



Impacto de Cobit 4.0 sobre el negocio

Manuel Ballester, José Ángel Peña
Madrid, España, Monterrey, México



Temario

1. Introducción
2. Secciones Cobit 4.0
3. Contenido por proceso
4. Relación con objetivos de empresa y estándares



- **CobiT fue desarrollado en 1992**
- **En el 2000 se publicó la tercera versión**
- **Cobit 4.0 a fines del 2005**

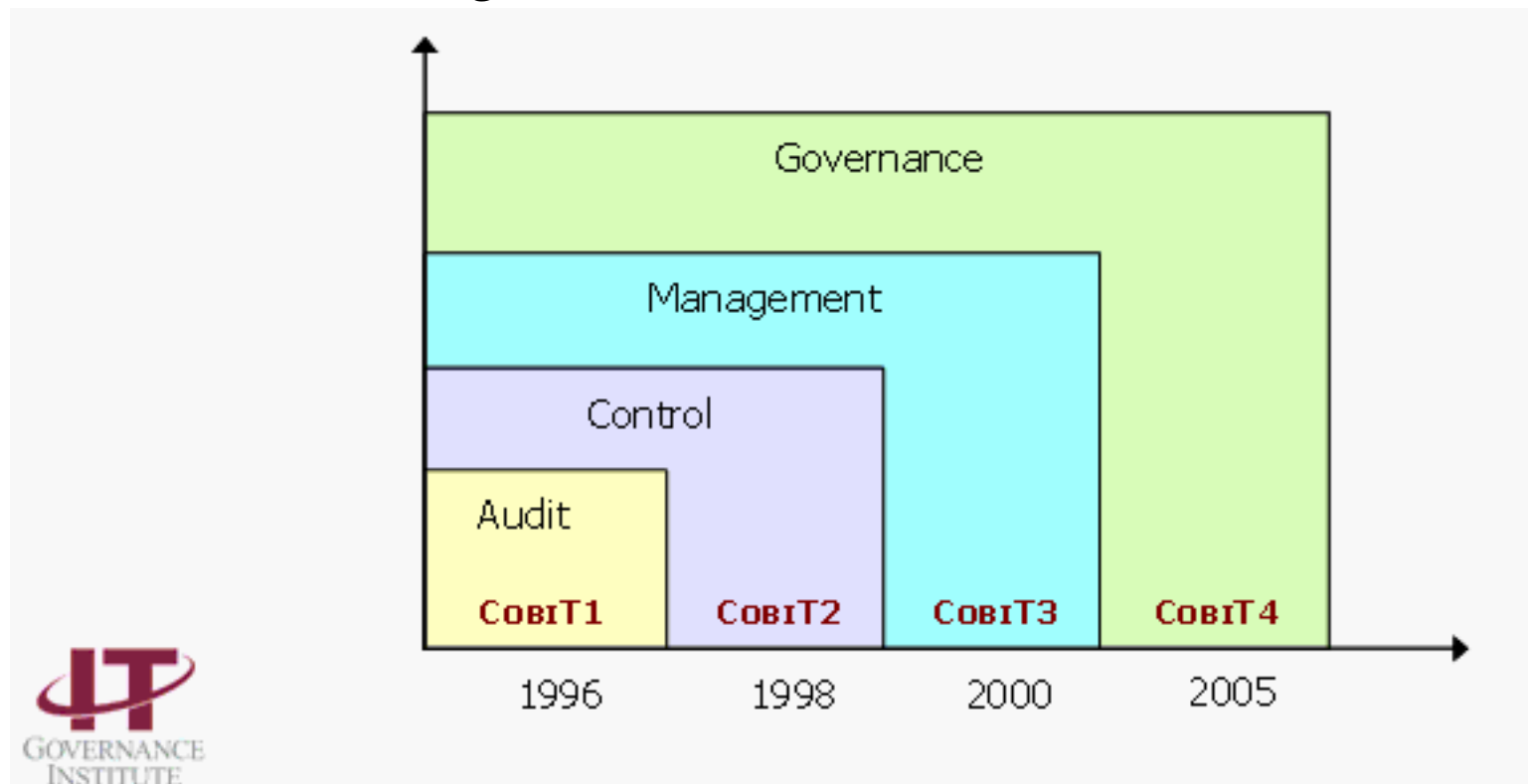




El ámbito de negocios ha cambiado desde 1992:

- **Fuerte dependencia de TI en los procesos de negocio críticos.**
- **Se ha incrementado el foco en la administración de valor, riesgos y costos de TI**
- **Mayor preocupación por el gobierno corporativo.**
- **Los estándares de TI han madurado.**
- **La regulación ha crecido**

En respuesta a esos cambios, CobiT ha evolucionado de ser una herramienta de auditoría a ser un marco de referencia de gobierno de TI.

