



Why, What, and How of COBIT Framework

Author: Deepak Chebbi



- ❖ **Technology makes new business processes possible leading to loss of control and more regulation**
- ❖ **Developments in IT and business practices make corporate governance more difficult**
- ❖ **Officers and management will be held accountable**
- ❖ **Already major changes have occurred but pressure to continue to change remains**



Committee for Sponsoring Organizations (COSO)

In order to discharge management's responsibilities as well as to achieve its objectives, they must establish an adequate system of internal control. This control system or framework must be in place to support business requirements for effectiveness and efficiency of operations, reliability of information and compliance with laws and regulations.

National Institute for Standards and Technology

"While computer security helps manage risks, it does not eliminate it. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighed against the cost, can be a difficult management decision."



Control

“The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.”

IT Control Objective

“A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.”



The Five Elements of COBIT

- **Executive Summary** **senior executives (CEO, CIO)**
 “There is a method...”
- **Framework** **senior operational management**
 “The method is...”
- **Control Objectives** **middle management**
 “Minimum controls are...”
- **Audit Guidelines** **line management, controls practitioner**
 “Here’s how you audit...”
- **Implementation Tool Set** **director, middle management**
 “Here’s how you implement...”



Standards and Regulations

COBIT includes 36 national and international standards

- **Codes of conduct issued by Council of Europe, OECD, ISACA, etc.**
- **Qualification criteria for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.**
- **Professional standards in internal control and auditing: COSO Report, IFAC, AICPA, IIA, ISACA, PCIE, GAO standards, etc.**
- **Industry practices and requirements from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc.**
- **Technical standards from ISO, EDIFACT, etc.**
- **Emerging industry-specific requirements such as from banking, electronic commerce and IT manufacturing**



Why Should an Organization Adopt COBIT?

- **Attention on Corporate Governance**
- **Management accountability for resources**
- **Specific need for control of IT resources**
- **Business oriented solutions**
- **Framework for risk assessment**
- **Authoritative basis**
- **Improved communication among management, users and auditors**



Who needs COBIT?

- **Management needs COBIT**
 - to evaluate IT investment decisions
 - to balance risk and control of investment in an often unpredictable IT environment
 - to benchmark existing and future IT environment
- **Users need COBIT**
 - to obtain assurance on security and controls of products and services provided by internal and third-parties.
- **IS auditors need COBIT**
 - to substantiate opinions to management on internal controls
 - to answer the question: What minimum controls are necessary?



A Product For Many Audiences

- **Executive manager**
- **Business manager**
- **IT manager**
- **Project manager**
- **Developer**
- **Information security officer**
- **Auditor**



COBIT for the ... Executive Manager

Use COBIT process model to establish common language between business and IT; allocate clear responsibilities

RISK		Importance = How important for the organisation on a scale from 1 (not at all) to 5 (very) Performance = How well is it done from 1 (don't know or badly) to 5 (very well) Audited = Yes, No or ? Formality = Is there a contract, SLA, or a clearly documented Procedure? (Yes, No or ?) Accountable = Name or "don't know"	Who Does It?				Audited	Formality	Who is Accountable?
Importance	Performance		IT	Other	Outside	Don't Know			
COBIT's Domains and Processes									
Planning & Organisation									
		PO1 Define a Strategic IT Plan							
		PO2 Define the Information Architecture							
		PO3 Determine the 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							
Acquisition & Implementation									
		A11 Identify Solutions							
		A12 Acquire and Maintain Application Software							
		A13 Acquire and Maintain Technology Architecture							
		A14 Develop and Maintain IT Procedures							
		A15 Install and Accredite Systems							
		A16 Manage Changes							
Delivery & Support									
		DS1 Define Service Levels							
		DS2 Manage Third-Party Services							
		DS3 Manage Performance and Capacity							
		DS4 Ensure Continuous Service							
		DS5 Ensure System Security							
		DS6 Identify and Attribute Costs							
		DS7 Educate and Train Users							
		DS8 Assist and Advise IT Customers							
		DS9 Manage the Configuration							
		DS10 Manage Problems and Incidents							
		DS11 Manage Data							
		DS12 Manage Facilities							
		DS13 Manage Operations							
Monitoring									
		M1 Monitor the Processes							
		M2 Assess Internal Control Adequacy							
		M3 Obtain Independent Assurance							
		M4 Provide for Independent Audit							



COBIT for the ... IT Manager

Use the COBIT control model to establish SLAs and communicate with business functions

