

# Computer Center Management

- IT Standards & Frameworks

# Best Practices

## Quality & Control Models

- ISO 900x
- ISO 2000
- COBIT
- TQM
- EFQM
- Six Sigma
- COSO
- Deming
- etc..

## Process Frameworks

- IT Infrastructure Library
- Application Service Library
- Gartner CSD
- IBM Processes
- EDS Digital Workflow
- Microsoft MOF
- Telecom Ops Map
- etc..

- What is not **defined** cannot be **controlled**
- What is not **controlled** cannot be **measured**
- What is not **measured** cannot be **improved**
  - Define -- Improve
  - Measure -- Control And Stabilize

# ISO 900x

- A set of international standards on quality management and quality assurance developed to help companies effectively document the quality system elements to be implemented to maintain an efficient quality system.
  - ISO 9000 deals with the fundamentals of quality management systems
  - ISO 9001 deals with the requirements that organizations wishing to meet the standard must fulfill.

# ISO 2000

- **ISO 2000** is a set of standards relating to quality management systems designed to assist organizations while ensuring the needs of customers and other stakeholders.

# TQM

- **Total Quality Management (TQM)** is a comprehensive and structured approach to organizational management that seeks to improve the quality of products and services through ongoing refinements in response to continuous feedback

# EFQM

- The **EFQM** Excellence Model is a non-prescriptive framework for organizational management systems, promoted by **EFQM** (formerly known as the European Foundation for Quality Management) and designed for helping organizations in their drive towards being more competitive.

# Six Sigma

- **Six Sigma** seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes.

# IT Governance Model

## Audit Models

COSO

CobIT

Sarbanes-Oxley

US Securities & Exchange Commission

## Quality Systems & Mgmt. Frameworks

CMMi

ISO

Six Sigma

ITIL

BS 15000  
ISO 20000

ASL

Service Mgmt.

App. Dev. (SDLC)

IT Security

Project Mgmt.

