

IDT

Institute of Law
and Technology

UAB



IAITG

INSTITUTE
OF AUDIT &
IT-GOVERNANCE

IT-GOVERNANCE

Strategy, Management and Measurement

Antoni Bosch-Pujol, CISA, CISM

Director Institute Audit & IT-Governance (IAITG)

Director IT-Governance (IDT-UAB)

President ISACA-Barcelona

antoni.bosch@uab.es

<http://idt.uab.es>

www.isacabcn.org

www.eae.es

IT-GOVERNANCE

- **IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.**

(Font IT Governance Institute Cobit 4.0, USA 2005)

- **IT governance: Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT.**

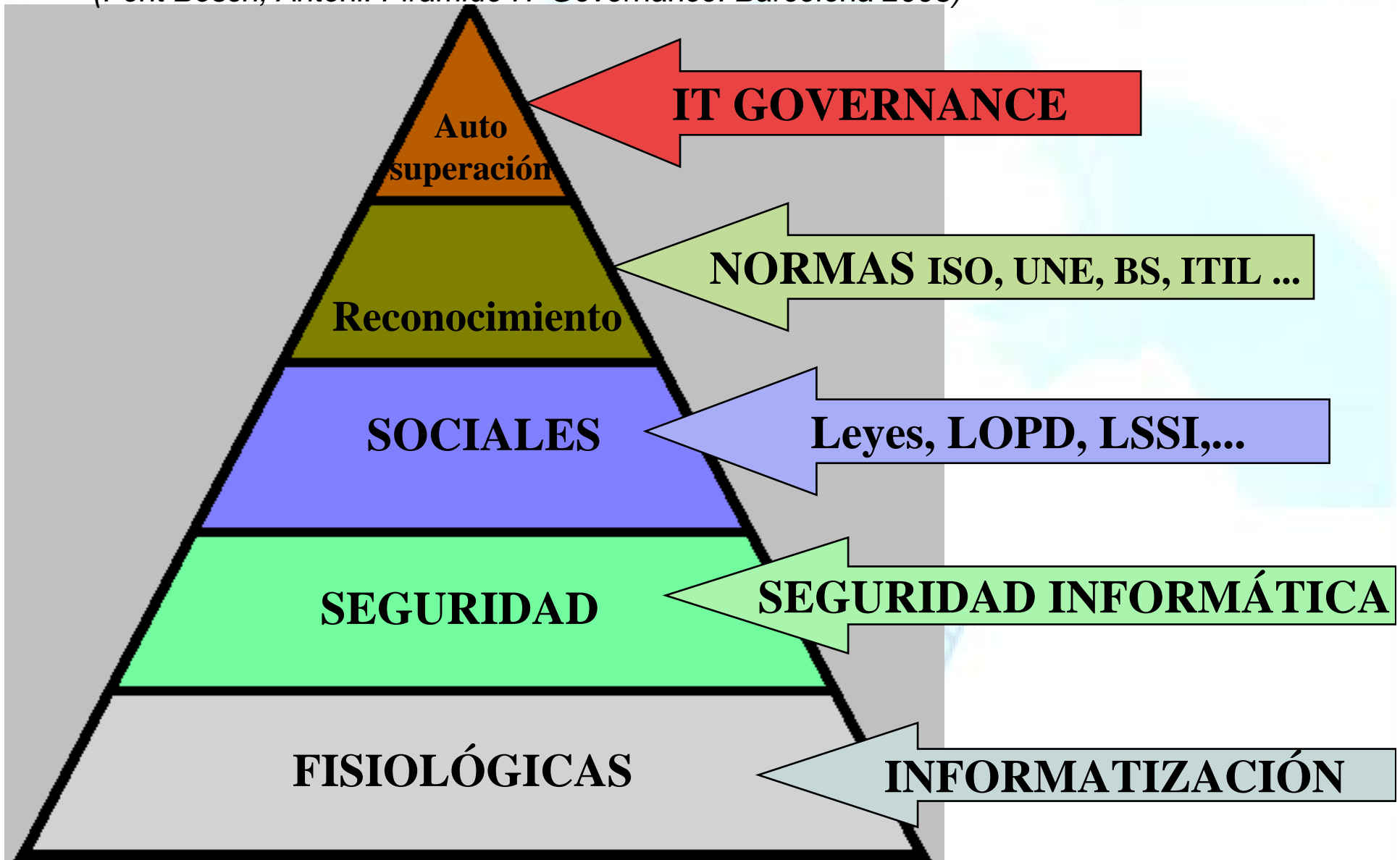
(Font Weill & Ross. IT-Governance. HBSP,2004)

- **IT governance: The system by which the current and future use of IT is directed and controlled. It involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans**

(Font DIS 29382, ISO/IEC JTC1/SC7,2007)

IT-GOVERNANCE

(Font Bosch, Antoni. Piràmide IT-Governance. Barcelona 2003)



IT-GOVERNANCE

- ¿Qué decisiones se han de tomar?
- ¿Quién las ha de tomar?
- ¿Quién provee la información?
- ¿Cómo se han de tomar?
- ¿Cuándo se han de tomar?
- ¿Cómo se han de monitorizar y controlar?