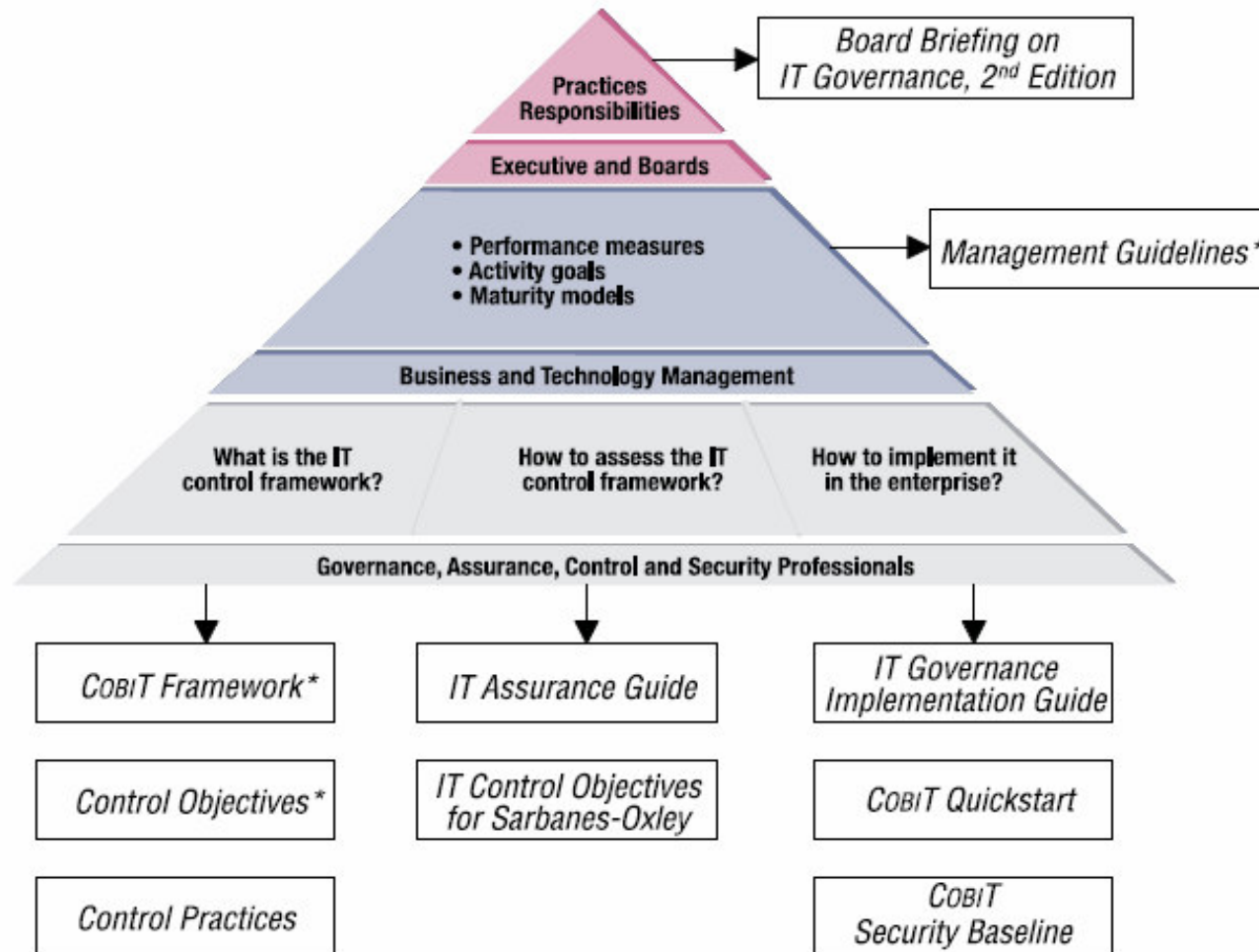




Enfoque de CobiT 4.0

- **En gobierno de TI.**
- **Armonización con otros estándares.**
- **Flujo de procesos.**
- **Lenguaje más conciso y orientado a la acción.**

Productos CobiT



* Now integrated into COBIT 4.0



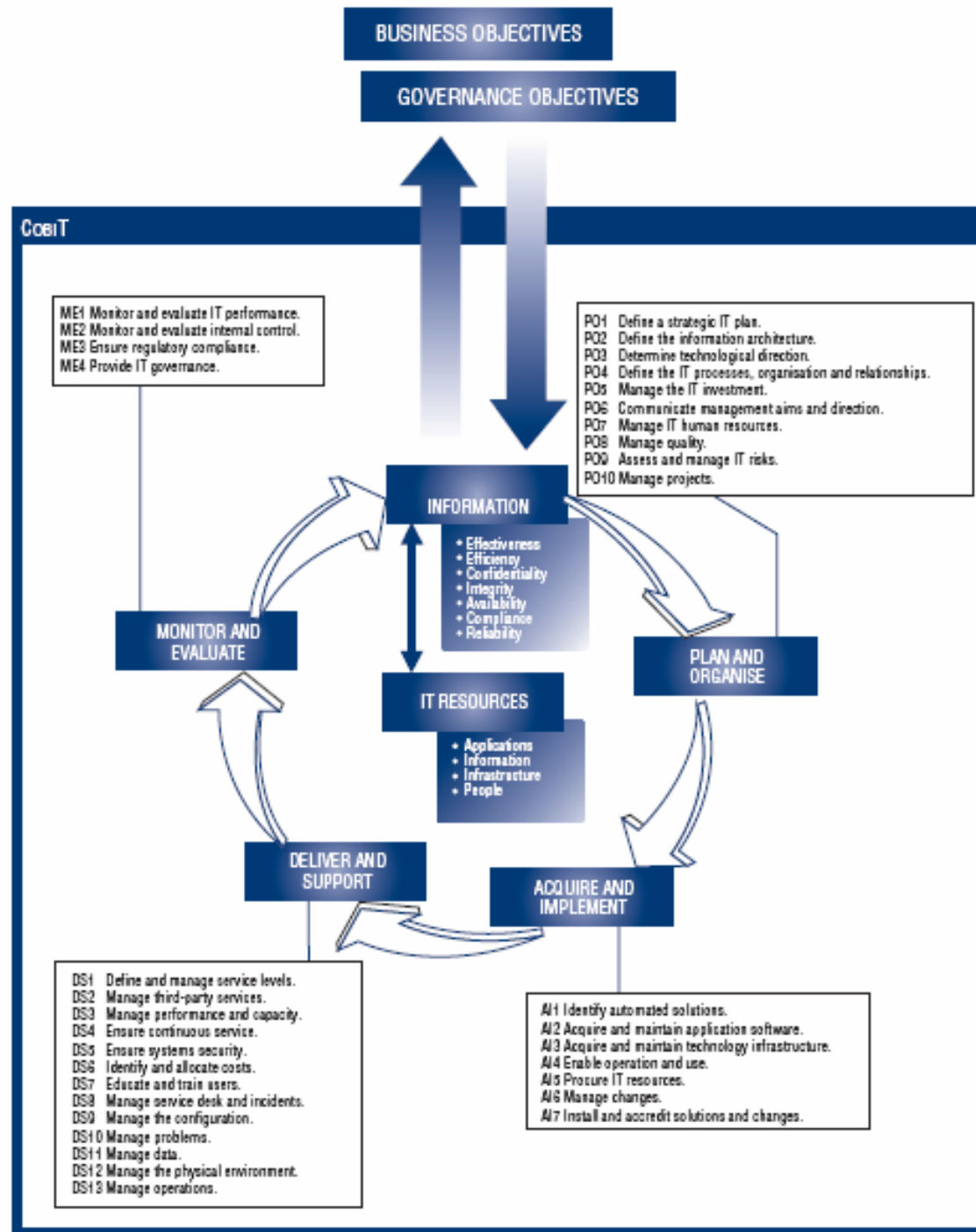
Principales novedades

- **Framework, Objetivos de Control y Management Guidelines integrados en un libro.**
- **30 % menos objetivos de control.**
- **Objetivos genéricos en el framework.**
- **Cada proceso tiene una descripción de los principales objetivos y actividades.**