IT Planning

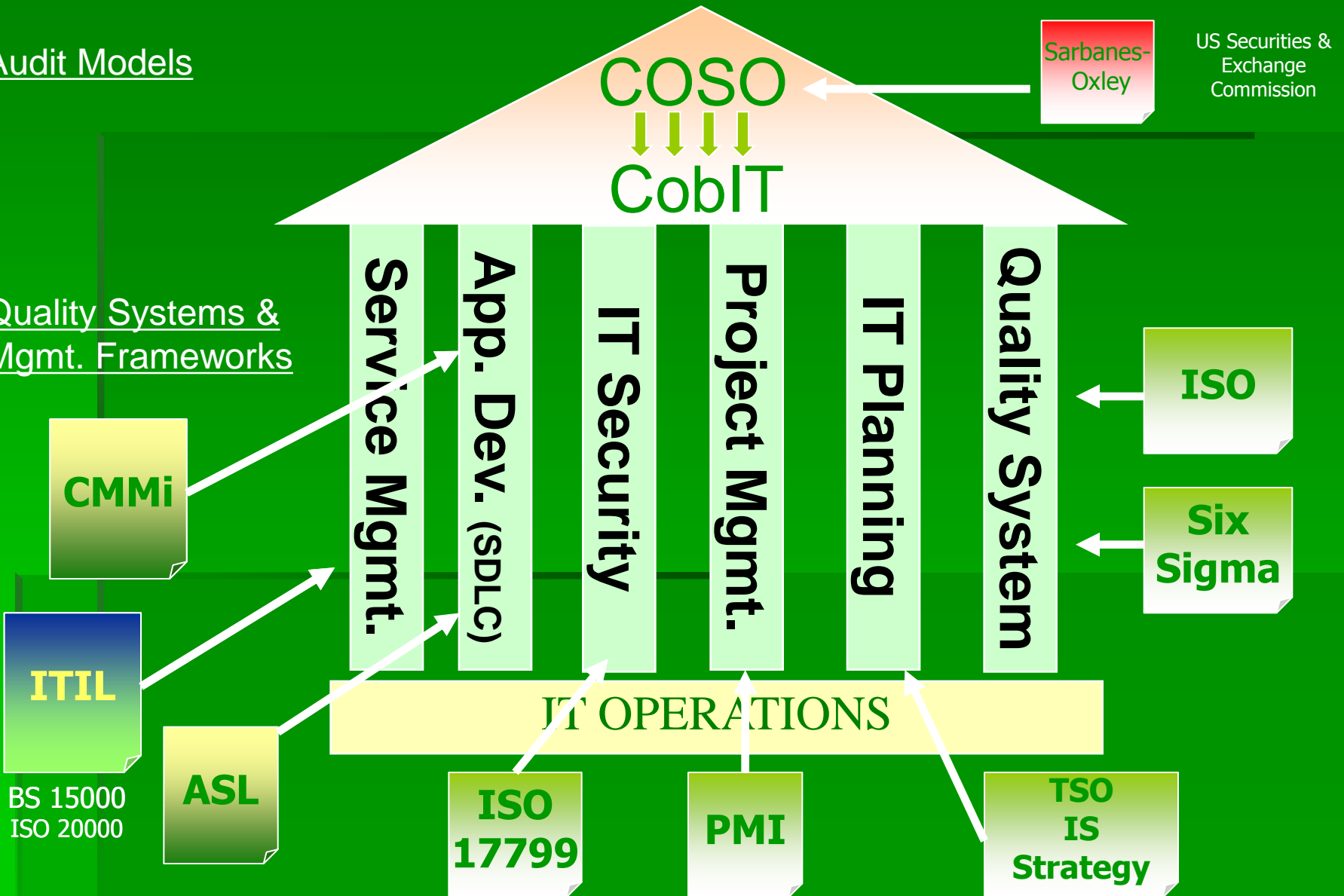
Quality System

IT OPERATIONS

ISO 17799

PMI

TSO IS Strategy





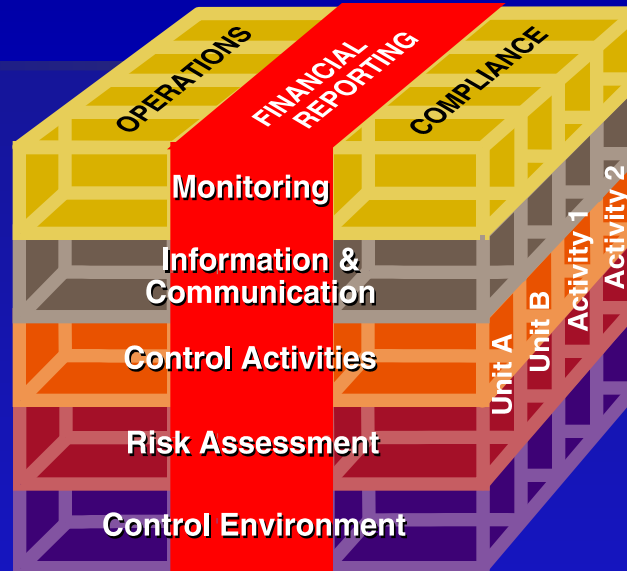
# Committee of Sponsoring Organizations (COSO) – The Components

## Monitoring

- Assess control system performance over time
- Ongoing and separate evaluations
- Management and supervisory activities

## Information and Communication

- Relevant information identified, captured and communicated timely
- Access to internal and externally generated information
- Information flow allows for management action



## Control Activities

- Policies that ensure management directives are carried out
- Approval and authorizations, verifications, evaluations, safeguarding assets security and segregation of duties

