COBIT: An Overview

released by the

IT Governance Institute

July 2000

What Does COBIT Stand For?

C	**C**ontrol
OB	**OB**jectives
I	for **I**nformation
T	and Related **T**echnology

Scope and Objectives

* Generally Applicable and Accepted Standard for Good Practice for Information and Information Technology (IT) Control

* For Application to Enterprise-Wide IT

* Starting from a Framework for Control in IT

* Based on the IT Governance Institute's Control Objectives

* Management Oriented

* Aligned with De Jure and De Facto Standards and Regulations

* Based on Critical Review of Tasks and Activities Regarding Business Re-Engineering

Standards and Regulations

* Technical standards from ISO, EDIFACT, etc.

* 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, CICA, IFAC, IIA, AICPA, GAO, PCIE, ISACA standards, etc.

* Industry practices and requirements from industry forums (BS 7799, ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc.

* Emerging industry specific requirements such as from banking, electronic commerce and IT manufacturing

COBIT *FRAMEWORK*

Audience -- *Management*:

To Help Them Balance Risk and Control Investment in an Often Unpredictable IT Environment

Audience -- *Users*:

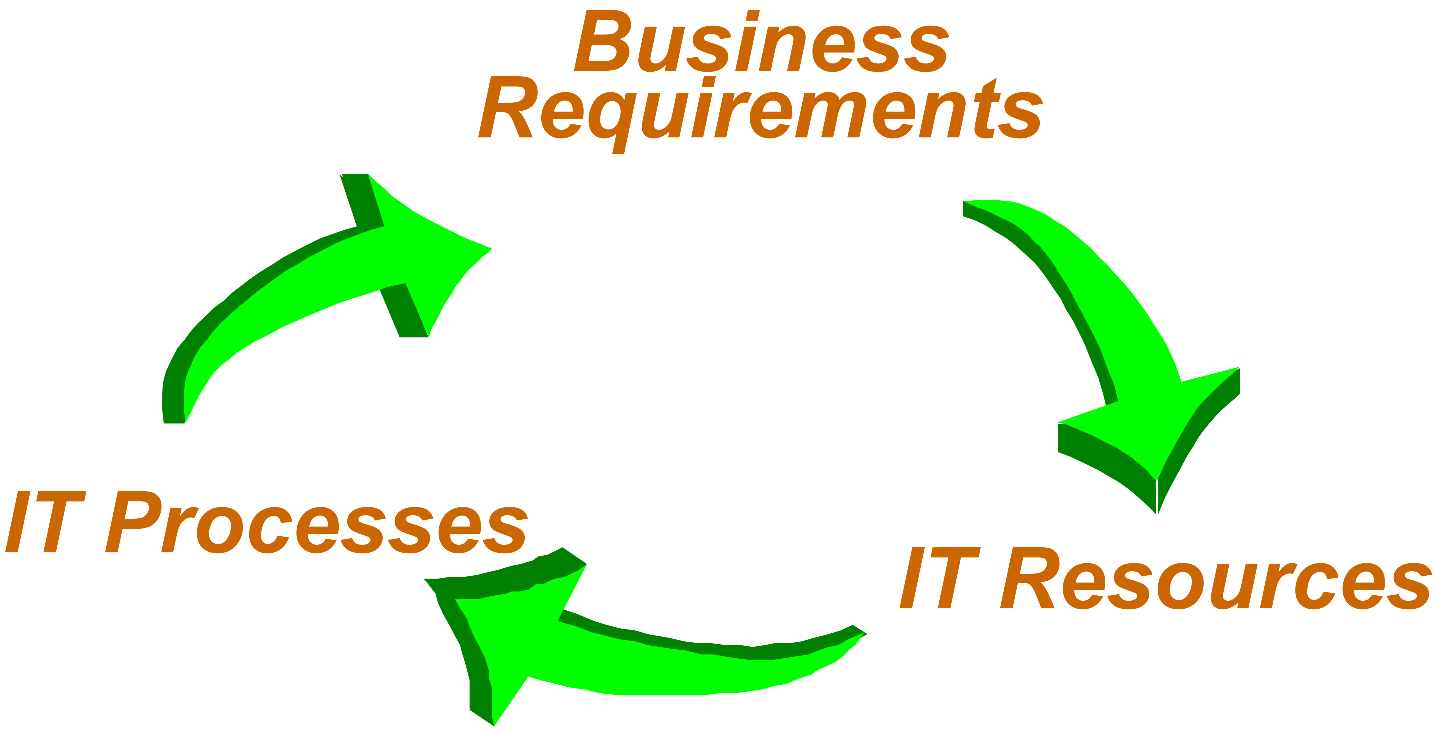
To Obtain Assurance on Security and Controls of IT Services Provided by Internal and Third Parties

Audience -- *Auditors*:

To Substantiate Their Opinions and/or Provide Advice to Management on Internal Controls

IT GOVERNANCE INSTITUTE™

The Framework's Principles



Business Requirements

IT Resources

IT Processes

Business Requirements = Information Criteria

Quality Requirements

Quality
Cost
Delivery

Fiduciary Requirements (COSO Report)

Effectiveness and Efficiency of Operations
Reliability of Information
Compliance with Laws and Regulations

Security Requirements

Confidentiality
Integrity
Availability

IT GOVERNANCE INSTITUTE™

Business Requirements = 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) usage of resources.

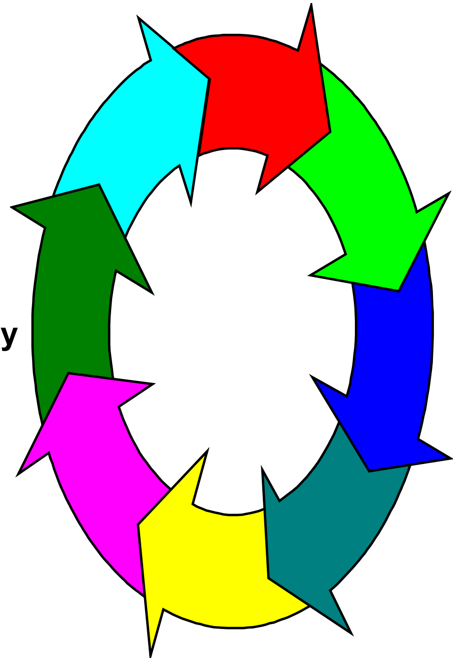
confidentiality - concerns protection of sensitive information from unauthorized disclosure.

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.



IT GOVERNANCE INSTITUTE™

Information Technology Resources

Data

Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, etc.

Application Systems

Application systems is understood to be the sum of manual and programmed procedures.

