaluate

Plan and Organise

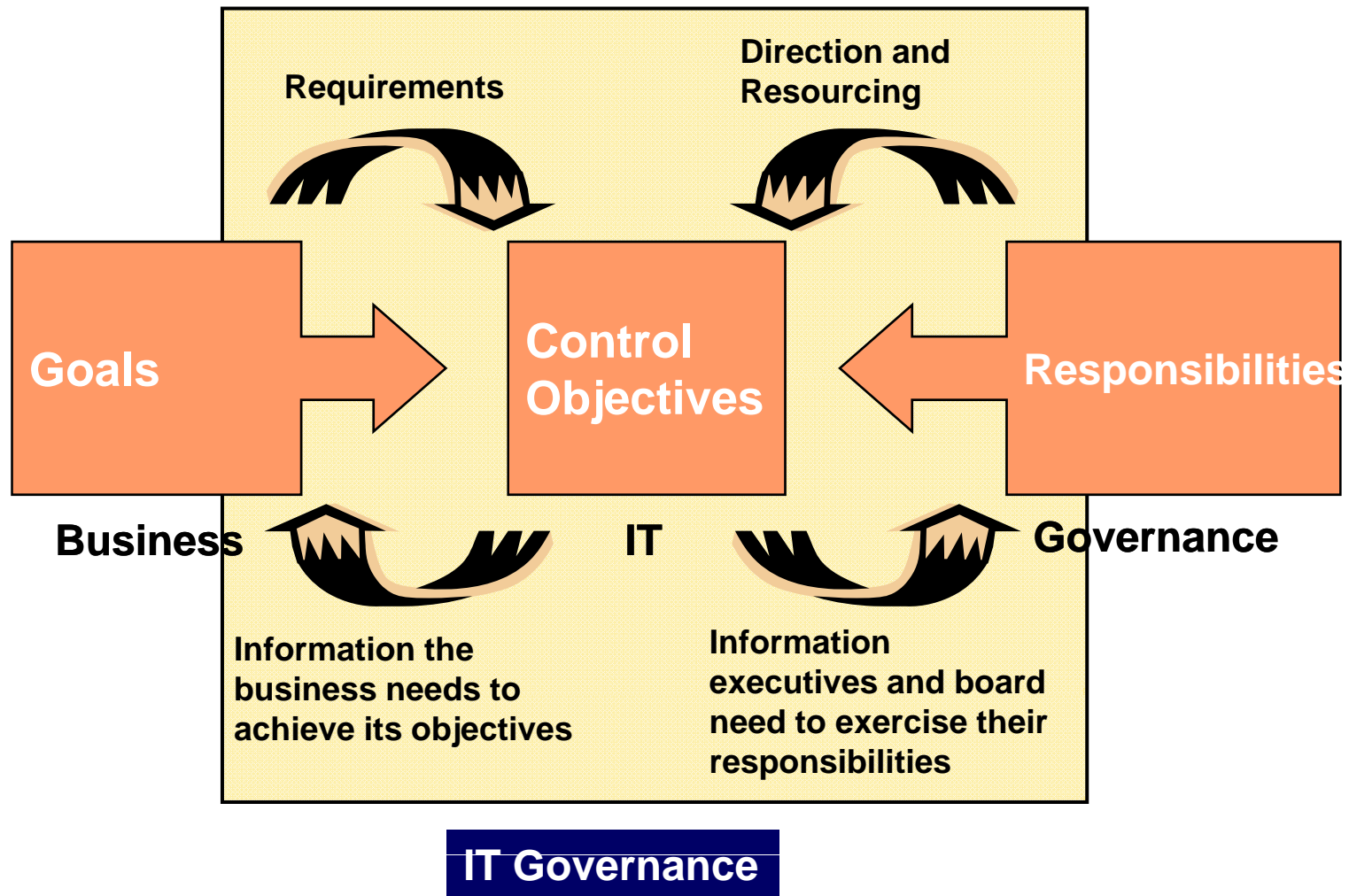
Deliver and Support

Acquire and Implement

IT Life Cycle

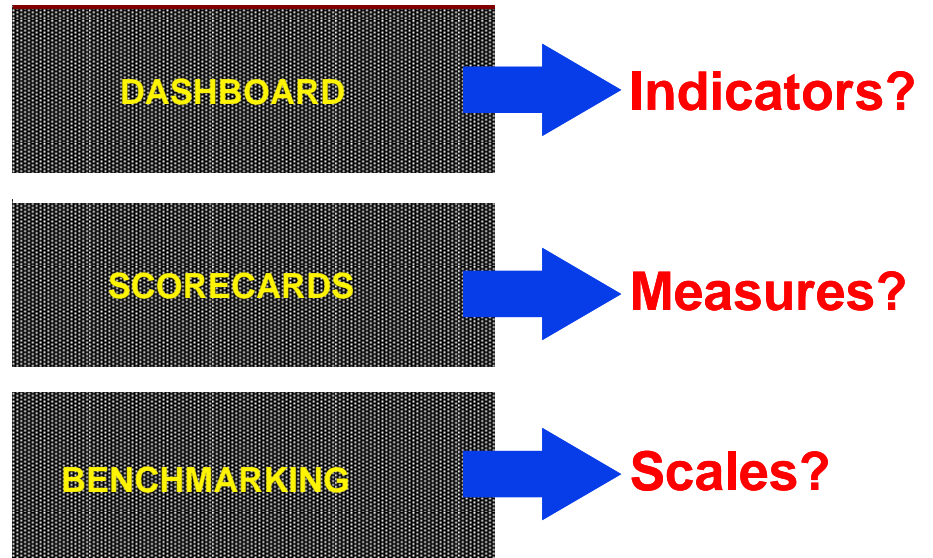


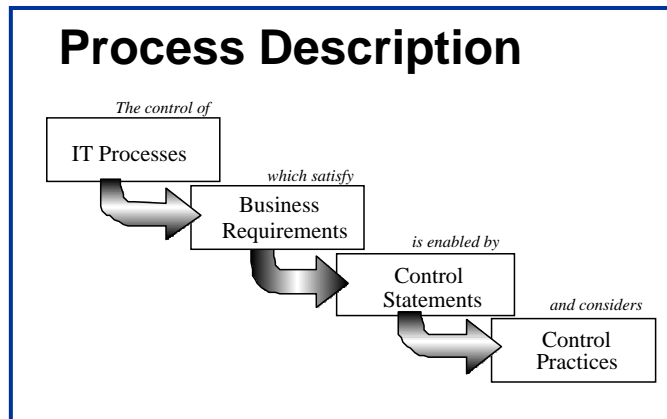
# How Does COBIT Link to IT Governance?



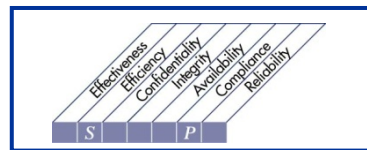
## However, management has questions that go beyond a control framework:

- How do responsible managers "keep the ship on course"?
- How to achieve results that are satisfactory for the largest possible segment of our stakeholders ?
- How to adapt the organisation in a timely manner to trends and developments in the enterprise's environment ?