## Control Environment

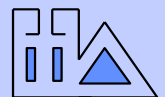
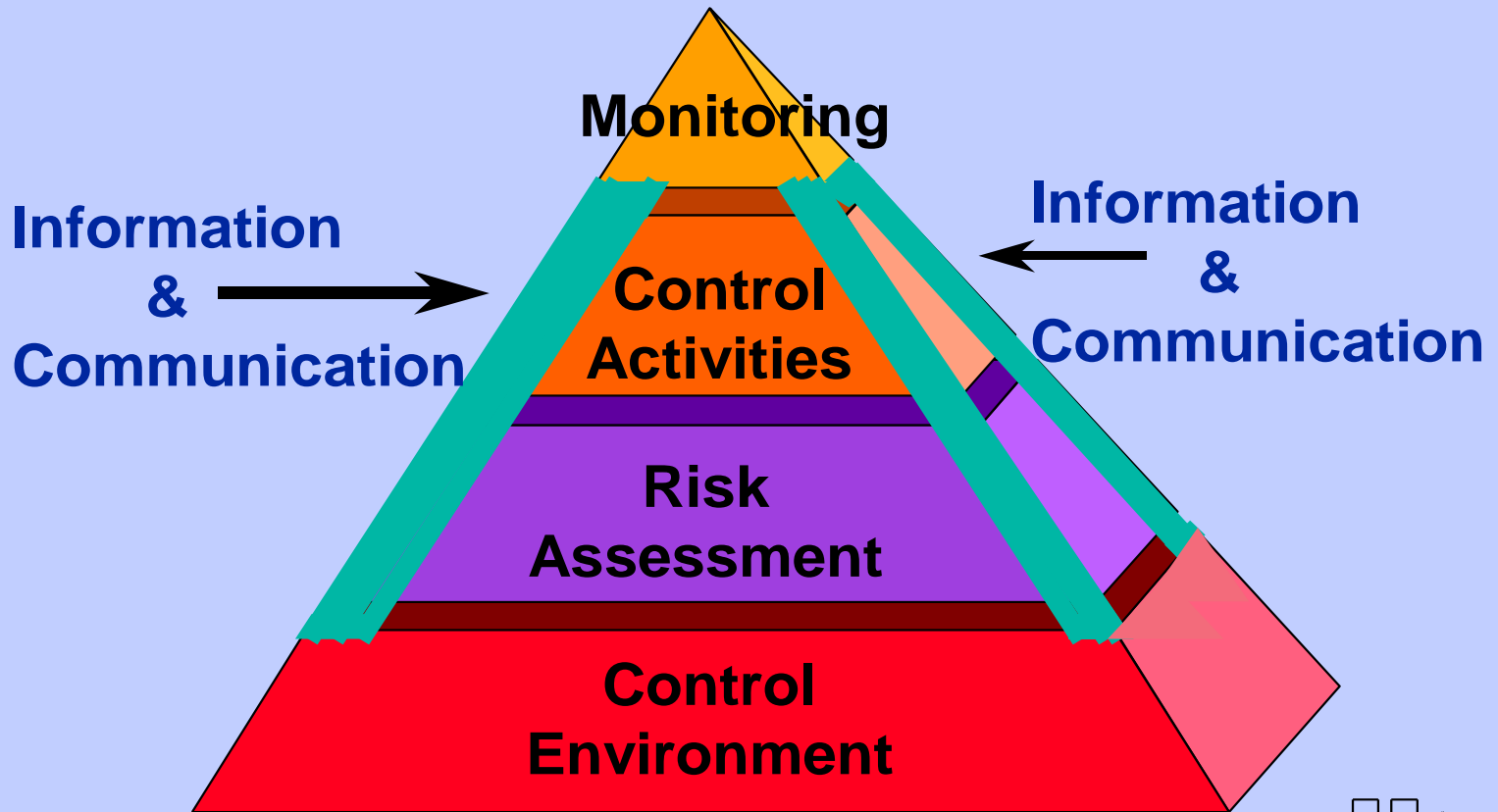
- Sets “tone at the top”
- Foundation for all other components of control
- Integrity, ethical values, competence, authority, responsibility

## Risk Assessment

- Identify and analyze relevant risks to achieving the entity’s objectives

# COSO Enterprise Risk Management (ERM) Model

## Graphical Representation



# The COSO ERM Framework

- Entity objectives can be viewed in the context of four categories
  - ❖ Strategic
  - ❖ Operations
  - ❖ Reporting
  - ❖ Compliance
- ERM considers activities at all levels of the organization
  - ❖ Enterprise-level
  - ❖ Division or subsidiary
  - ❖ Business unit processes