CONTRACT SERVICE/SERVICE LEVEL AGREEMENT (SLA) FORM

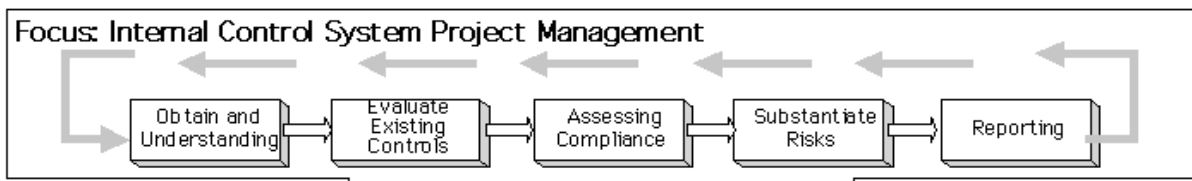
Performed By				IT Process	Internal Controls			Formal Contract/SLA in place?				WP Ref.	
IT Department	Within Organisation	Outsourced	Not Sure		Documented	Not Documented	Not Sure	Yes	No	Not Applicable	Not Sure		
				PO1	Define a Strategic IT Plan								
				PO2	Define the Information Architecture								
				PO3	Determine the Technological Direction								
				PO4	Define the IT Organisation and Relationships								
				PO5	Manage the Information Technology 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								
				A11	Identify Solutions								
				A12	Acquire and Maintain Application Software								
				A13	Acquire and Maintain Technology Architecture								
				A14	Develop and Maintain Information Technology Procedures								
				A15	Install and Accredited Systems								
				A16	Manage Changes								
				DS1	Define Service Levels								
				DS2	Manage Third-Party Services								
				DS3	Manage Performance and Capacity								
				DS4	Ensure Continuous Service								
				DS5	Ensure Systems Security								
				DS6	Identify and Attribute Costs								
				DS7	Educate and Train Users								
				DS8	Assist and Advise Information Technology Customers								
				DS9	Manage the Configuration								
				DS10	Manage Problems and Incidents								
				DS11	Manage Data								
				DS12	Manage Facilities								
				DS13	Manage Operations								
				M1	Monitor the Processes								
				M2	Assess Internal Control Adequacy								
				M3	Obtain Independent Assurance								
				M4	Provide for Independent Audit								



COBIT for the ... Project Manager

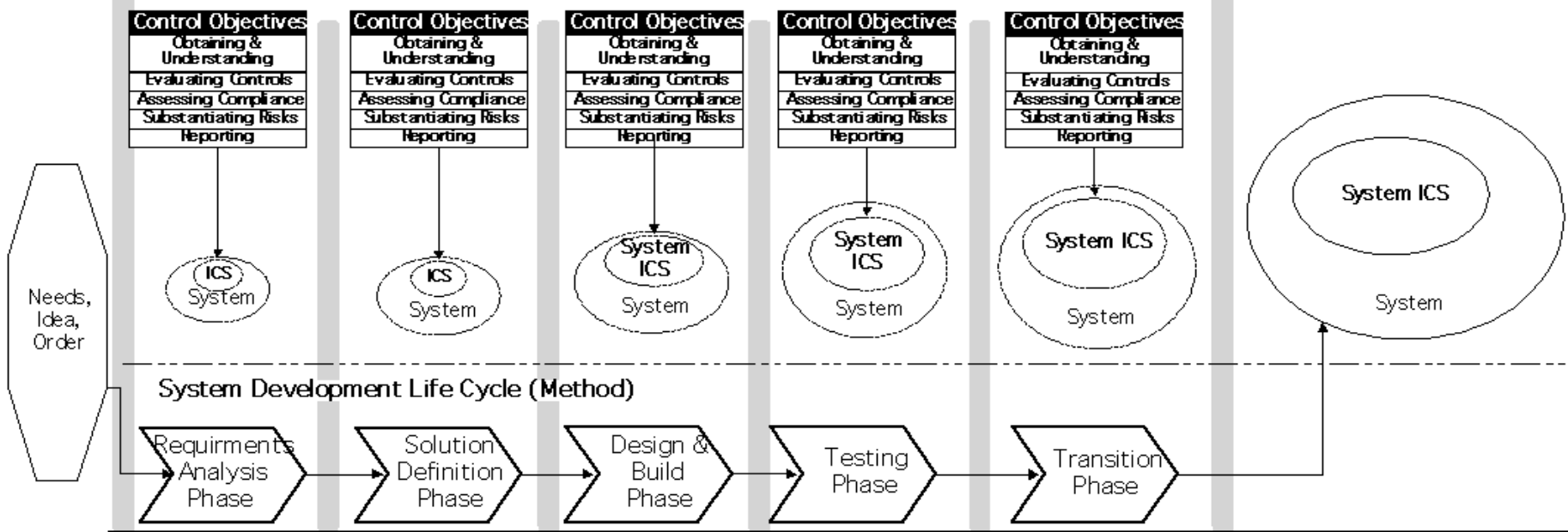
Use COBIT to help ensure that project plans incorporate generally accepted phases in IT planning, acquisition and development, service delivery and project management, and assessment