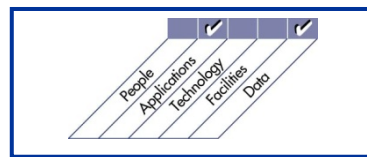




- ### Critical Success Factors
- - 
  - 
  - 
  - 
  -



Information Criteria



Resources

- ### Key Goal Indicators
- - 
  -

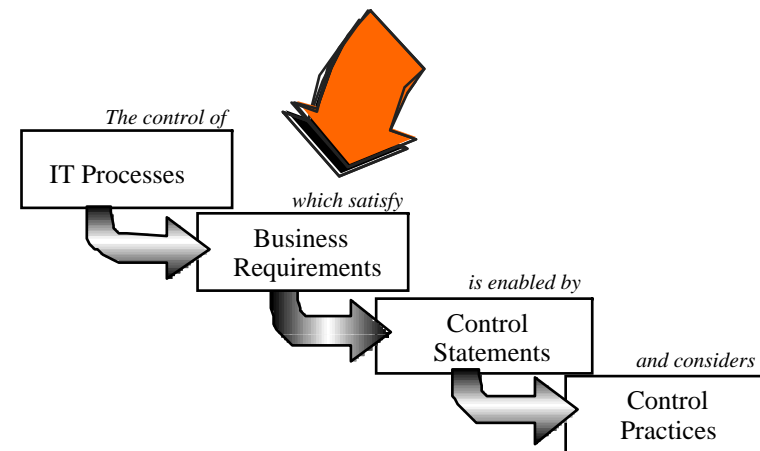
- ### Key Performance Indicators
- -

### Maturity Model

- 0 - Management processes are not applied at all.
- 1 - Processes are *ad hoc* and disorganised.
- 2 - Processes follow a regular pattern.
- 3 - Processes are documented and communicated.
- 4 - Processes are monitored and measured.
- 5 - Best practices are followed and automated.