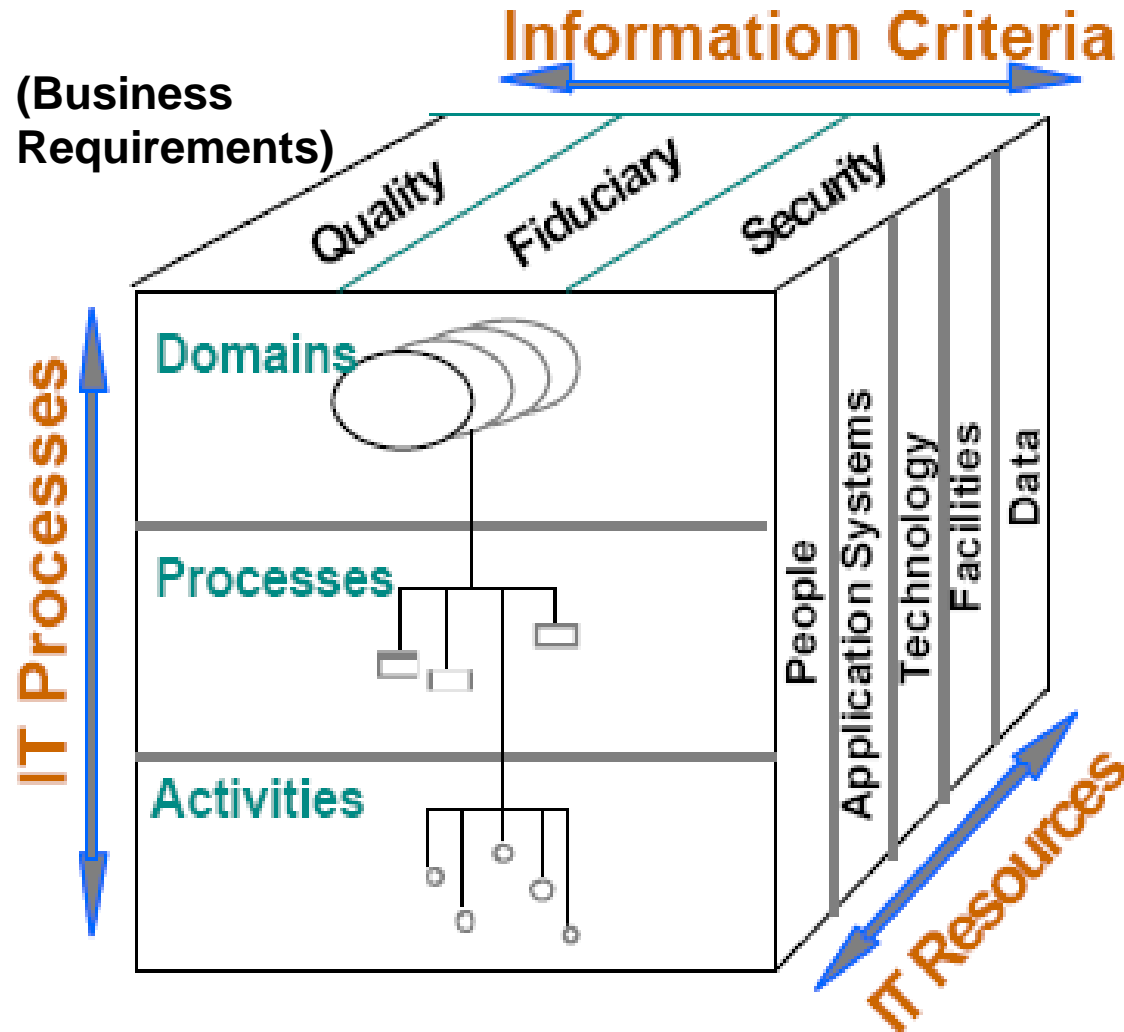


# **CobIT:**

## **Control Objectives for IT**

- CobIT is an open standard control framework for IT Governance with a focus on IT Standards and Audit
- Based on over 40 International standards and is supported by a network of 150 IT Governance Chapters operating in over 100 countries
- CobIT describes standards, controls and maturity guidelines for four domains, and 34 control processes