Project Audit - Internal Control System (ICS)



Focus: Internal Control System built into New System

System Audit - System ICS



COBIT for the ... Developer

Use COBIT to ensure that all applicable IT control objectives in the development project have been addressed

IT Process		Information								Criteria				IT Resources						
		effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data							
PO1	Define Requirements	P	S																	
PO2	Define Architecture	P	S	S	S															
PO3	Define Requirements	P	S																	
PO4	Define Requirements	P	S																	
PO5	Manage Requirements	P	P							S										
PO6	Manage Requirements	P								S										
PO7	Manage Human Resources	P	P																	
PO8	Manage Human Resources	P								P	S									
PO9	Assess Risks	S	S	P	P	P	S	S												
PO10	Manage Projects	P	P																	
PO11	Manage Quality	P	P		P					S										
AI1	Identify Solutions	P	S																	
AI2	Assess Alternatives	P	P		S			S	S											
AI3	Assess Alternatives	P	P		S															
AI4	Develop Prototypes	P	P		S			S	S											
AI5	Implement Systems	P			S	S														
AI6	Managing Changes	P	P		P	P				S										
DS1	Define Service Levels	P	P	S	S	S	S	S	S											
DS2	Manage Third-Party Services	P	P	S	S	S	S	S	S											
DS3	Manage Capacity	P	P				S													
DS4	Ensure Continuous Service	P	S					P												
DS5	Ensure Security			P	P	S	S	S	S											
DS6	Manage Costs		P							P										
DS7	Manage Risks	P	S																	
DS8	Assess and Design IT Controls	P																		
DS9	Manage Configuration	P					S		S											
DS10	Manage Information	P					S													
DS11	Manage Data					P				P										
DS12	Manage Facilities					P	P													
DS13	Manage Operations	P	P		S	S														
M1	Monitor the Process	P	S	S	S	S	S	S	S											
M2	Assess Control Adequacy	P	P	S	S	S	S	S	S											
M3	Obtain Assurance	P	P	S	S	S	S	S	S											
M4	Provide Guidance	P	P	S	S	S	S	S	S											



COBIT for the ... Security Officers

Use COBIT to structure the information security program, policies and procedures

RISK ASSESSMENT FORM

Importance				IT Process	Risk					Internal Controls			WP Ref.
Very Important	Somewhat Important	Not Important	Not Sure		High	Medium	Low	Immaterial	Not Sure	Documented	Not Documented	Not Sure	
				PO1	Define a Strategic IT Plan								
				PO2	Define the Information Architecture								
				PO3	Determine the Technological Direction								
				PO4	Define the IT Organisation and Relationships								
				PO5	Manage the Information Technology 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								
				A11	Identify Solutions								
				A12	Acquire and Maintain Application Software								
				A13	Acquire and Maintain Technology Architecture								
				A14	Develop and Maintain Information Technology Procedures								
				A15	Install and Accredite Systems								
				A16	Manage Changes								
				DS1	Define Service Levels								
				DS2	Manage Third-Party Services								
				DS3	Manage Performance and Capacity								
				DS4	Ensure Continuous Service								
				DS5	Ensure Systems Security								
				DS6	Identify and Attribute Costs								
				DS7	Educate and Train Users								
				DS8	Assist and Advise Information Technology Customers								
				DS9	Manage the Configuration								
				DS10	Manage Problems and Incidents								
				DS11	Manage Data								
				DS12	Manage Facilities								
				DS13	Manage Operations								
				M1	Monitor the Processes								
				M2	Assess Internal Control Adequacy								
				M3	Obtain Independent Assurance								
				M4	Provide for Independent Audit								