## Definitions

- Describe the outcome of the process (i.e., measurable after the fact); are measures of “what,” and may describe the impact of not reaching the process goal
- Are indicators of the success of the process and its business contribution
- Focus on the customer and financial dimensions of the balanced scorecard

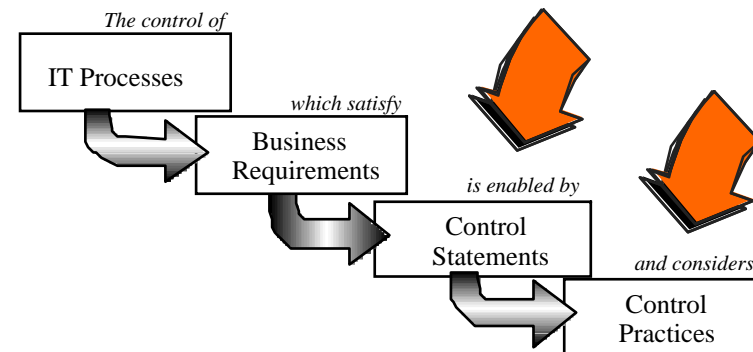


## Examples

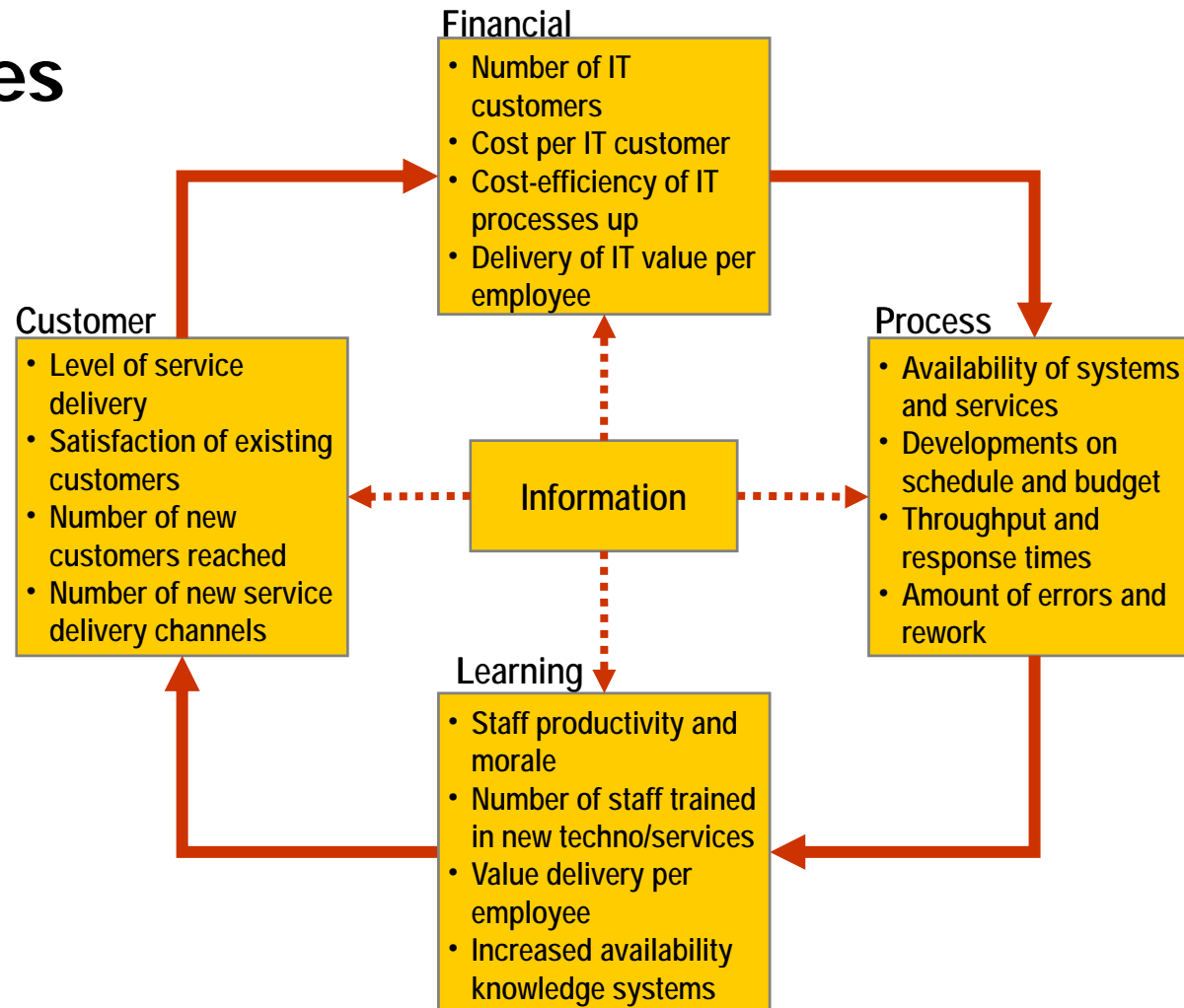
- **Increased level of service delivery**
- **Number of customers and cost per customer served**
- **Availability of systems and services**
- **Absence of integrity and confidentiality risks**
- **Cost-efficiency of processes and operations**
- **Confirmation of reliability and effectiveness**
- **Adherence to development cost and schedule**
- **Cost-efficiency of the process**
- **Staff productivity and morale**
- **Number of timely changes to processes and systems**
- **Improved productivity (e.g., delivery of value per employee)**