Technology

Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

Facilities

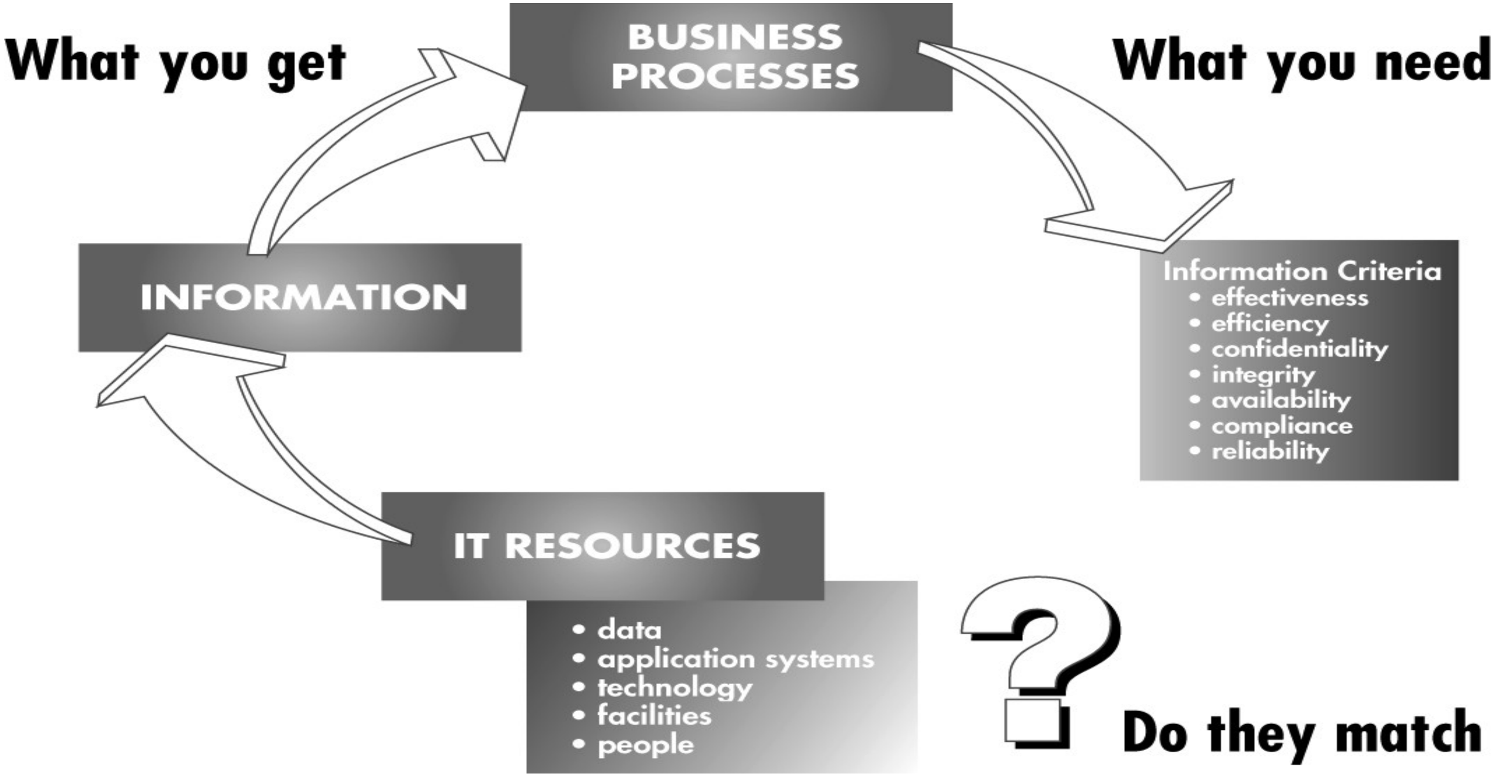
Resources to house and support information systems.

People

Staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

IT GOVERNANCE INSTITUTE™

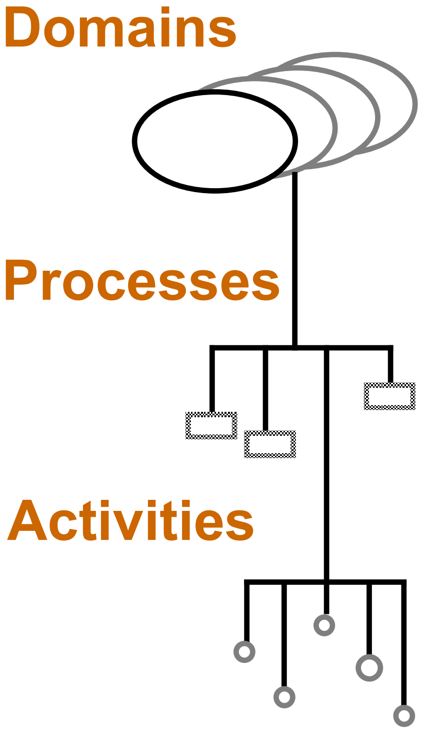
The Framework's Principles



Information Criteria
- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

- data
- application systems
- technology
- facilities
- people

IT Domains & Processes



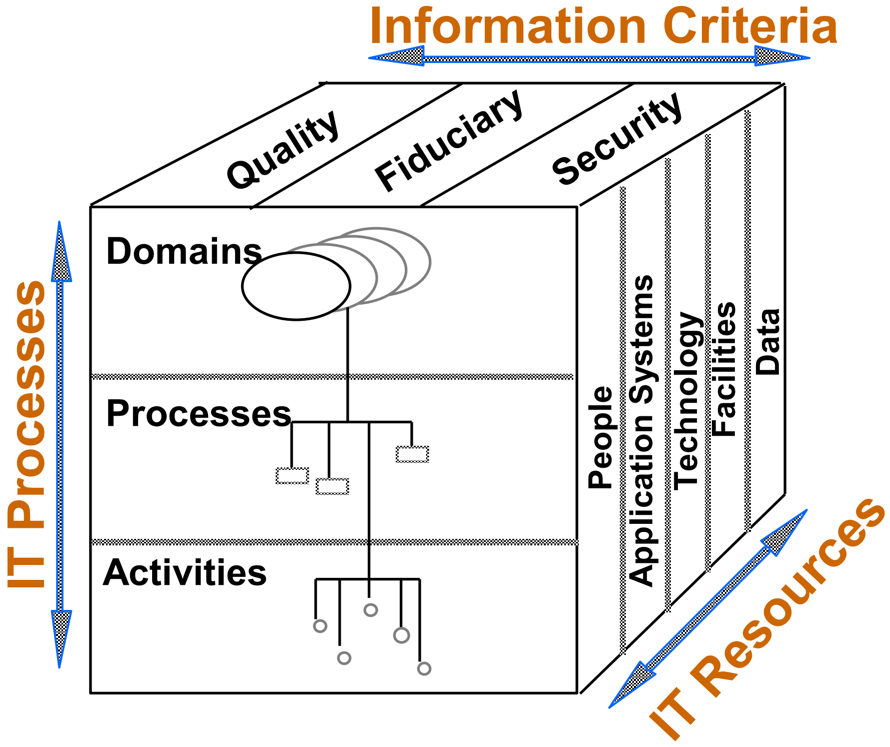
Natural grouping of processes, often matching an organisational domain of responsibility.