# The CobIT Cube



4 Domains

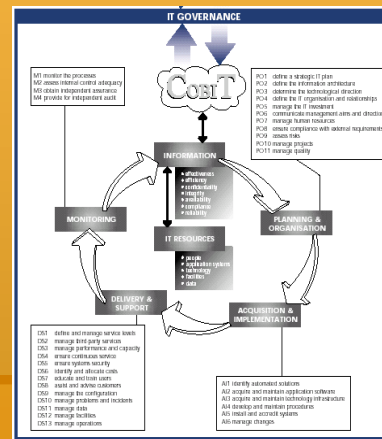
34  
Processes

318  
Control  
Objectives

# CobiT Domains

**Plan &  
Organize**  
(PO Process Domain)

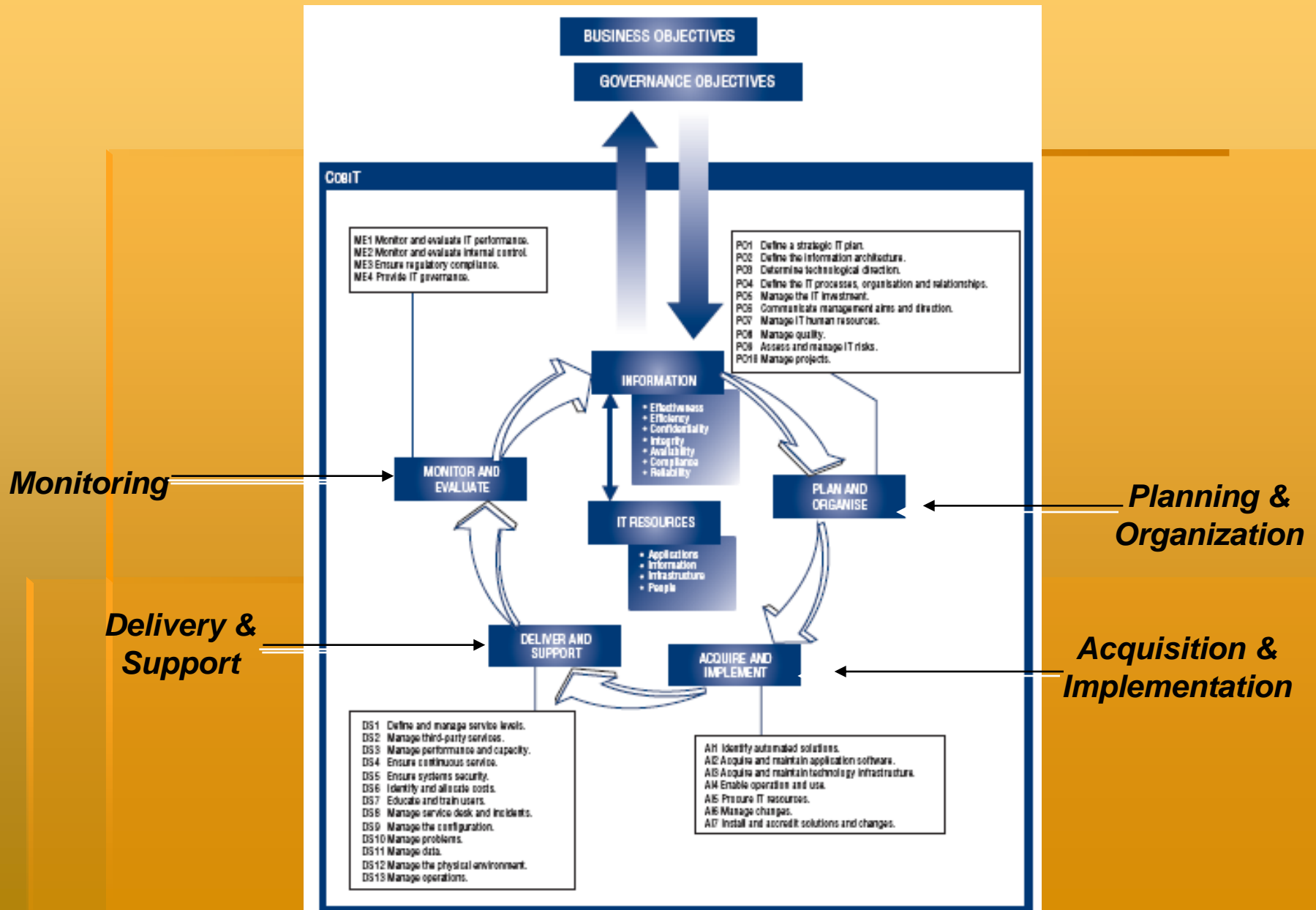
**Acquire & Implement**  
(AI Process Domain)



**Monitor**  
(M Process Domain)

**Deliver & Support**  
(DS Process Domain)

# CobiT Processes by Domain



# The 34 Defined CobiT Processes

## 1 PLANNING AND ORGANISATION

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Organisation and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage Human Resources
- PO8 Ensure Compliance with External Requirements
- PO9 Assess Risks
- PO10 Manage Projects
- PO11 Manage Quality