¿Qué decisiones tomar?

LAS 5 PRINCIPALES DECISIONES <i>(Weill & Ross. IT-Governance. HBSP,2004)</i>	Las 5 AREAS <i>(IT Governance Institute Cobit 4.1, USA 2007)</i>	LOS 6 PRINCIPIOS <i>(DIS 29382, ISO/IEC JTC1/SC7,2007)</i>
Principios IT	Alineamiento estratégico	Responsabilidad
Arquitectura IT	Entrega de Valor	Estrategia
Infraestructura IT	Gestión de Recursos	Adquisición
Aplicaciones de negocio	Gestión de Riesgos	Performance
Inversiones y prioridades	Medida del Performance	Cumplimiento
		Recursos Humanos

¿Quién las ha de tomar ?

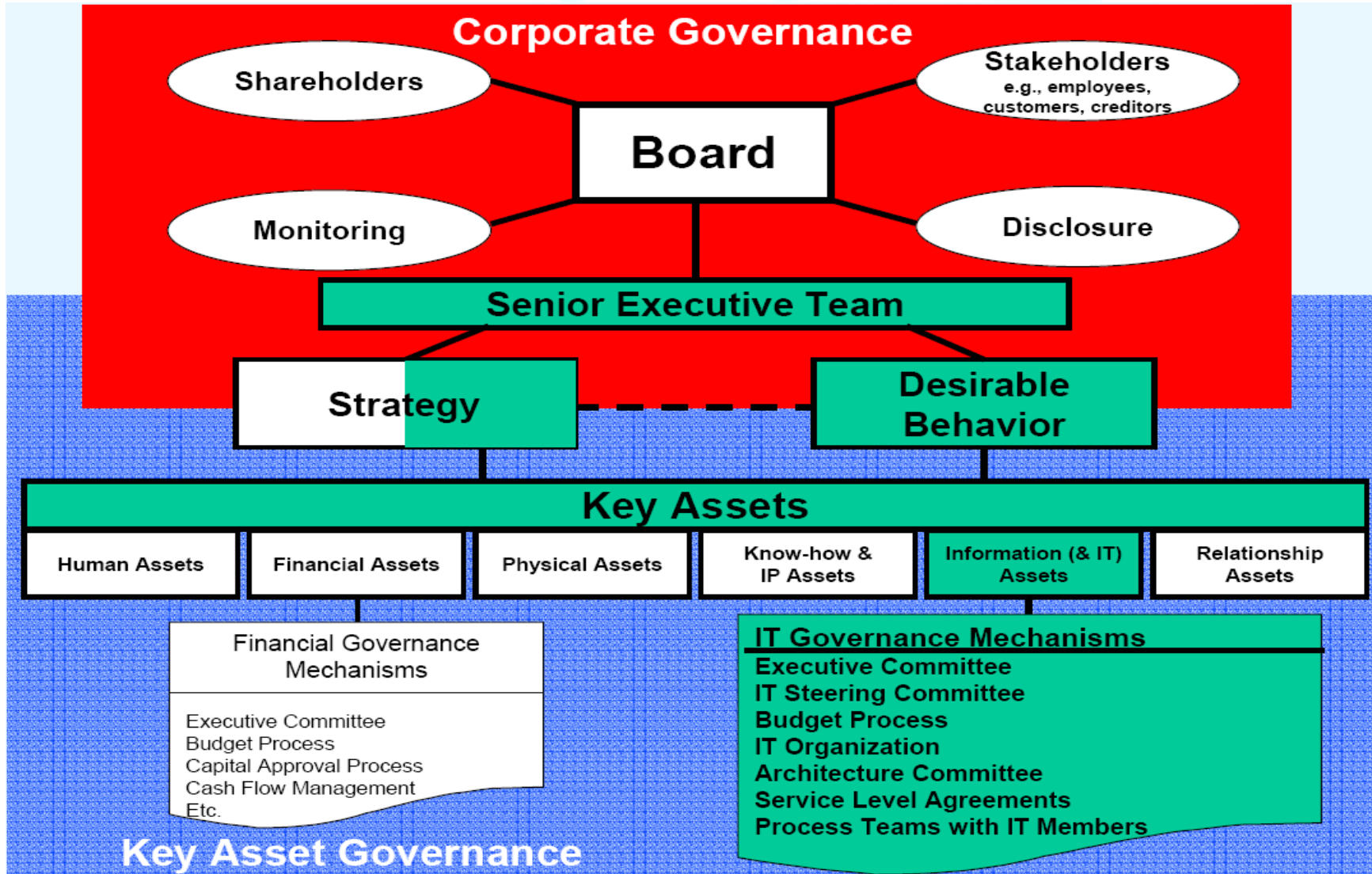
- **Monarquía de Negocios**
- **Monarquía de IT**
- **Federal**
- **Duopolio IT**
- **Feudal**
- **Anarquía**

¿Quién provee la información ?