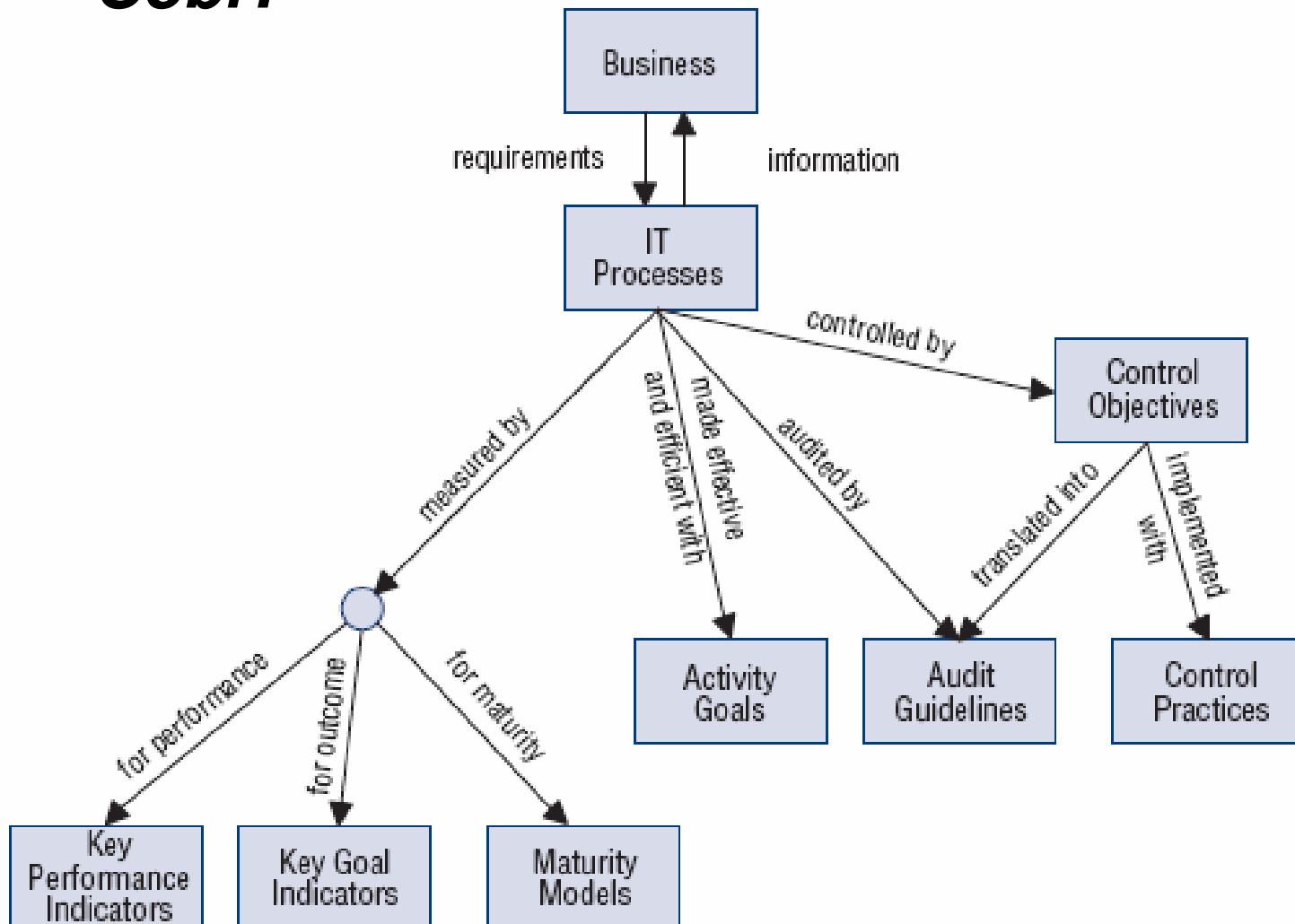
CobiT 4.0 tiene 4 secciones:

- 1. Resumen ejecutivo.**
- 2. Framework.**
- 3. Contenido central: Objetivos de control, guías de administración y modelos de madurez.**
- 4. Apéndices**

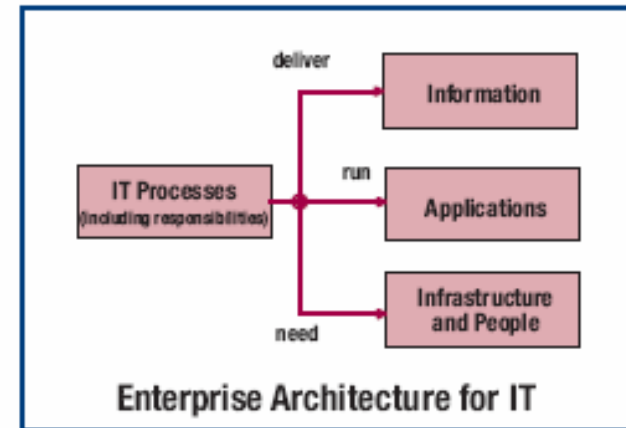
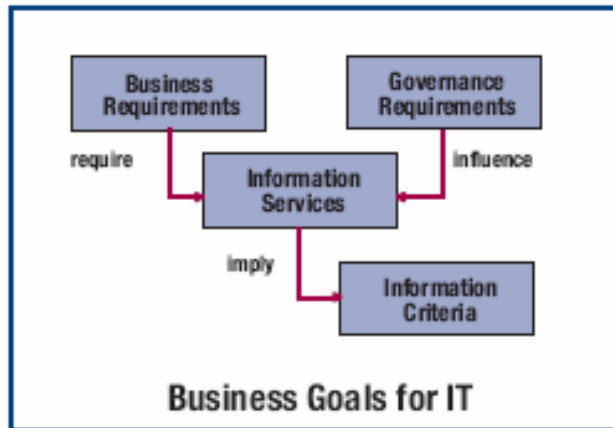
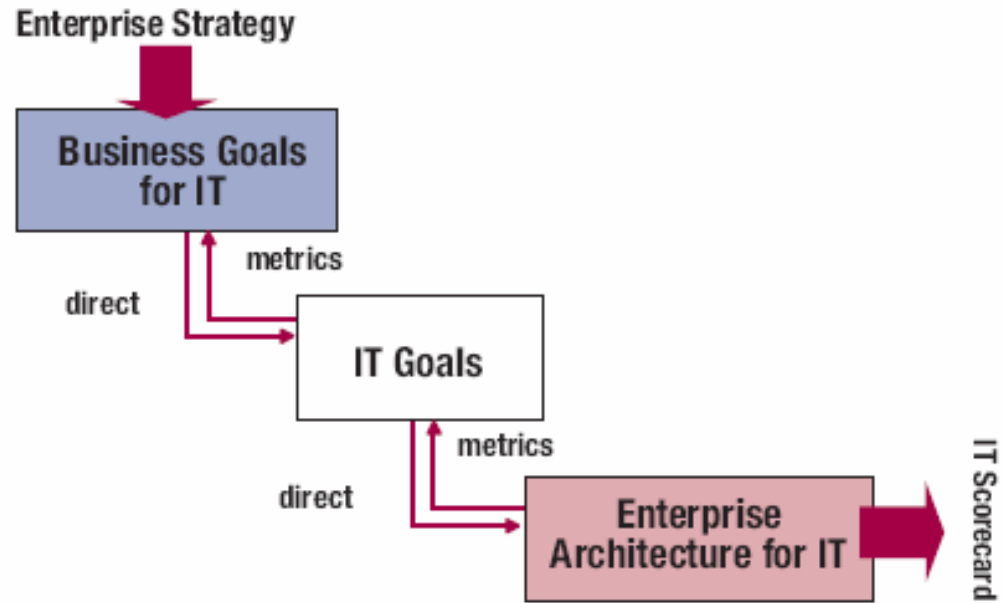