## 2 ACQUISITION AND IMPLEMENTATION

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Develop and Maintain Procedures
- AI5 Install and Accredite Systems
- AI6 Manage Changes

## 3 DELIVERY 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 Assist and Advise Customers
- DS9 Manage the Configuration
- DS10 Manage Problems and Incidents
- DS11 Manage Data
- DS12 Manage Facilities
- DS13 Manage Operations

## 4 MONITORING

- M1 Monitor the Processes
- M2 Assess Internal Control Adequacy
- M3 Obtain Independent Assurance
- M4 Provide for Independent Audit



# The 7 CobiT Principles

## 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.

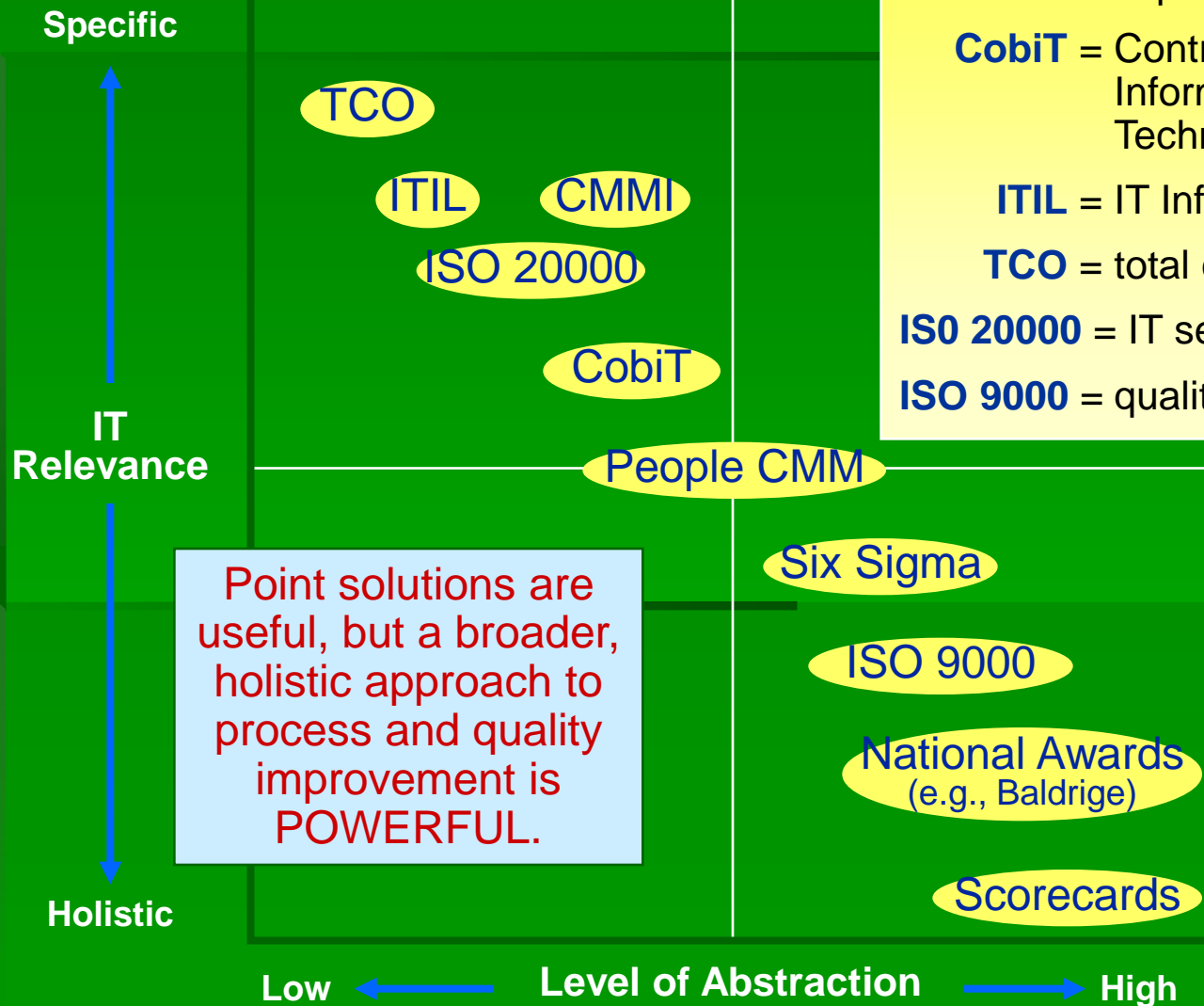
## Compliance

deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.