- Director ejecutivo (CEO)
- Director financiero (CFO)
- Directores áreas funcionales (CxO)
- Director de S.I. (CIO)
- Propietario del proceso de negocio
- Director de Operaciones
- Encargado de tratamiento
- Director de Arquitectura
- Director de Desarrollo
- Director de Administración de TI.
- Director Oficina de proyectos
- Responsables de control.
- Auditores de SI (externos o internos)
- Consultores externos (outsourcing)
- ...

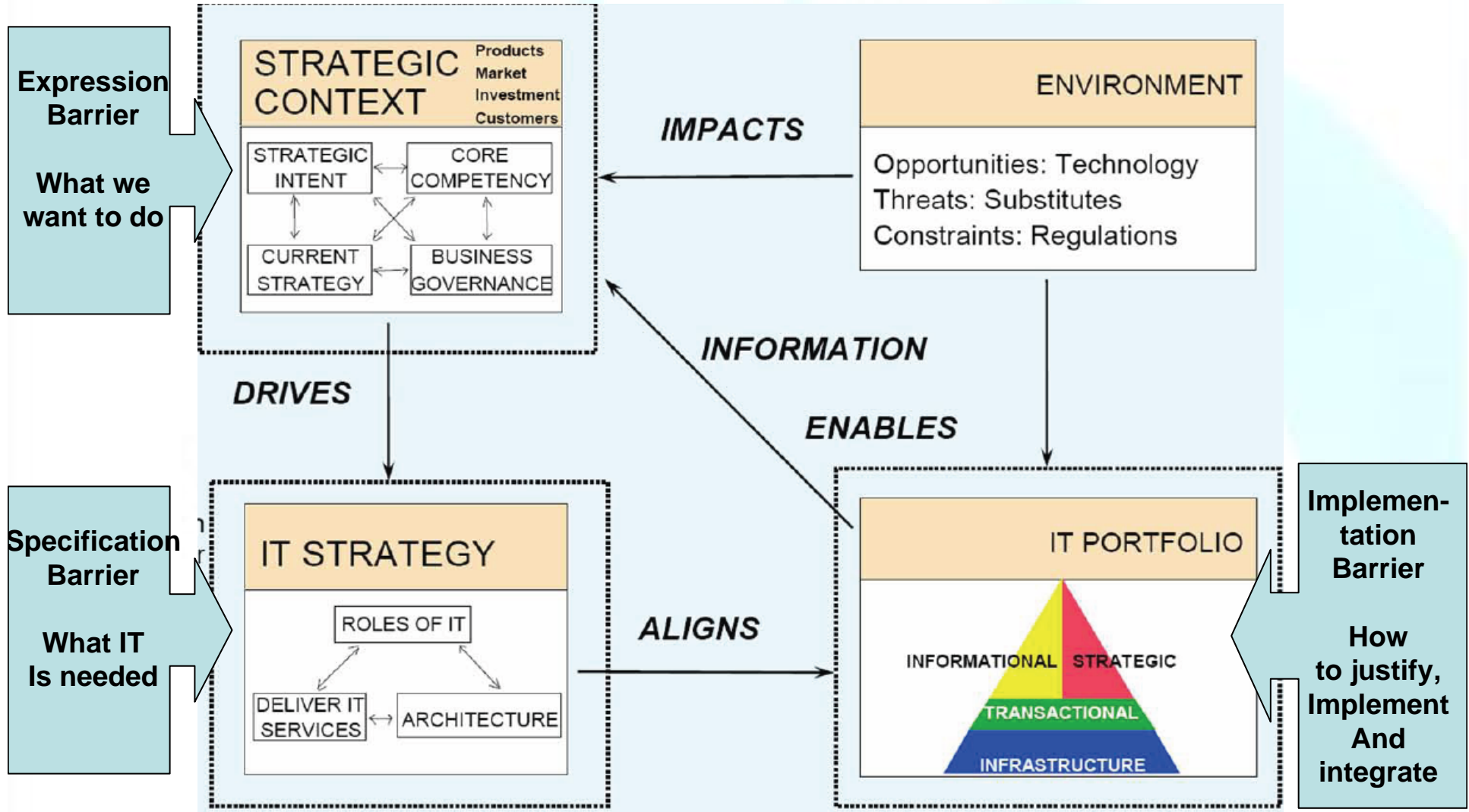
Modelo MIT Sloan CISR

(Font Weill & Ross. IT-Governance. HBSP,2004)