- 4 dominios
- 34 procesos

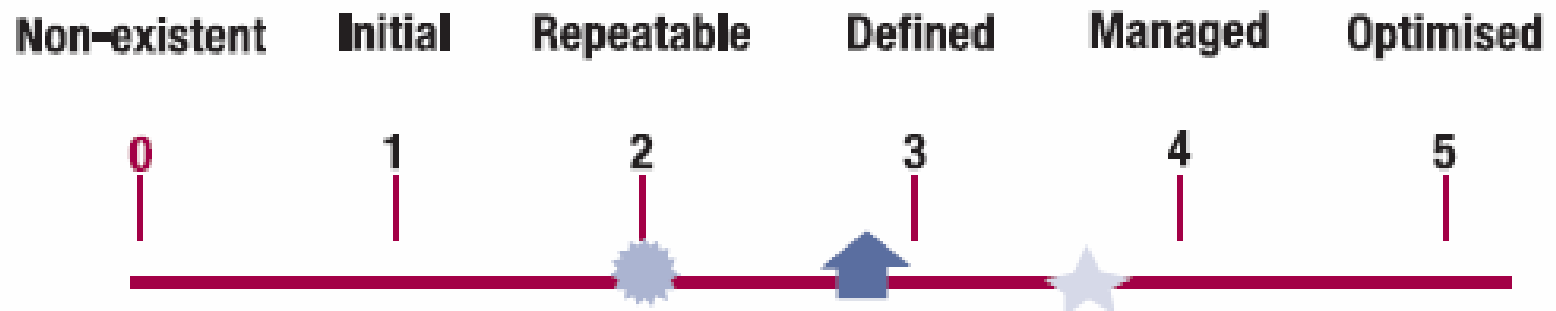
Interrelación de los componentes de CobiT