COBIT for the ... Auditors

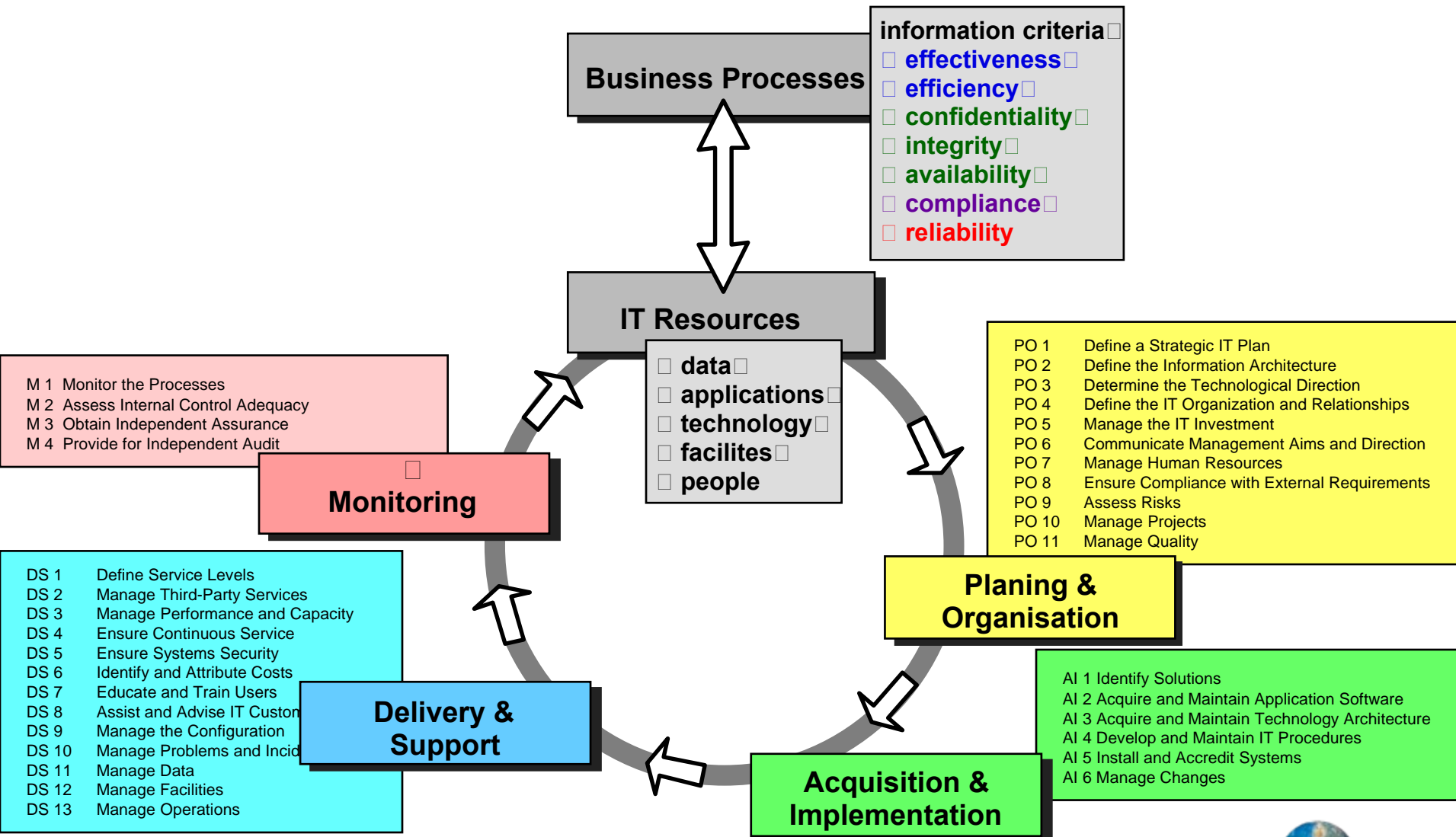
Use COBIT as criteria for review and examination, and for framing IT-related audits

In Prior Scope				Prior Audit Opinion				Material Weaknesses	Findings	Disposition of Findings			
Yes	No			Unqualified	Qualified	Adverse	Disclaimer			Resolved	Unresolved	N/A	Not Determined
IT Process													
		PO 1	Define a Strategic IT plan										
		PO 2	Define the Information Architecture										
		PO 3	Determine the Technological Direction										
		PO 4	Define IT Organization and Relationships										
		PO 5	Manage the Investment										
		PO 6	Communicate Management Aims and Direction										
		PO 7	Manage Human Resources										
		PO 8	Ensure Compliance with External Requirements										
		PO 9	Assess Risks										
		PO 10	Manage Projects										
		PO 11	Manage Quality										
		A 11	Identify Automated Solutions										
		A 12	Acquire & Maintain Application Software										
		A 13	Acquire & Maintain Technology Architecture										
		A 14	Develop & Maintain Procedures										
		A 15	Install & Accredit System										
		A 16	Manage Changes										
		DS 1	Define Service Levels										
		DS 2	Manage Third-Party Services										
		DS 3	Manage Performance & Capacity										
		DS 4	Ensure Continuous Service										
		DS 5	Ensure System Security										
		DS 6	Identify & Allocate Costs										
		DS 7	Educate & Train Users										
		DS 8	Assist & Advise Customers										
		DS 9	Manage the Configuration										
		DS 10	Manage Problems & Incidents										
		DS 11	Manage Data										
		DS 12	Manage Facilities										
		DS 13	Manage Operations										
		M 1	Monitor the Processes										
		M 2	Obtain independent assurance										
		M 3	Obtain Independent Assurance										
		M 4	Provide for Independent Audit										
			Insert the number of findings if there is more than one per process category and then reflect the appropriate number under each column.										