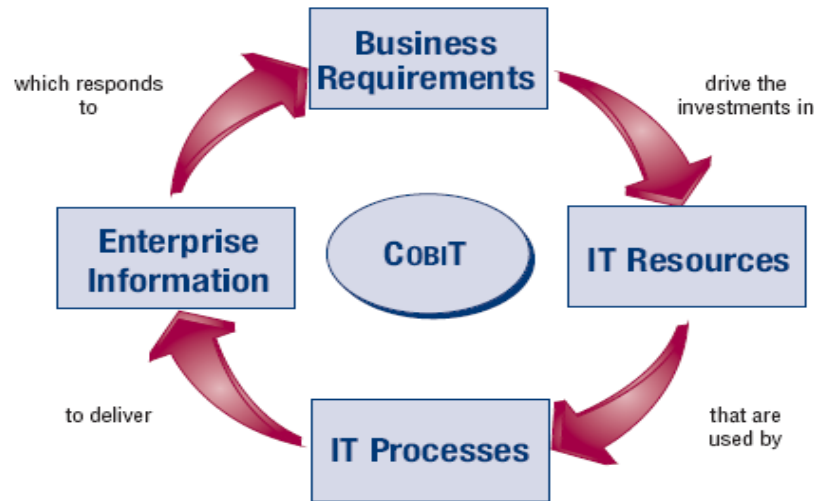
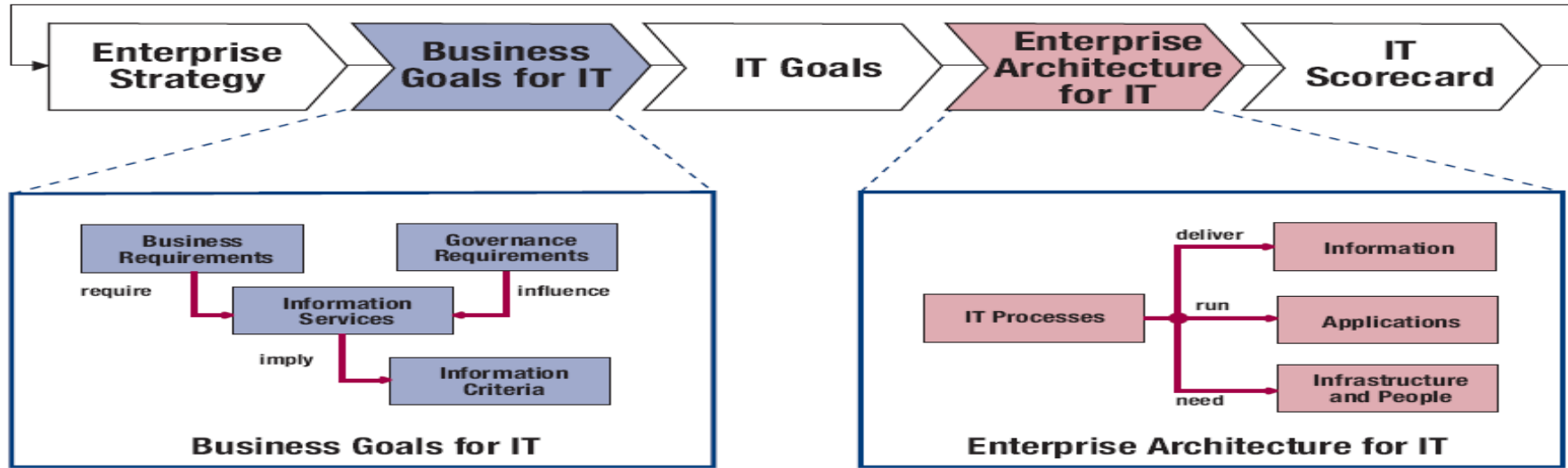
IT and Business Strategy

(Font Weill & Broadbent. Leveraging the New Infrastructure. HBSP, 1998).



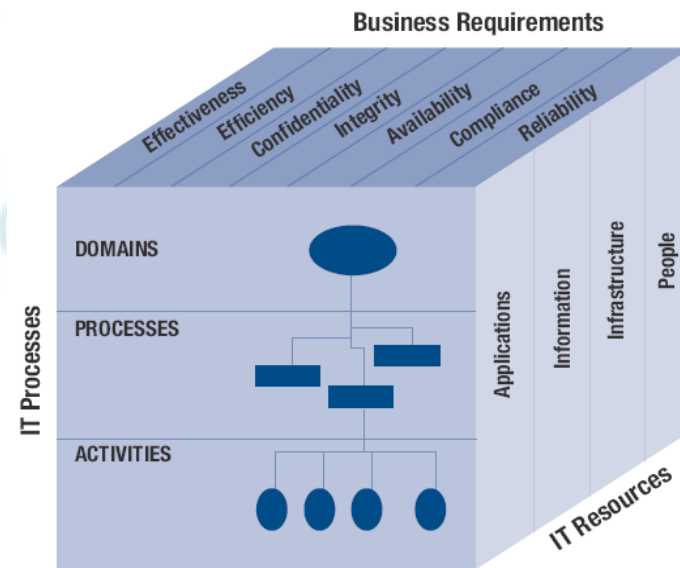
Modelo COBIT

(Font IT Governance Institute Cobit 4.1, USA 2007)