A series of joined activities with natural (control) breaks.

Actions needed to achieve a measurable result. Activities have a life-cycle whereas tasks are discreet.

IT GOVERNANCE INSTITUTE™

COBIT Cube


Information Criteria
Quality
Fiduciary
Security
IT Processes
Domains
Processes
Activities
People
Application Systems
Technology
Facilities
Data
IT Resources

CONTROL OBJECTIVES

The DOMAINS

* Planning & Organisation

* Acquisition & Implementation

* Delivery & Support

* Monitoring

IT GOVERNANCE INSTITUTE™

Planning & Organisation

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

Acquisition & Implementation

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

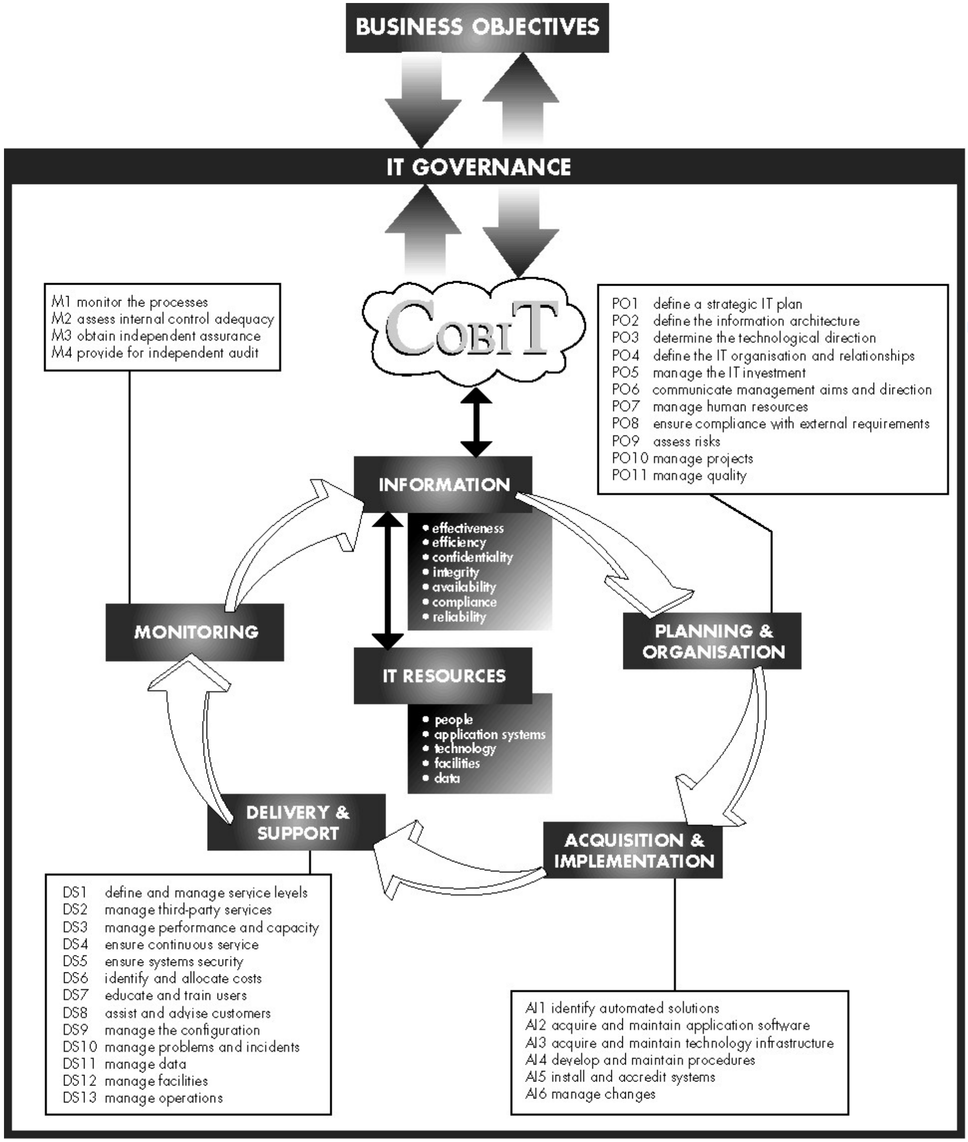
Delivery & Support

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

Monitoring

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

GOVERNANCE INSTITUTE™



BUSINESS OBJECTIVES

IT GOVERNANCE

COBIT

M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit

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

INFORMATION

- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

MONITORING

PLANNING & ORGANISATION

IT RESOURCES

- people
- application systems
- technology
- facilities
- data

DELIVERY & SUPPORT

ACQUISITION & IMPLEMENTATION

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

AI1 identify automated solutions
AI2 acquire and maintain application software
AI3 acquire and maintain technology infrastructure
AI4 develop and maintain procedures
AI5 install and accredit systems
AI6 manage changes

COBIT's Golden Rule

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

IT GOVERNANCE INSTITUTE™

IT Processes

Planning and Organisation

PO 1	Define a Strategic IT Plan
PO 2	Define the Information Architecture
PO 3	Determine 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

DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

PO 1

1.1 IT as Part of the Organisation’s Long- and Short-Range Plan

CONTROL OBJECTIVE

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organisation’s mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organisation’s long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organisation.

1.2 IT Long-Range Plan

CONTROL OBJECTIVE

IT management and business process owners are responsible for regularly developing IT long-range plans supporting the achievement of the organisation’s overall missions and goals. The planning approach should include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

1.3 IT Long-Range Planning - Approach and Structure

CONTROL OBJECTIVE

IT management and business process owners should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan which covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resources risks. Aspects which need to be taken into account and adequately addressed during the planning process include the organisational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the market, planning horizon, business process re-engineering, staffing, in- or out-sourcing, data, application systems and technology architectures. Benefits of the choices made should be clearly identified. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans such as the organisation quality plan and the information risk management plan.

1.4 IT Long-Range Plan Changes

CONTROL OBJECTIVE

IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organisation's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long- and short-range plans are developed and maintained.