## Definitions

- Are measures of “how well” the process is performing
- Predict the probability of success or failure
- Focus on the process and learning dimensions of the balanced scorecard
- Are expressed in precise, measurable terms
- Should help in improving the IT process

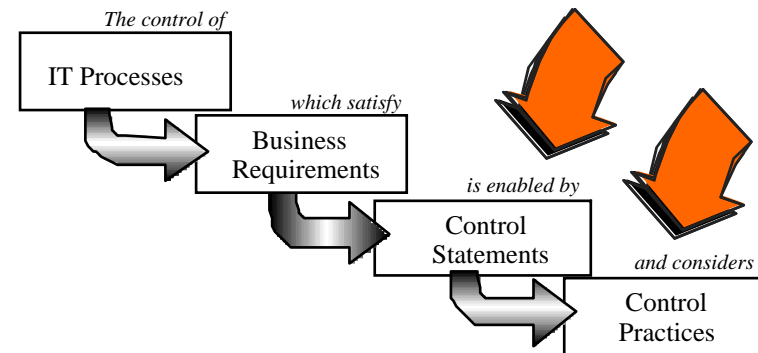


## Examples



## Definitions

- Are the most important things to do to increase the probability of success of the process
- Are observable—usually measurable—characteristics of the organisation and process
- Focus on obtaining, maintaining and leveraging capability, skills and behaviour



## Examples

### Strategy

- The IT strategic plan clearly states a risk position such as leading-edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality.

### Policy

- If you are not ready to enforce the policy, do not issue the policy.

### Compliance

- A building permit programme for building IT systems and a “driver’s licence” programme for those doing the building

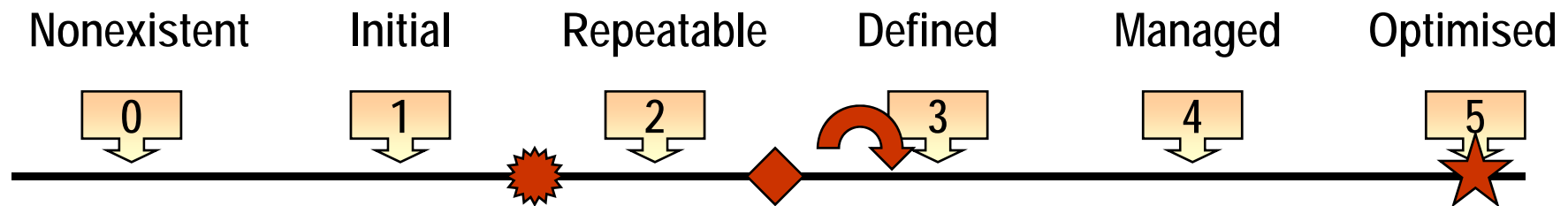
### Security

- A good security plan takes time to evolve.

## Definitions

- Refer to business requirements (KGIs) and the enabling aspects (KPIs) at the different levels
- Are a scale that lend themselves to pragmatic comparison, where the difference can be made measurable in an easy manner
- Are recognisable as a profile of the enterprise in relation to IT governance and control
- Assist in determining as-is and to-be positions relative to IT governance and control maturity and analyse the gap
- Are not industry-specific nor generally applicable. The nature of the business determines what is an appropriate level.

## Usage



### Legend for Symbols Used

- Enterprise current status
- International standard guidelines
- Industry best practice
- Enterprise strategy

### Legend for Rankings Used

- 0 - Management processes are not applied at all.
- 1 - Processes are *ad hoc* and disorganised.
- 2 - Processes follow a regular pattern.
- 3 - Processes are documented and communicated.
- 4 - Processes are monitored and measured.
- 5 - Best practices are followed and automated.

*"The complexity and difficulty of explaining IT governance is one of the most serious barriers to increasing the value derived from IT"*

*Weill and Broadbent 2002.*

- *The implementation is not easy and requires work.*
- *COBIT is aimed at providing a framework for governance implementation.*

Where were the auditors?...

*Contact : Kris Seeburn*

*Email : kris\_seeburn@utm.intnet.mu*