The Framework's Principles

Linking the management's **IT expectations** with the management's **IT responsibilities**





Quality

Security

Fiduciary

- **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) usage of resources.
- **confidentiality** - concerns protection of sensitive information from unauthorized disclosure.
- **integrity** - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.
- **availability** - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.
- **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 systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing information to report to regulatory bodies with regard to compliance with laws and regulations.



- **Data** : Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, etc.
- **Application Systems** : understood to be the sum of manual and programmed procedures.
- **Technology** : covers hardware, operating systems, database management systems, networking, multimedia, etc..
- **Facilities** : Resources to house and support information systems.
- **People** : Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.



Planning & Organization

- **PO 1** **Define a Strategic IT Plan**
- **PO 2** **Define the Information Architecture**
- **PO 3** **Determine the Technological Direction**
- **PO 4** **Define the IT Organisation and Relationships**
- **PO 5** **Manage the IT Investment**
- **PO 6** **Communicate Management Aims and Direction**
- **PO 7** **Manage Human Resources**
- **PO 8** **Ensure Compliance with External Requirements**
- **PO 9** **Assess Risks**
- **PO 10** **Manage Projects**
- **PO 11** **Manage Quality**

- * Strategy and tactics for IT contribution
- * Meeting business objectives
- * Appropriately planned, communicated and managed
- * Proper organization and technological infrastructure



Acquisition & Implementation

- **AI 1** **Identify Solutions**
- **AI 2** **Acquire and Maintain Application Software**
- **AI 3** **Acquire and Maintain Technology Architecture**
- **AI 4** **Develop and Maintain IT Procedures**
- **AI 5** **Install and Accredit Systems**
- **AI 6** **Manage Changes**

- * **Realization of IT strategy**
- * **Solutions identified, developed, or acquired and implemented**
- * **Solutions integrated into business process**
- * **Change and maintenance of systems**



Delivery and Support

- **DS 1** **Define Service Levels**
- **DS 2** **Manage Third-Party Services**
- **DS 3** **Manage Performance and Capacity**
- **DS 4** **Ensure Continuous Service**
- **DS 5** **Ensure Systems Security**
- **DS 6** **Identify and Attribute Costs**
- **DS 7** **Educate and Train Users**
- **DS 8** **Assist and Advise IT Customers**
- **DS 9** **Manage the Configuration**
- **DS 10** **Manage Problems and Incidents**
- **DS 11** **Manage Data**
- **DS 12** **Manage Facilities**
- **DS 13** **Manage Operations**

- * Actual delivery of required services
- * Actual operations through security including training
- * Establishment of support processes
- * Actual processing of data by applications



Monitoring

- **M 1 Monitor the Processes**
- **M 2 Assess Internal Control Adequacy**
- **M 3 Obtain Independent Assurance**
- **M 4 Provide for Independent Audit**

- * **Regular assessment of all IT processes**
- * **Compliance with and quality of controls**



Pros and Cons

- **A package for every possible target group**
 - Executive, business and IT manager, user
 - Project manager, developer, operations
 - Information security officer, auditor
 - **Well structured, comprehensive, precise**
 - **Nationally and internationally accepted**
 - **Very complete package**
 - Executive Summary “There is a method...”
 - Framework “The method is...”
 - Control Objectives “Minimum controls are...”
 - Audit Guidelines “Here’s how you audit...”
 - Implementation Tool Set “Here’s how you implement...”
 - CD with Info-DB
- Needs a big starting effort
 - Has reputation of an audit standard
 - No control self assessment



Putting it All Together

- Don't concentrate on details
- Don't use all those gadgets
- Forget about "do-it-yourself"

- ... only a comprehensive planning, acquisition, delivery and support of all IT resources will guarantee your success.