IT GOVERNANCE INSTITUTE™

1.5 Short-Range Planning for the IT Function

CONTROL OBJECTIVE

IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

1.6 Communication of IT Plans

CONTROL OBJECTIVE

Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organisation.

GOVERNANCE INSTITUTE™

1.7 Monitoring and Evaluating of IT Plans

CONTROL OBJECTIVE

Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feed-back obtained should be evaluated and considered in future IT planning.

IT GOVERNANCE INSTITUTE™

1.8 Assessment of Existing Systems

CONTROL OBJECTIVE

Prior to developing or changing the strategic, or long-range IT plan, IT management should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses, in order to determine the degree to which the existing systems support the oganisation's business requirements.

IT Processes

Acquisition and Implementation

AI 1	Identify Automated Solutions
AI 2	Acquire and Maintain Application Software
AI 3	Acquire and Maintain Technology Infrastructure
AI 4	Develop and Maintain Procedures
AI 5	Install and Accredit Systems
AI 6	Manage Changes

IT Processes

Delivery and Support

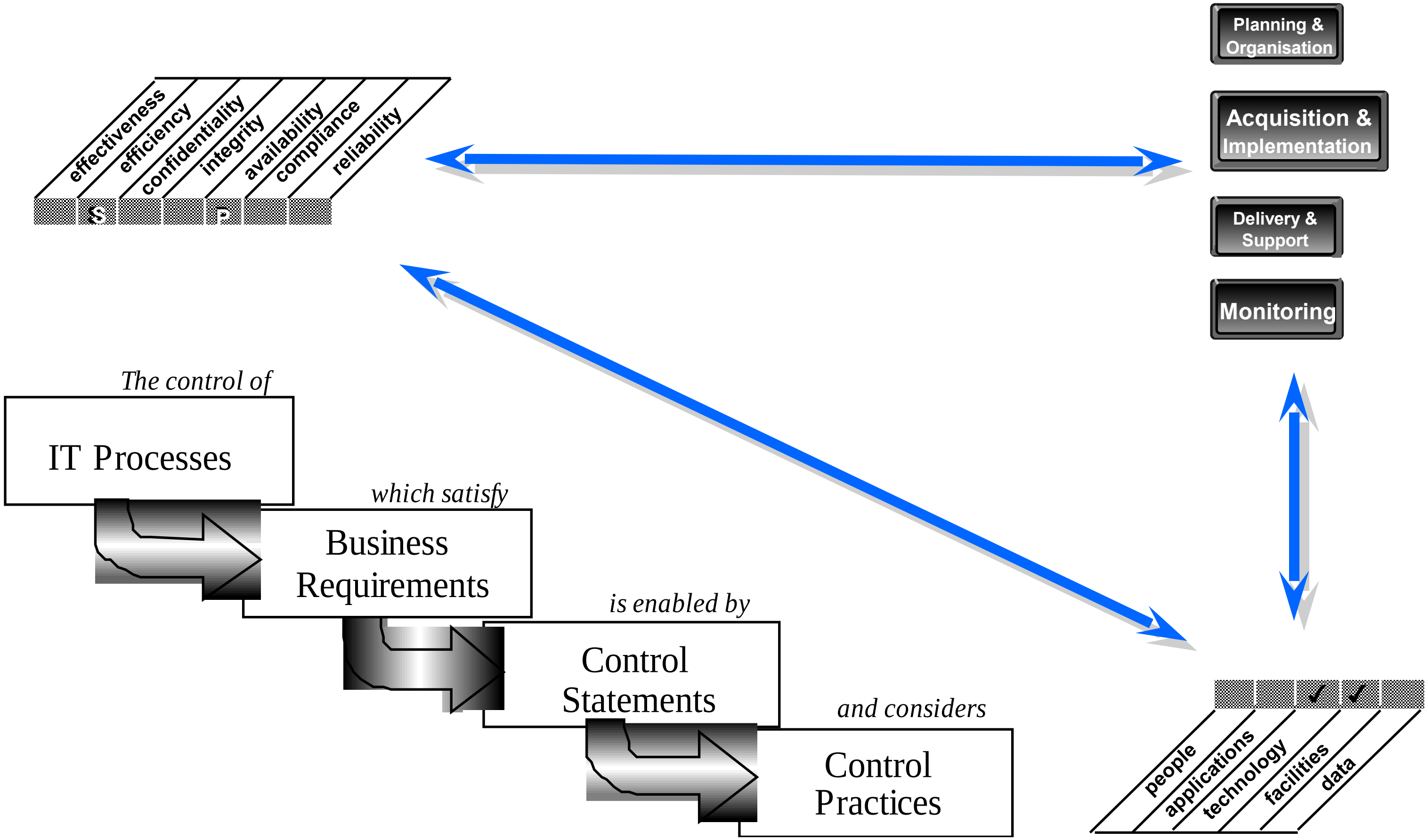
DS 1	Define and Manage Service Levels
DS 2	Manage Third-Party Services
DS 3	Manage Performance and Capacity
DS 4	Ensure Continuous Service
DS 5	Ensure Systems Security
DS 6	Identify and Allocate Costs
DS 7	Educate and Train Users
DS 8	Assist and Advise Customers
DS 9	Manage the Configuration
DS 10	Manage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

IT Processes

Monitoring

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

COBIT's Waterfall and Navigation Aids



effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

S P

Planning & Organisation

Acquisition & Implementation

Delivery & Support

Monitoring

The control of

IT Processes

which satisfy

Business Requirements

is enabled by

Control Statements

and considers

Control Practices

✓ ✓

people
applications
technology
facilities
data

AUDIT GUIDELINES

The objectives of auditing are to:

* *provide management with reasonable assurance that control objectives are being met;*
* *where there are significant control weaknesses, to substantiate the resulting risks; and*
* *advise management on corrective actions.*

AUDIT GUIDELINES

The process is audited by:

Obtaining an understanding of business requirements, related risks, and relevant control measures

Evaluating the appropriateness of stated controls

Assessing compliance by testing whether the stated controls are working as prescribed, consistently and continuously

Substantiating the risk of the control objectives not being met by using analytical techniques and/or consulting alternative sources.

GENERIC AUDIT GUIDELINE

OBTAINING AN UNDERSTANDING

The audit steps to be performed to document the activities underlying the control objectives as well as to identify the stated control measures/procedures in place.

Interview appropriate management and staff to gain an understanding of:

- Business requirements and associated risks
- Organisation structure
- Roles and responsibilities
- Policies and procedures
- Laws and regulations
- Control measures in place
- Management reporting (status, performance, action items)

Document the process-related IT resources particularly affected by the process under review. Confirm the understanding of the process under review, the Key Performance Indicators (KPI) of the process, and the control implications (e.g., by a process walk through).