## Reliability of Information

relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

# Positioning the Frameworks



**CMM** = capability maturity model

**CobiT** = Control Objectives for Information and Related Technology

**ITIL** = IT Infrastructure Library

**TCO** = total cost of ownership

**ISO 20000** = IT service mgt standard

**ISO 9000** = quality mgt standard

Point solutions are useful, but a broader, holistic approach to process and quality improvement is **POWERFUL**.

# Process Framework - ITIL

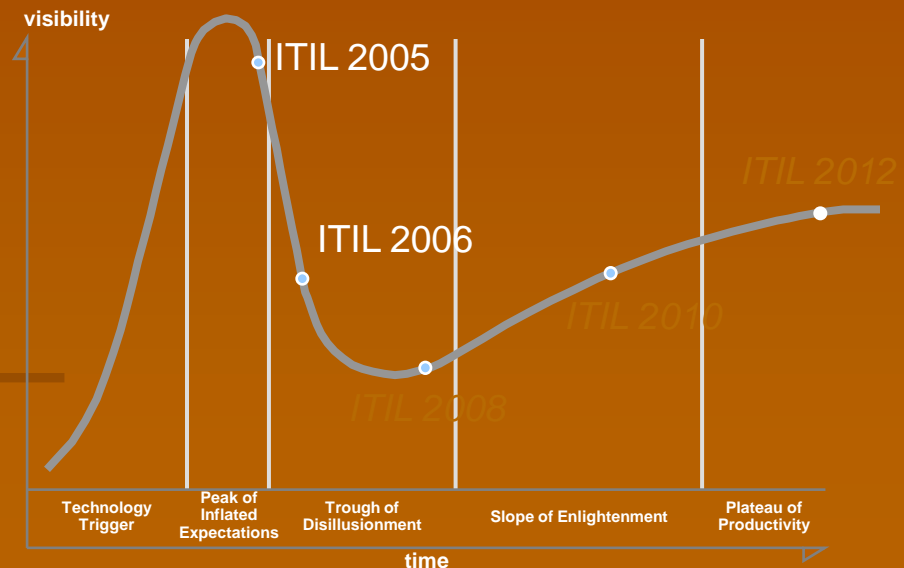
- ITIL is a best-practice process framework.
  - Service delivery
  - Service support
  - Others (application management, security management)
- Initiated by the U.K.'s government Central Computing and Telecommunication Agency (CCTA). CCTA is merged into the Office of Government Commerce.
- Shows the goals, general activities, inputs and outputs of the various processes.
- Does not "cast in stone" every action you should do on a day-to-day basis.
- ITIL Refresh or "Version 3" is in delivered.

# Hype Surrounding ITIL

- ITIL makes the business love the IT group!
- ITIL is easy!
- Buy our tool and have ITIL!
- Everybody is doing it ...

- What's next ...
  - ▮ ITIL cures cancer!
  - ▮ ITIL solves world hunger!

IT Operations Management Hype Cycle



# ITIL: The Good and the Bad

## ■ Service Delivery:

- Service-level management
- Financial management
- Capacity management
- IT service continuity
- Availability management

## ■ Service Support:


- Incident management
- Problem management
- Change management
- Configuration management
- Release management

## ■ Service Desk

### Core Benefits:

- ✓ Standard process language
- ✓ Emphasis on process vs. technology
- ✓ Process integration
- ✓ Standardization enables cost and quality improvements
- ✓ Focus on customer

### Limitations:

- Not a process improvement methodology
  - **Specifies "what" but not "how"**
  - Doesn't cover all processes
  - Doesn't cover organization issues
  - Hype driving unrealistic expectations
- 

# Assuming Tools Will Solve Your Problems

*"Man is a tool-using animal. Nowhere do you find him without tools; without tools he is nothing, with tools he is all."* (Thomas Carlyle)

- Be wary of vendor hype
- Focus on process first
- Tools can be enablers or inhibitors
- Assess capabilities of your current tools
- Review new tools where they would pay significant dividends
- Buy what you need, as you need it