2008 IT-Governance

ABP - 9



© 2008 Antoni Bosch

IT Processes and domains

Business Objectives

(Font IT Governance Institute Cobit 4.0, USA 2005)

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



- PO1 Define a strategic IT plan.
- PO2 Define the information architecture.
- PO3 Determine technological direction.
- PO4 Define the IT processes, organisation and relationships.
- PO5 Manage the IT investment.
- PO6 Communicate management aims and direction.
- PO7 Manage IT human resources.
- PO8 Manage quality.
- PO9 Assess and manage IT risks.
- PO10 Manage projects.

- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure regulatory compliance.
- ME4 Provide IT governance.

IT RESOURCES

- Applications
- Information
- Infrastructure
- People

PLANNING AND ORGANISATION

MONITORING

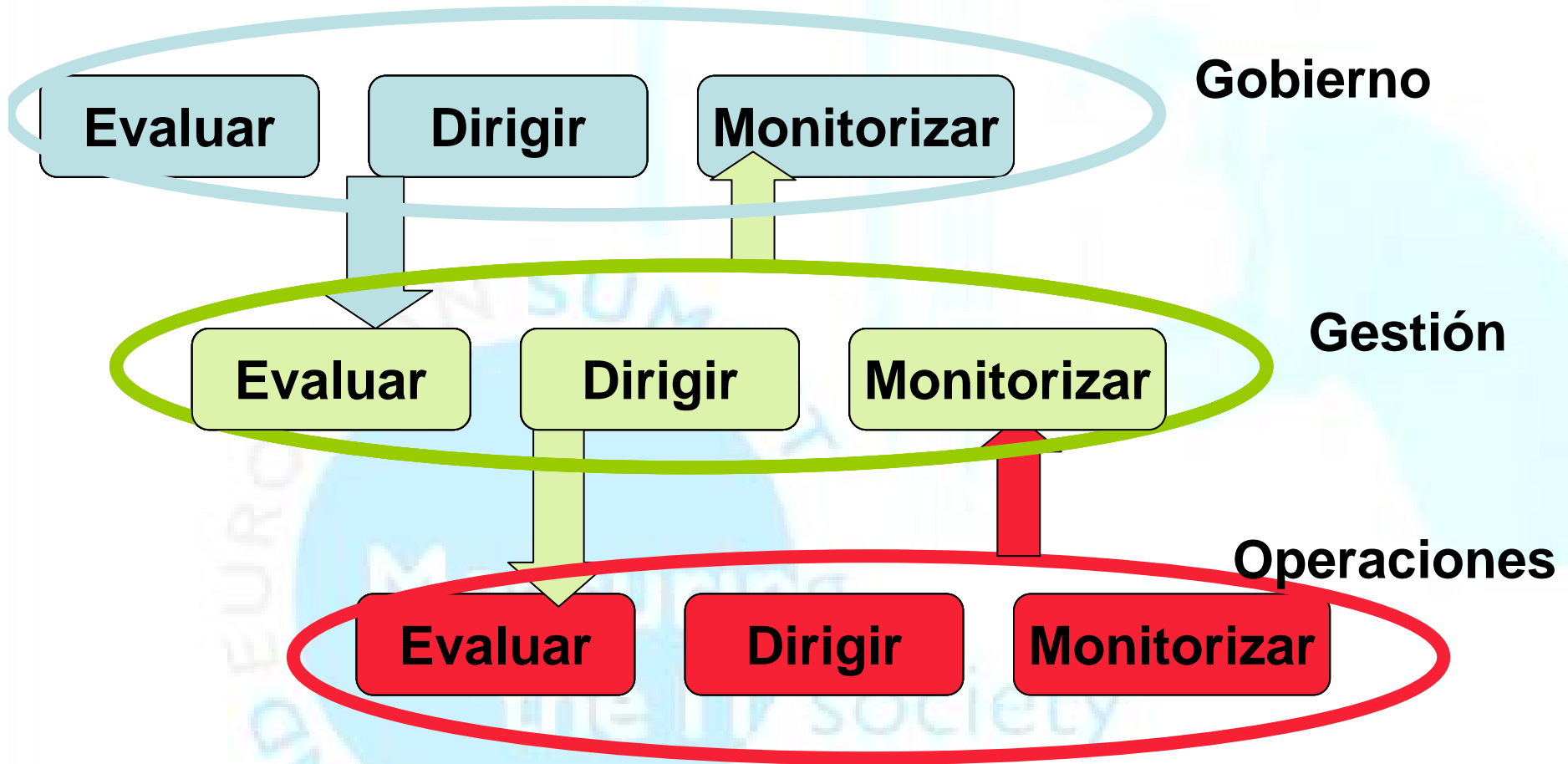
AQUISITION AND IMPLEMENTATION

- 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 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS10 Manage problems.
- DS11 Manage data.
- DS12 Manage the physical environment.
- DS13 Manage operations.