GENERIC AUDIT GUIDELINE

EVALUATING THE CONTROLS

The audit steps to be performed in assessing the effectiveness of control measures in place or the degree to which the control objective is achieved. Basically deciding what, whether and how to test.

Evaluate the appropriateness of control measures for the process under review by considering identified criteria and industry standard practices, the Critical Success Factors (CSF) of the control measures and applying professional judgment.

- Documented processes exist
- Appropriate deliverables exist
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Conclude the degree to which the control objective is met.

GENERIC AUDIT GUIDELINE

ASSESSING COMPLIANCE

The audit steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously, and to conclude on the appropriateness of the control environment.

Obtain direct or indirect evidence for selected items/periods to ensure that the procedures have been complied with for the period under review using both direct and indirect evidence.

Perform a limited review of the adequacy of the process deliverables.

Determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

GENERIC AUDIT GUIDELINE

SUBSTANTIATING THE RISK

The audit steps to be performed to substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources. The objective is to support the opinion and to "shock" management into action. Auditors have to be creative in finding and presenting this often sensitive and confidential information.

Document the control weaknesses and resulting threats and vulnerabilities.

Identify and document the actual and potential impact (e.g., through root-cause analysis).

Provide comparative information (e.g., through benchmarks).

PO 1 DEFINE A STRATEGIC IT PLAN

CONTROL OBJECTIVES

1 IT as Part of the Organisation’s Long- and Short-Range Plan
2 IT Long-Range Plan
3 IT Long-Range Planning - Approach and Structure
4 IT Long-Range Plan Changes
5 Short-Range Planning for the IT Function
9 Communication of IT Plans
10 Monitoring and Evaluating of IT Plans
11 Assessment of Existing Systems

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

Interviewing:

Chief Executive Officer
Chief Operations Officer
Chief Financial Officer
Chief Information Officer
IT planning/steering committee members
IT senior management and human services staff

Obtaining:

Policies and procedures relating to the planning process

Senior management steering roles and responsibilities

Organisation objectives and long- and short-range plans

IT objectives and long- and short-range plans

Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

Considering whether:

IT function or business enterprise policies and procedures address a structured planning approach

A methodology is in place to formulate and modify the plans and at a minimum, they cover:

- organisation mission and goals
- IT initiatives to support organisation mission and goals
- opportunities for information technology initiatives
- feasibility studies of IT initiatives
- risk assessments of IT initiatives
- optimal investment of current and future IT investments
- re-engineering of IT initiatives to reflect changes in the organisation’s mission and goals
- evaluation of alternative strategies for data applications, technology and organisation

Considering whether, *(continued)*

Organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, in- and out-sourcing, etc. are taken into account and adequately addressed in the planning process

Long- and short-range IT plans exist, are current, adequately address overall enterprise, its mission, and key business functions

IT projects are supported by the appropriate documentation as identified in the information technology planning methodology

Checkpoints exist to ensure that IT objectives and long- and short-range plans continue to meet organisational objectives and long- and short-range plans

Review and sign-off occurs by process owners and senior management of IT plans

The IT plan assesses the existing information systems in terms of degree of business automation, stability, functionality, complexity, costs, strengths and weaknesses.

IT GOVERNANCE INSTITUTE™

Assessing the compliance by:

Testing that:

Minutes from IT planning/steering committee meetings reflect the planning process

Planning methodology deliverables exist and are as prescribed

Relevant IT initiatives are in the long- and short-range plans (i.e., hardware changes, capacity planning, information architecture, new system development or procurement, disaster recovery planning, installation of new processing platforms, etc.)

IT initiatives support long- and short-range plans and consider requirements for research, training, staffing, facilities, hardware and software

Assessing the compliance by:

Testing that: (continued)

Technical implications of IT initiatives have been identified

Consideration has been given to optimising current and future IT investments

IT long- and short-range plans are consistent with the organisation’s long- and short-range plans and organisation requirements

Plans have been changed to reflect changing conditions

IT long-range plans are periodically translated into short-range plans

Tasks exist to implement the plans

Substantiating the risk of control objectives not being met by:

Performing:

Benchmarking of strategic IT plans against similar organisations or appropriate international standards/recognised industry best practices

Detailed review of IT plans to ensure that IT initiatives reflect the organisation’s mission and goals

Detailed review of the IT plans to determine if known areas of weakness within the organisation are being identified for improvement as part of the IT solutions contained in the plans

Identifying:

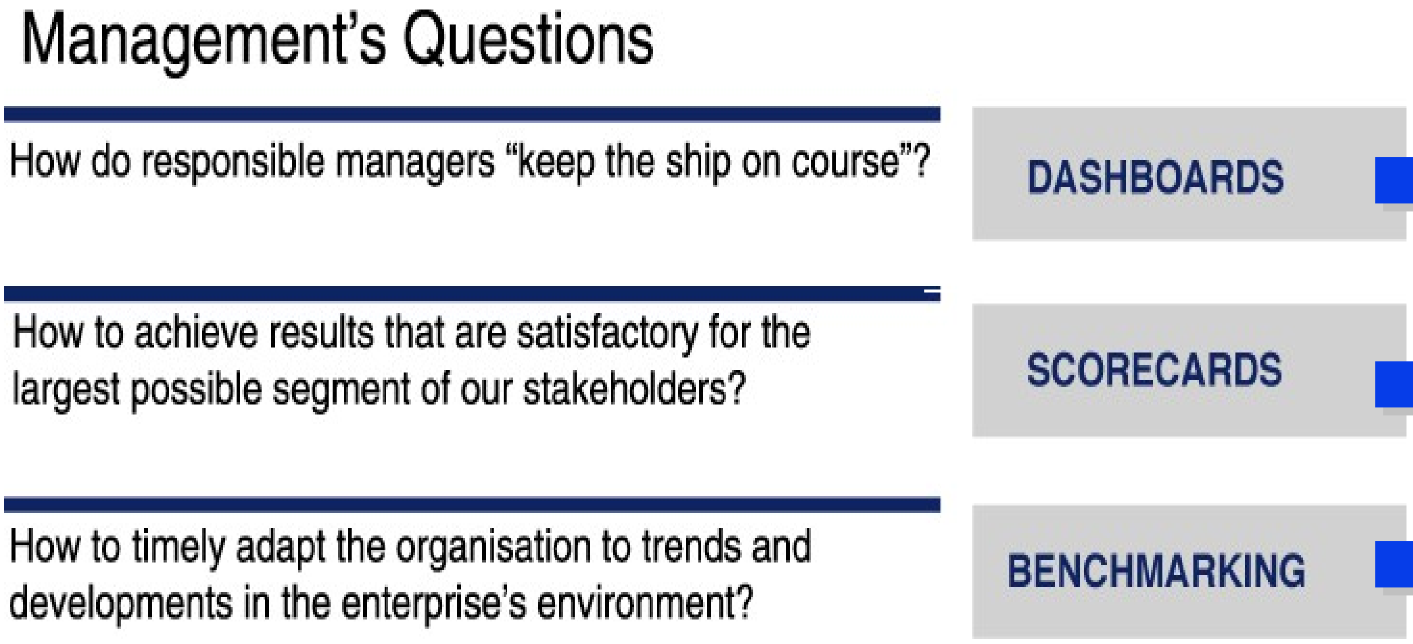
IT failures to meet the organisation's missions and goals
IT failures to match short-range plans with long-range plans
IT projects failures to meet short-range plans
IT failures to meet cost and time guidelines
Missed business opportunities
Missed information technology opportunities