IT Goals – Enterprise Architecture



Modelo de madurez



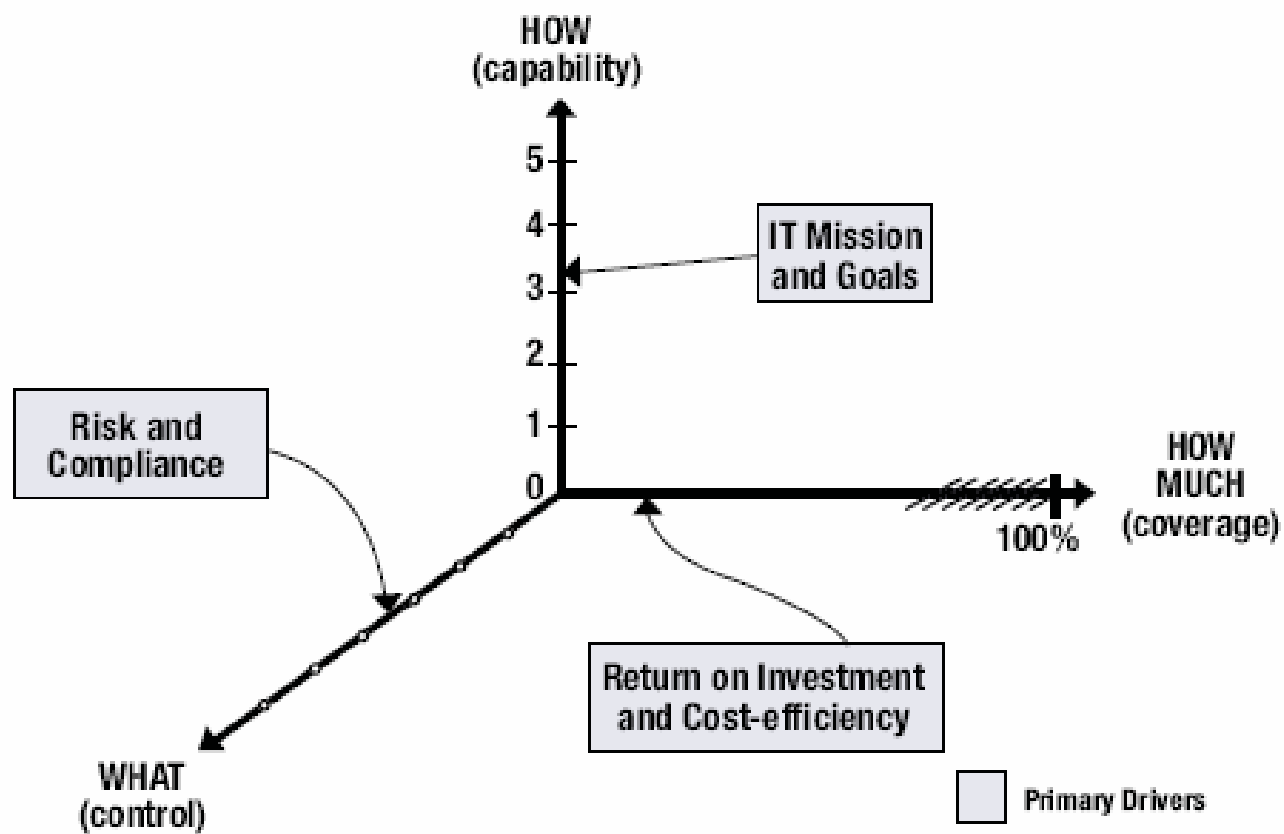
LEGEND FOR SYMBOLS USED

-  Enterprise current status
-  Industry average
-  Enterprise target

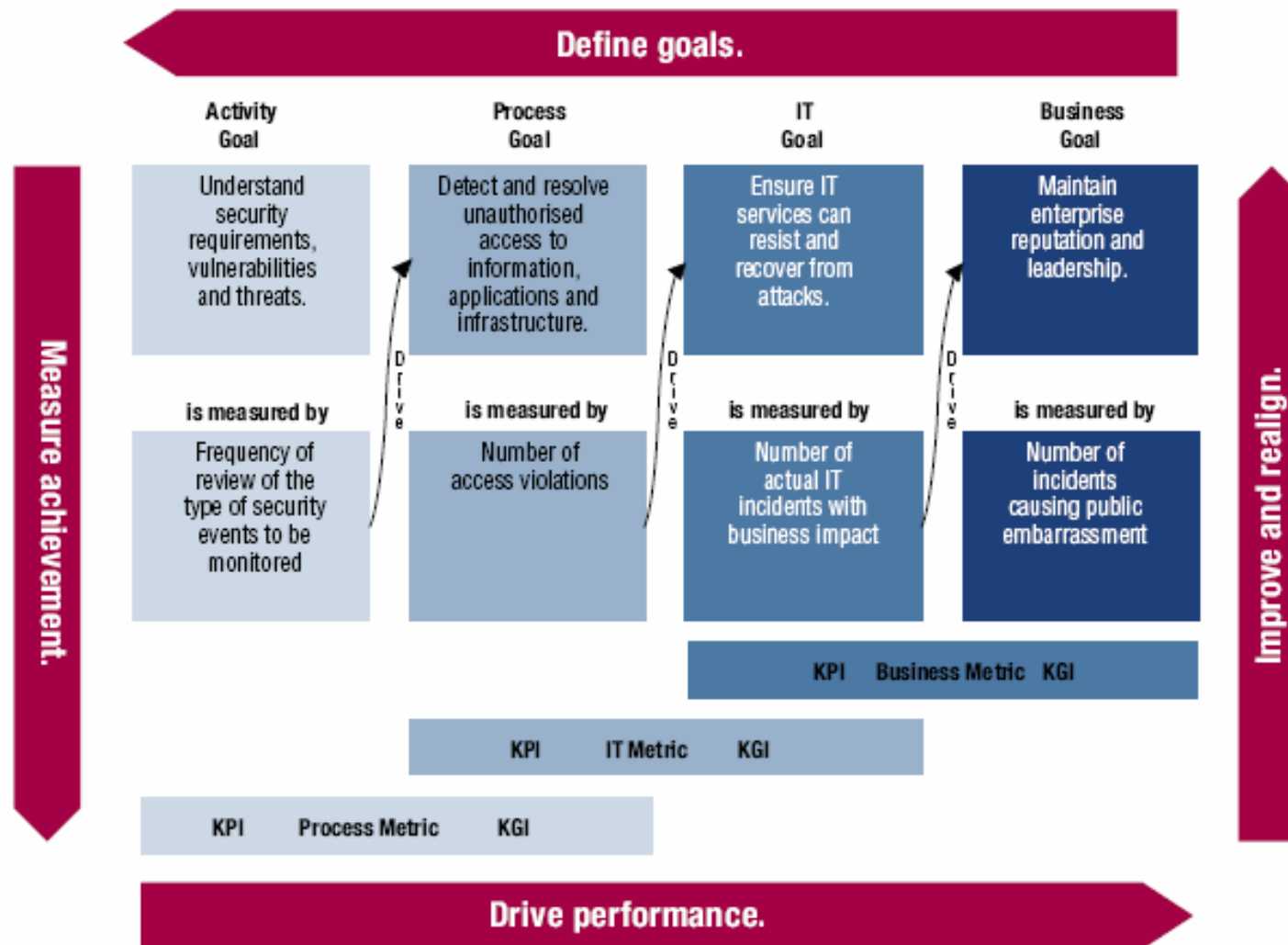
LEGEND FOR RANKINGS USED

- 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—Good practices are followed and automated.

Tres dimensiones de madurez



Relación entre procesos, metas y métricas.



Áreas de enfoque

	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

Controles genéricos de procesos

PC1 Process Owner

Assign an owner for each COBIT process such that responsibility is clear.

PC2 Repeatability

Define each COBIT process such that it is repeatable.

PC3 Goals and Objectives

Establish clear goals and objectives for each COBIT process for effective execution.

PC4 Roles and Responsibilities

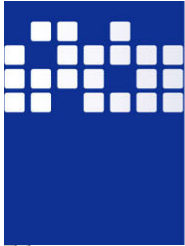
Define unambiguous roles, activities and responsibilities for each COBIT process for efficient execution.

PC5 Process Performance

Measure the performance of each COBIT process against its goals.

PC6 Policy, Plans and Procedures

Document, review, keep up to date, sign off on and communicate to all involved parties any policy, plan or procedure that drives a COBIT process.



Controles de aplicación

Data Origination/Authorisation Controls

AC1 Data Preparation Procedures

Data preparation procedures are in place and followed by user departments. In this context, input form design helps ensure that errors and omissions are minimised. Error-handling procedures during data origination reasonably ensure that errors and irregularities are detected, reported and corrected.

AC2 Source Document Authorisation Procedures

Authorised personnel who are acting within their authority properly prepare source documents and an adequate segregation of duties is in place regarding the origination and approval of source documents.

AC3 Source Document Data Collection

Procedures ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.

AC4 Source Document Error Handling

Error-handling procedures during data origination reasonably ensure detection, reporting and correction of errors and irregularities.