DELIVERY AND SUPPORT

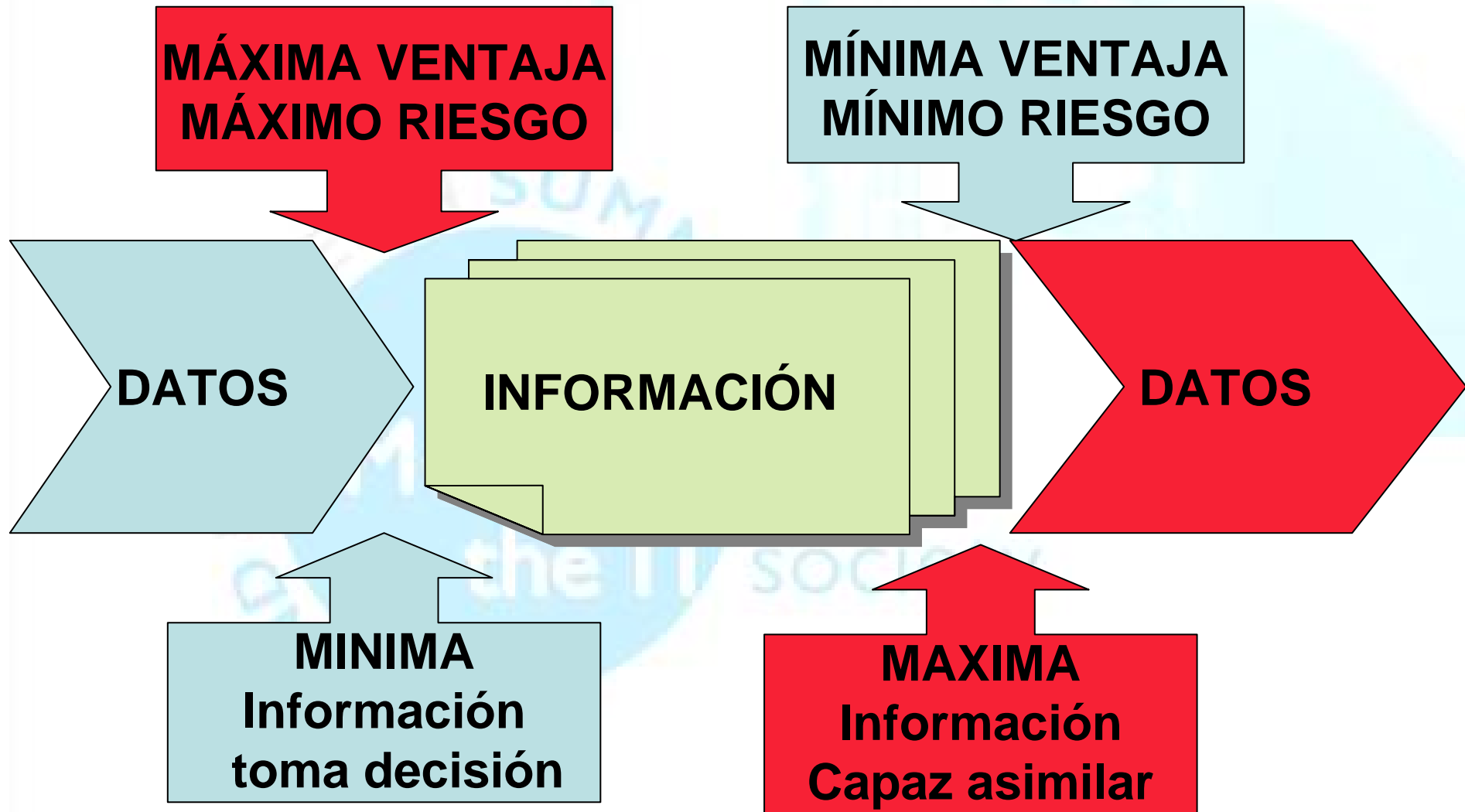
- AI1 Identify automated solutions.
- AI2 Acquire and maintain application software.
- AI3 Acquire and maintain technology infrastructure.
- AI4 Enable operation and use.
- AI5 Procure IT resources.
- AI6 Manage changes.
- AI7 Install and accredit solutions and changes.