Management Guidelines

* Maturity Models

* Critical Success Factors

* Key Performance Indicators



Management's Questions

How do responsible managers "keep the ship on course"? — DASHBOARDS → Indicators?

How to achieve results that are satisfactory for the largest possible segment of our stakeholders? — SCORECARDS → Measures?

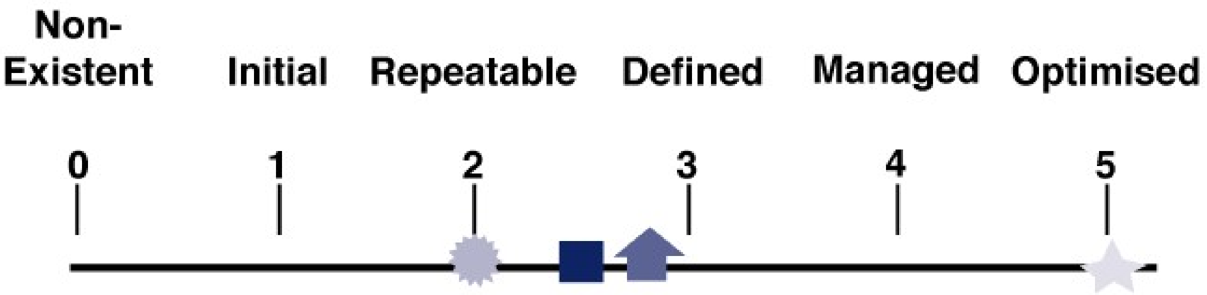
How to timely adapt the organisation to trends and developments in the enterprise's environment? — BENCHMARKING → Scales?

Management Guidelines

- Generic and action oriented
- For the purpose of
  - IT Control profiling – what is important?
  - Awareness – where is the risk?
  - Benchmarking - what do others do?
- Supporting decision making and follow-up
  - Key performance indicators of IT Processes
  - Critical success factors of controls
  - Control implementation choices

IT GOVERNANCE INSTITUTE™

Maturity Models for Self-Assessment



Non-Existent Initial Repeatable Defined Managed Optimised

0 1 2 3 4 5

LEGEND FOR SYMBOLS USED

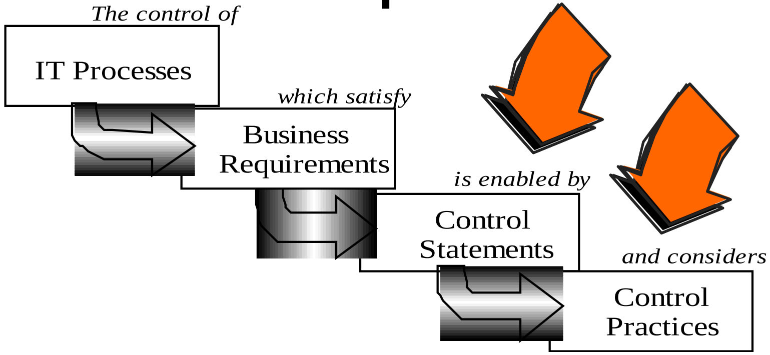
- ✹ Enterprise Current Status
- ■ International Standard Guidelines
- ⬆ Industry Best Practice
- ☆ Enterprise Strategy

LEGEND FOR RANKINGS USED

0	Non-Existent	– Management processes are not applied at all
1	Initial	– Processes are ad hoc and disorganised
2	Repeatable	– Processes follow a regular pattern
3	Defined	– Processes are documented and communicated
4	Managed	– Processes are monitored and measured
5	Optimised	– Best practices are followed and automated

Critical Success Factors

- Management oriented IT control implementation guidance
- Most important things that contribute to the IT process achieving its goal
  - Strategically
  - Technically
  - Organisationally
  - Process or Procedure



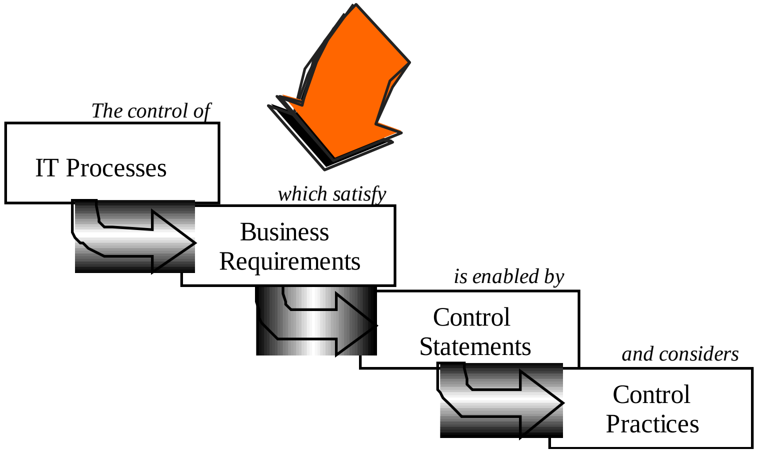
- Control Statement and Considerations of the ‘Waterfall’
- Visible and measurable signs of success
- Short, focussed and action oriented
- Leveraging the resources of primary importance in this process

IT GOVERNANCE INSTITUTE™

Critical Success Factors

- Represent 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
- Are either strategic, technological, organisational or procedural in nature
- Focus on obtaining, maintaining and leveraging capability and skills
- Are expressed in terms of the process, not necessarily the business