AC5 Source Document Retention

Procedures are in place to ensure original source documents are retained or are reproducible by the organisation for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.

Data Input Controls

AC6 Data Input Authorisation Procedures

Procedures ensure that only authorised staff members perform data input.

AC7 Accuracy, Completeness and Authorisation Checks

Transaction data entered for processing (people-generated, system-generated or interfaced inputs) are subject to a variety of control to check for accuracy, completeness and validity. Procedures also assure that input data are validated and edited as close to the point



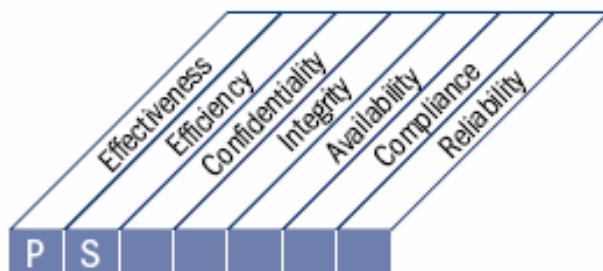
Cada proceso tiene 4 secciones

- 1. Objetivo de control de alto nivel.**
- 2. Objetivos de control detallado.**
- 3. Guías de administración.**
- 4. Modelo de madurez del proceso.**

HIGH-LEVEL CONTROL OBJECTIVE

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.



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

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

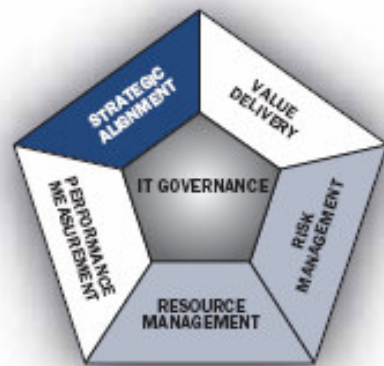
incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

is achieved by

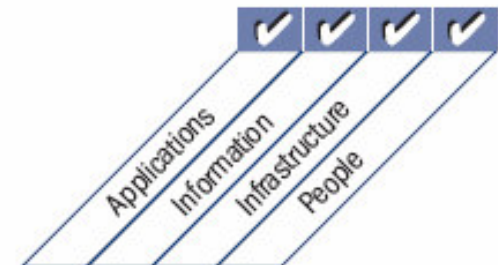
- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

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



■ Primary ■ Secondary



PO1 Plan and Organise

Define a Strategic IT Plan

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

P01 Define a Strategic IT Plan

From	Inputs
P05	Cost/benefits reports
P09	Risk assessment
P010	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	P02...P06	P08	P09	AI1	DS1	
Tactical IT plan	P02...P06	P09	AI1	DS1		
IT project portfolio	P05	P06	P010	AI6		
IT service portfolio	P05	P06	P09	DS1		
IT sourcing strategy	DS2					
IT acquisition strategy	AI5					

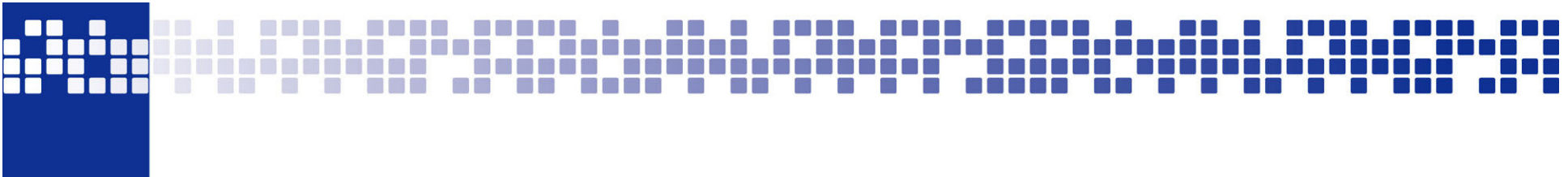
RACI Chart

Functions

Activities

	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
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 Responsible, Accountable, Consulted and/or Informed.



Goals and Metrics

Activity Goals

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

Process Goals

- Define how business requirements are translated in service offerings.
- Define the strategy to deliver service offerings.
- Contribute to the management of the portfolio of IT-enabled business investments.
- Establish clarity of business impact of risks to IT objectives and resources.
- Provide transparency and understanding of IT costs, benefits, strategy, policies and service levels.

IT Goals

- Respond to business requirements in alignment with the business strategy.
- Respond to governance requirements in line with board direction.

are measured by

Key Performance Indicators

- Delay between updates of business strategic/tactical plan and updates of IT strategic/tactical plan
- % of strategic/tactical IT plan meetings where business representatives have actively participated
- Delay between updates of IT strategic plan and updates of IT tactical plans
- % of tactical IT plans complying with the predefined structure/contents of those plans
- % of IT initiatives/projects championed by business owners

are measured by

Process Key Goal Indicators

- % of IT objectives in the IT strategic plan that support the strategic business plan
- % of IT initiatives in the IT tactical plan that support the tactical business plan
- % of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plan

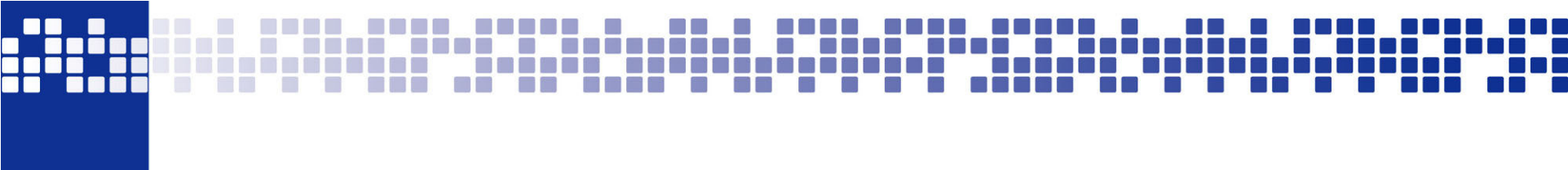
are measured by

IT Key Goal Indicators

- Degree of approval of business owners of the IT strategic/tactical plans
- Degree of compliance with business and governance requirements
- Level of satisfaction of the business with the current state (number, scope, etc.) of the project and applications portfolio

Drive

Drive



PO1 Plan and Organise

Define a Strategic IT Plan

MATURITY MODEL

P01 Define a Strategic IT Plan

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:

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

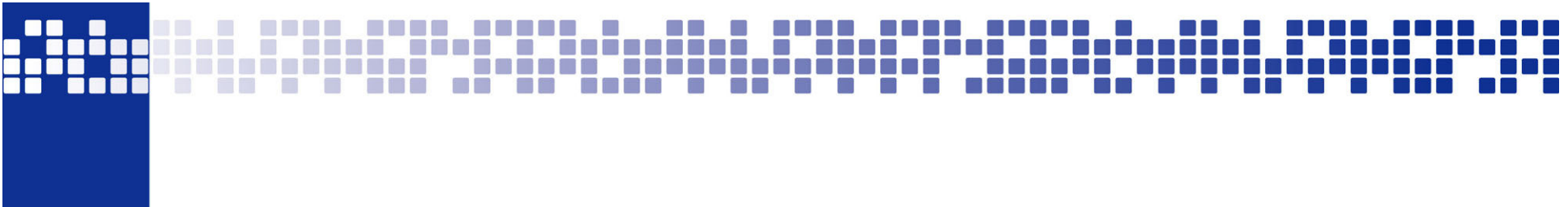
The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes 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



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.





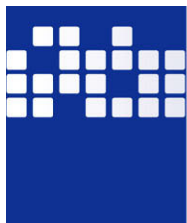
Interrelaciones

A P P E N D I X I

L I N K I N G B U S I N E S S G O A L S A N D I T G O A L S

This appendix provides a global view of how generic business goals relate to IT goals, the IT processes and information criteria. There are three tables:

1. The first table maps the business goals, organised according to a balanced scorecard, to the IT goals and information criteria. This helps show, for a given generic business goal, the IT goals that typically support this goal and the CoBIT information criteria that relate to the business goal.
2. The second table maps the IT goals to CoBIT's IT processes and the information criteria on which the IT goal is based.
3. The third table provides a reverse mapping showing for each IT process the IT goals that are supported.



APPENDIX II

MAPPING IT PROCESSES TO IT GOVERNANCE FOCUS AREAS, COSO, COBIT IT RESOURCES AND COBIT INFORMATION CRITERIA

This appendix provides a mapping between the CoBIT IT processes and the five IT governance focus areas, the components of COSO, IT resources and the information criteria. The table also provides a relative importance indicator (high, medium and low) based on benchmarking via CoBIT Online. This matrix demonstrates on one page and at a high level how the CoBIT framework addresses IT governance and COSO requirements, and shows the relationship between IT processes and the IT resources and information criteria. P is used when there is a primary relation and S when there is only a secondary relation. No P or S does not mean that there is no relation, only that it is less important, or marginal. The importance values are based on a survey and the opinions of experts, and are provided only as a guide. Users should consider what processes are important within their own organisations.



APPENDIX III

MATURITY MODEL FOR INTERNAL CONTROL

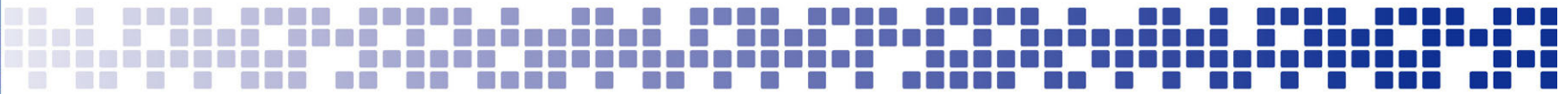
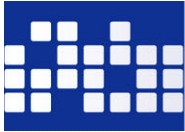
This appendix provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimised level. The model provides a high-level guide to help CoBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.



APPENDIX IV

COBIT 4.0 PRIMARY REFERENCE MATERIAL





COBIT 4.0 PRIMARY REFERENCE MATERIAL

For the earlier COBIT development and updating activities, a broad base of more than 40 international detailed IT standards, frameworks, guidelines and best practices was used to ensure the completeness of COBIT in addressing all areas of IT governance and control.

Because COBIT is focused on *what* is required to achieve adequate management and control of IT, it is positioned at a high level. The more detailed IT standards and best practices are at a lower level of detail describing *how* to manage and control specific aspects of IT. COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements.

For this COBIT update (COBIT 4.0), six of the major global IT-related standards, frameworks and practices were focused on as the major supporting references to ensure appropriate coverage, consistency and alignment. These are:

- Committee of Sponsoring Organisations of the Treadway Commission (COSO):

Internal Control—Integrated Framework, 1994

Enterprise Risk Management—Integrated Framework, 2004

- Office of Government Commerce (OGC®):

IT Infrastructure Library® (ITIL®), 1999-2004

- International Organisation for Standardisation:

ISO/IEC 17799:2005, Code of Practice for Information Security Management

- Software Engineering Institute (SEI®):

SEI Capability Maturity Model (CMM®), 1993

SEI Capability Maturity Model Integration (CMMI®), 2000

- Project Management Institute (PMI®):

Project Management Body of Knowledge (PMBOK®), 2000

- Information Security Forum (ISF):

The Standard of Good Practice for Information Security, 2003

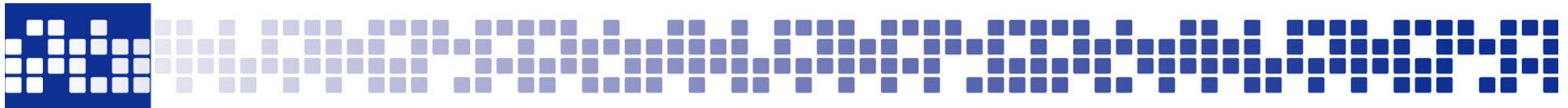




A P P E N D I X V

C R O S S - R E F E R E N C E S B E T W E E N C O B I T 3^{R D} E D I T I O N A N D C O B I T 4 . 0





Cross-reference: COBIT 3rd Edition to COBIT 4.0

COBIT 3 rd Edition	COBIT 4.0
P01 Define a strategic IT plan.	
1.1 IT as part of the organisation's long-and short-range plan	1.4
1.2 IT long-range plan	1.4
1.3 IT long-range planning —approach and structure	1.4
1.4 IT long-range plan changes	1.4
1.5 Short-range planning for the IT function	1.5
1.6 Communication of IT plans	1.4
1.7 Monitoring and evaluating of IT plans	1.3
1.8 Assessment of existing systems	1.3
P02 Define the information architecture.	
2.1 Information architecture model	2.1
2.2 Corporate data dictionary and data syntax rules	2.2