Modelo ISO 29382



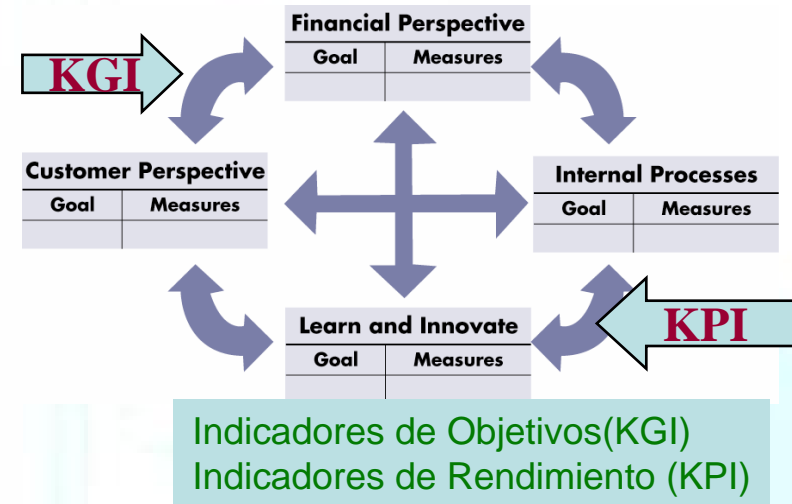
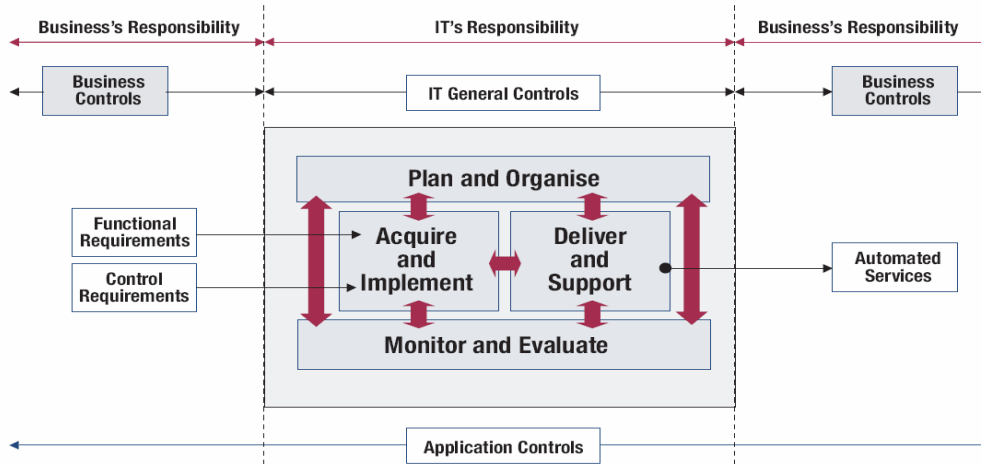
Responsabilidad	Adquisición	Cumplimiento
Estrategia	Performance	Recursos Humanos

¿Cuándo se han de tomar ?

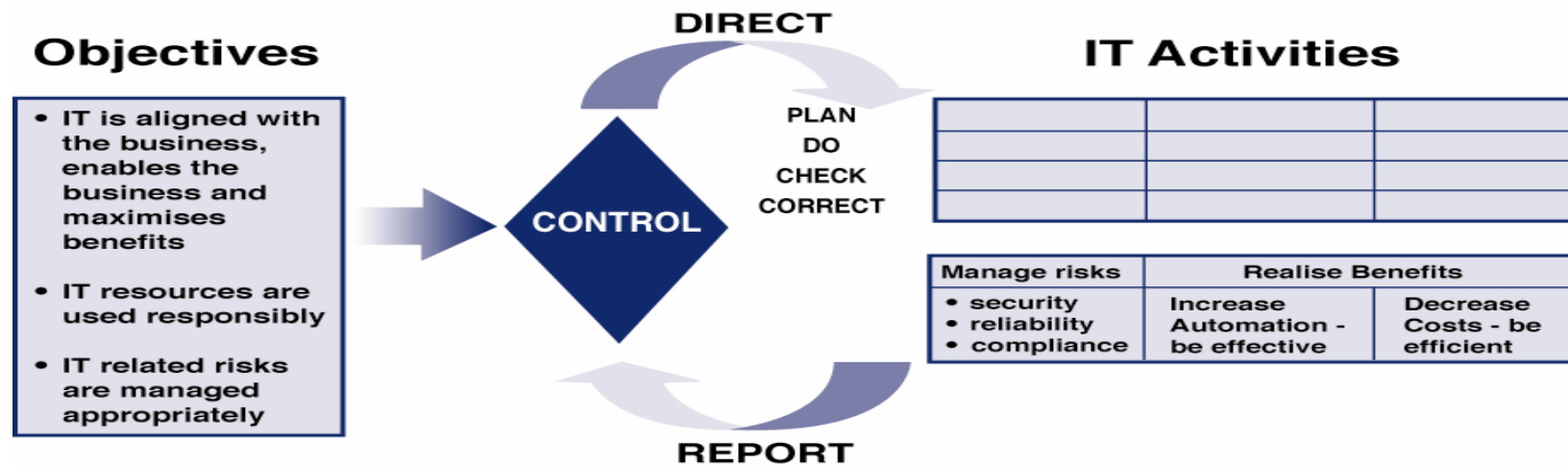


Modelo CONTROL

(Font IT Governance Institute Cobit 4.1, USA 2007)