Key Goal Indicators

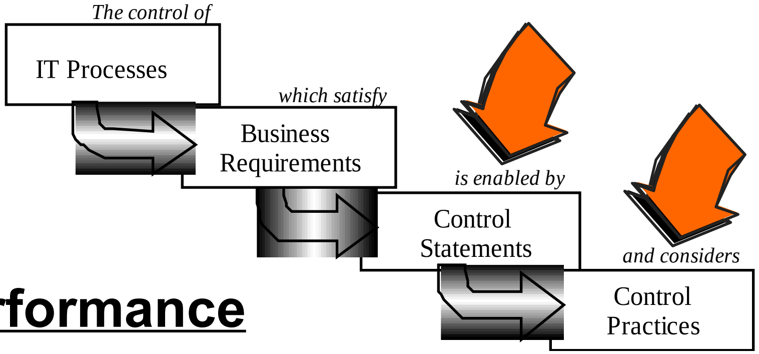


- KGI for goal
  measurable indicators
  of the process achieving
  its goal
- f(Business Requirement of the 'Waterfall')
- Influenced by the primary and secondary information criteria
- A potential source can be found in COBIT's 'Substantiating Risk' section in the Audit Guidelines

Key Goal Indicators

- Describe the outcome of the process and are therefore ‘lag’ indicators, i.e., measurable after the fact
- Are indicators of the success of the process, but may be expressed as well in terms of the business contribution, if that contribution is specific to that IT process
- Focus on the customer and financial dimensions of the balanced business scorecard
- Represent the process goal, i.e., a measure of “what”, a target to achieve
- May describe a measure of the impact of not reaching the process goal
- Are IT oriented, but business driven
- Are expressed in precise measurable terms, wherever possible
- Focus on those information criteria that have been identified to be of most importance for this process

Key Performance Indicators



- **KPI for performance**
  measurable indicators of performance of the enabling factors
- **f(Control Statement and Considerations in 'Waterfall')**
- **How well they leverage/manage the resources needed**

GOVERNANCE INSTITUTE™

Key Performance Indicators

- Are a measure of “how well” the process is performing
- Predict the probability of success or failure in the future, i.e., is a ‘LEAD’ indicator
- Are process oriented, but IT driven
- Focus on the process and learning dimensions of the balanced scorecard
- Are expressed in precise, measurable terms
- Help in improving the IT process

Why Should an Organisation 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
- Self-assessment, Performance Measurement and Benchmarking Capabilities

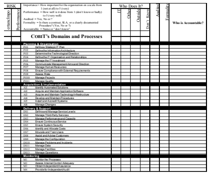
IT GOVERNANCE INSTITUTE™

COBIT Management Awareness Diagnostic Tools

One of the most challenging tasks will be getting top management’s attention. Two tools for getting management’s attention and raising management’s awareness are:

- IT Governance Self-Assessment
- Management’s IT Concerns Diagnostic

IT Governance Self-Assessment



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)

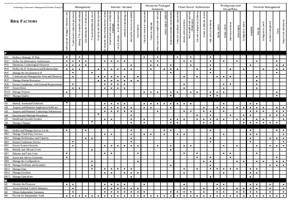
Audited = Yes, No or ?

Formality = Is there a contract, SLA, or a clearly documented Procedure? (Yes, No or ?)

Accountable = Name or "don't know"

RISK		COBIT's Domains and Processes		Who Does It?						
ertanc Impo	Performance			IT	Othe	Outsid	Don't Know	Audited	Formality	Who is Accountable?
		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								
		AI1	Identify Automated Solutions							
		AI2	Acquire and Maintain Application Software							
		AI3	Acquire and Maintain Technology Infrastructure							
		AI4	Develop and Maintain Procedures							
		AI5	Install and Accredit Systems							
		AI6	Manage Changes							
		Delivery & Support								
		DS1	Define and Manage Service Levels							
		DS2	Manage Third-Party Services							
		DS3	Manage Performance and Capacity							
		DS4	Ensure Continuous Service							
		DS5	Ensure System 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							
		Monitoring								
		M1	Monitor the Processes							
		M2	Assess Internal Control Adequacy							
		M3	Obtain Independent Assurance							
		M4	Provide for Independent Audit							

Management’s IT Concerns Diagnostic



Technology Concerns to Management (Gartner Group) ➔		Management						Internet / Intranet						Enterprise Packaged Solutions					Client/Server Architecture						Workgroups and GroupWare					Network Management					
RISK FACTORS		with business strategy IT initiatives in line	IT policies and corporate governance	Utilising IT for competitive advantage	Consolidating the IT infrastructure	IT ownership/Reducing cost of	Acquiring and developing skills	to corporate network/Unauthorised access	Unauthorised access to confidential messages	Loss of integrity – corporate transactions	confidential data Leakage of	Interruption to service availability	Virus Infection	Failure to meet user requirements	Failure to integrate	infrastructure Not compatible with technical	Vendor support problems	Expensive/complex implementation	Failure to coordinate requirements	Access control problems	Not compatible with technical infrastructure	End user management problems	Control of software versions	High costs of ownership	Quality control	Access control	Informal procedures	Data integrity	Configuration control	Availability	Security	Configuration control	Incident management	Costs	Support and maintenance
P																																			
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 Investment in IT		●			●												●						●										●	
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																	●						●	●									●	
A																																			
AI1	Identify Automated Solutions	●						●	●	●	●			●	●	●	●	●	●	●	●					●				●	●				
AI2	Acquire and Maintain Application Software							●	●	●	●	●		●	●			●					●		●	●		●	●	●	●	●		●	●
AI3	Acquire and Maintain Technology Infrastructur							●	●	●	●	●				●				●	●		●	●		●				●	●	●		●	●
AI4	Develop and Maintain Procedures						●					●										●		●			●		●	●			●	●	●
AI5	Install and Accredit Systems							●	●			●		●				●	●	●		●	●	●	●	●		●	●		●	●			●
AI6	Manage Changes					●						●		●				●	●				●	●					●	●	●	●	●	●	
D																																			
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											●												●						●					
M																																			
M1	Monitor the Processes	●	●					●	●	●	●			●						●					●	●				●	●		●		●
M2	Assess Internal Control Adequacy		●					●	●	●	●	●	●							●			●		●	●		●	●	●	●		●		●
M3	Obtain Independent Assurance		●					●	●	●	●	●	●	●				●	●	●	●		●		●	●		●	●	●	●		●		●
M4	Provide for Independent Audit	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

How To Implement COBIT in an Organisation

- Top Down Approach
- Audit Committee Approach
- Audit and IT Management Consensus Approach
- Regulation/Legislation

GOVERNANCE INSTITUTE™

Introduction Within an Organisation

- One-hour *Orientation* Session to Management
- More Extensive Training for Hands-on Users
- Implementation Action Plan
- Implementation Kick-off Memorandum
- Roll-out
- Monitor/Report on Progress