COBIT 3 rd Edition	COBIT 4.0
2.3 Data classification scheme	2.3
2.4 Security levels	2.3
P03 Determine technological direction.	
3.1 Technological infrastructure planning	3.1
3.2 Monitor future trends and regulations.	3.3
3.3 Technological infrastructure contingency	3.1
3.4 Hardware and software acquisition plans	3.1, AI3.1
3.5 Technology standards	3.4, 3.5
P04 Define the IT organisation and relationships.	
4.1 IT planning or steering committee	4.3
4.2 Organisational placement of the IT function	4.4
4.3 Review of organisational achievements	4.5
4.4 Roles and responsibilities	4.6

COBIT 3 rd Edition	COBIT 4.0
4.5 Responsibility for quality assurance	4.7
4.6 Responsibility for logical and physical security	4.8
4.7 Ownership and custodianship	4.9
4.8 Data and system ownership	4.9
4.9 Supervision	4.10
4.10 Segregation of duties	4.11
4.11 IT staffing	4.12
4.12 Job or position descriptions for IT staff	4.6
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
P05 Manage the IT investment.	
5.1 Annual IT operating budget	5.3
5.2 Cost and benefit monitoring	5.4



Cross-reference: COBIT 4.0 to COBIT 3rd Edition

COBIT 4.0	COBIT 3 rd Edition
P01 Define a strategic IT plan.	
1.1 IT value management	5.3
1.2 Business-IT alignment	New
1.3 Assessment of current performance	1.7, 1.8
1.4 IT strategic plan	1.1, 1.2, 1.3, 1.4, 1.6
1.5 IT tactical plans	1.5
1.6 IT portfolio management	New
P02 Define the information architecture.	
2.1 Enterprise information architecture model	2.1
2.2 Enterprise data dictionary and data syntax rules	2.2
2.3 Data classification scheme	2.3, 2.4
2.4 Integrity management	New
P03 Determine technological direction.	
3.1 Technological direction planning	3.1, 3.3, 3.4
3.2 Technological infrastructure plan	New
3.3 Monitoring of future trends and regulations	3.2

COBIT 4.0	COBIT 3 rd Edition
4.12 IT staffing	4.11
4.13 Key IT personnel	4.13
4.14 Contracted staff policies and procedures	4.14
4.15 Relationships	4.15
P05 Manage the IT investment.	
5.1 Financial management framework	New
5.2 Prioritisation within IT budget	New
5.3 IT budgeting process	5.1, 5.3
5.4 Cost management	5.2, 5.3
5.5 Benefit management	5.3
P06 Communicate management aims and direction.	
6.1 IT policy and control environment	6.1
6.2 Enterprise IT control framework	6.8
6.3 IT policies management	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Policy rollout	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11

COBIT 4.0	COBIT 3 rd Edition
8.2 IT standards and quality practices	11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.16, 11.17, 11.19
8.3 Development and acquisition standards	11.5, 11.6, 11.7
8.4 Customer focus	New
8.5 Continuous improvement	New
8.6 Quality measurement, monitoring and review	11.18
P09 Assess and manage IT risks.	
9.1 IT and business risk management alignment	9.1, 9.4
9.2 Establishment of risk context	9.1, 9.4
9.3 Event identification	9.3, 9.4
9.4 Risk assessment	9.1, 9.2, 9.4
9.5 Risk response	9.5, 9.6
9.6 Maintenance and monitoring of a risk action plan	New
P010 Manage projects.	
10.1 Programme management framework	New
10.2 Project management	10.1





APPENDIX VI

APPROACH TO RESEARCH AND DEVELOPMENT

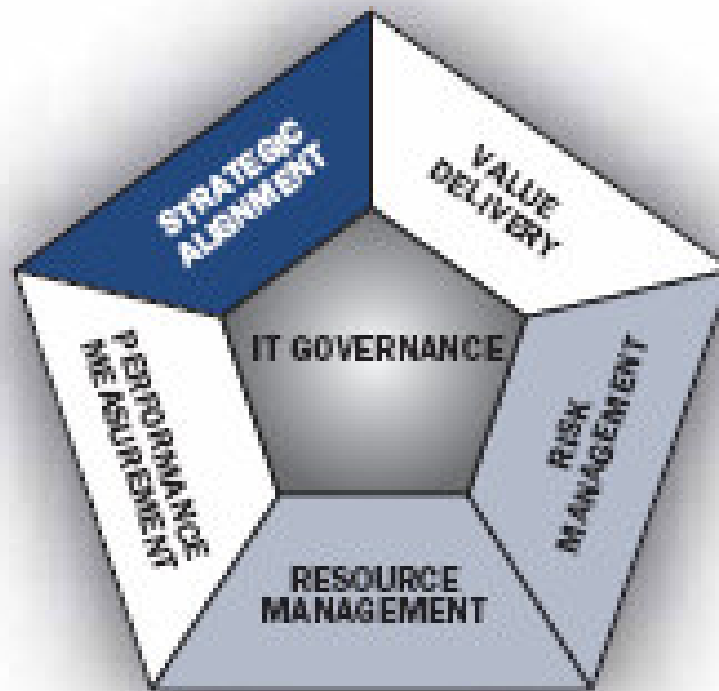




APPENDIX VII

GLOSSARY





■ Primary ■ Secondary



Resumen de cambios en procesos

Still 4 Domains and 34 Processes

- PO8 Ensure Compliance is now a new ME process
- New AI5 Procure IT Resources process
- Old AI5 plus release aspects of AI6 now AI7, aligned with ITIL
- DS8 and DS10 now aligned with ITIL
- DS11 now only addresses Data Management - *Application Controls now explained and listed in the Framework*
- New ME processes only covering IT responsibilities:
 - ME1 Monitor and evaluate IT Performance
 - ME2 Monitor and evaluate Internal Control
 - ME3 Ensure Regulatory Compliance
 - ME4 Provide IT Governance
- Resources reduced to four (People, Information, Applications, Infrastructure) and together with IT Goals and Processes form a simple enterprise architecture model



¡Gracias!

Manuel Ballester

mballester@temanova.com

José Ángel Peña Ibarra

japi@ccisa.com.mx