IT GOVERNANCE INSTITUTE™

Risk Assessment and Audit Planning Using COBIT

- Prior Audit Work Form
- Entity Short Form
- Entity Long Form
- Risk Assessment Form
- Responsible Party Form
- Contract Service/Service Level Agreement Form

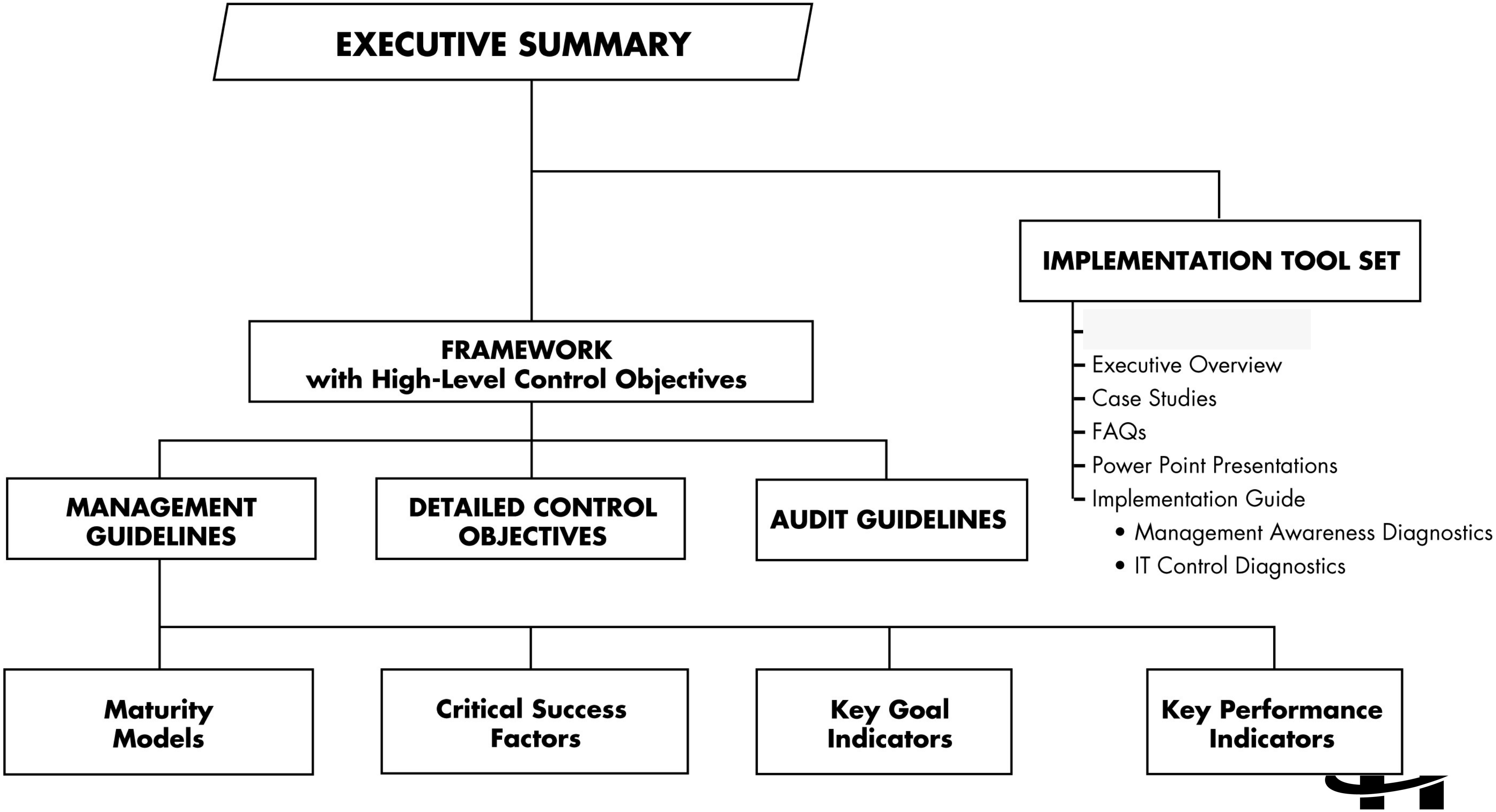
IT GOVERNANCE INSTITUTE™

COBIT

a living standard

IT GOVERNANCE INSTITUTE™

COBIT Family of Products



EXECUTIVE SUMMARY

FRAMEWORK
with High-Level Control Objectives

MANAGEMENT GUIDELINES

DETAILED CONTROL OBJECTIVES

AUDIT GUIDELINES

Maturity Models

Critical Success Factors

Key Goal Indicators

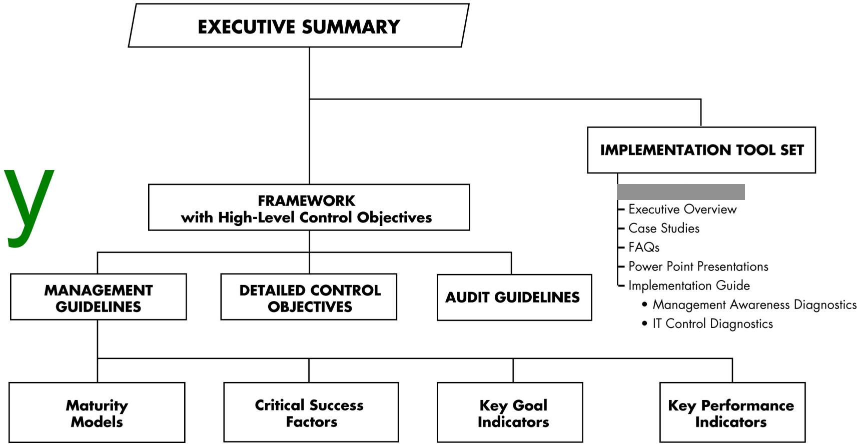
Key Performance Indicators

IMPLEMENTATION TOOL SET

- Executive Overview
- Case Studies
- FAQs
- Power Point Presentations
- Implementation Guide
  - Management Awareness Diagnostics
  - IT Control Diagnostics

COBIT Product Family

COBIT Family of Products



Six Major Elements

- COBIT as an **open standard** for increased world-wide adoption, consisting of the **Executive Summary, Framework, Detailed Control Objectives, Management Guidelines and Implementation Tool Set**
- **Audit Guidelines** : how to audit against the standard

COBIT

Questions and Answers

COBIT

For additional information -

www.isaca.org

www.itgi.org

the end

GOVERNANCE INSTITUTE™