IT Governance



IT Risk

(Font Westerman. MIT Sloan CISR,2005)

Enterprise IT Risks

Continuity

- Availability
- Business continuity
- Disaster recovery

Access Management

- Information protection
- Knowledge sharing
- Preventing malicious attacks

Integrity

- Data accuracy, timeliness, and consistency
- Regulatory compliance

Strategic Change

- Ability to implement major strategic change



IT Risk Factors

Technology & Infrastructure

- Configuration management
- Degree of standardization
- Age of technology

Applications & Information

- Architecture complexity
- Redundancy
- Data consistency
- Degree of customization

People & Skills

- Turnover
- Skills planning
- Recruiting/training
- IT/Business Relationship

Vendors & Other Partners

- SLAs
- Use of firm's methods/standards
- Sole source
- Customer risk tolerance

Policy & Process

- Controls architecture
- Degree of standardization
- Degree of accountability

Organizational

- Cost cutting
- Organizational Complexity
- Funding processes

External Threats
New regulation
Virus
Geopolitical

Modelo COBIT

(Font IT Governance Institute Cobit 4.0, USA 2005)

Management's Questions

How do responsible managers "keep the ship on course"?

DASHBOARDS

Indicadores?

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

SCORECARDS

Medidas?

How to timely adapt the organisation to trends and developments in the enterprise's environment?

BENCHMARKING

Escalas?

Non-Existent Initial Repeatable Defined Managed Optimised



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

IT-GOVERNANCE in one page

(Font Weill & Ross. IT-Governance. HBSP,2004)

1. Pregunta:

¿Que importancia otorga a los siguientes resultados del IT-Governance de su organización en una escala de 1 (nada importante) a 5 (muy importante)?

2. Pregunta:

¿Cual es la influencia del IT-Governance de su organización en los siguientes resultados en una escala de 1 (nada importante) a 5 (muy importante)?

a. Coste de la utilización efectiva de las IT		X		=	
b. Utilización efectiva de las IT para el aumento de negocio		X		=	
c. Utilización efectiva de las IT para el uso de los activos		X		=	
d. Utilización efectiva de las IT para ganar flexibilidad empresarial		X		=	
Importancia total =				Total=	

3. Calcule los resultados de gobierno: (Total x 100) / (5 x Importancia Total) =
 (Importancia Resultados*Influencia)/5*Importancia Resultados

1. Nuestros directivos pueden describir con detalle el IT-Governance de la organización.	
2. Nuestro IT-Governance fue diseñado de forma activa y no mediante acciones descoordinadas.	
3. Nuestro IT-Governance es estable y ha sufrido pocos cambios en los años recientes.	
4. Los gerentes que no conocen el IT-Governance reciben asesoramiento con el objetivo de que puedan seguir las directrices establecidas.	
5. Hay un número muy reducido de objetivos de negocio claves que dirigen el diseño del IT-Governance.	
6. Tenemos unos procesos de excepciones rápidos y bien definidos.	
7. El IT-Governance tiene un(os) claro(s) propietario(s) y existen indicadores de medida del éxito.	
8. Los sueldos, los incentivos y el IT-Governance están en concordancia.	
9. Tenemos un IT-Governance efectivo en la totalidad de la organización y en concordancia con los objetivos de negocio.	
10. Nuestro director de SI podría ausentarse dos meses y nuestro IT-Governance seguiría funcionando correctamente.	
Evalúe en una escala de 1 (muy en desacuerdo) a 5 (muy de acuerdo):	x 2 = TOTAL

GOBIERNO DE LAS TIC

IT GOVERNANCE

1. Sea Proactivo, no reactivo
2. Sepa cuando rediseñar
3. Involucre a todos los altos directivos
4. Tome decisiones
5. Clarifique el manejo de las Excepciones
6. Incentive
7. Asigne propiedad y responsabilidades
8. Considere diferentes niveles
9. Sea Transparente y eduque
10. Implemente mecanismos comunes

The logo for IDT (Institute of Law and Technology) features the letters 'IDT' in a bold, black, sans-serif font. The 'I' and 'D' are connected, and the 'T' is separate. The background is a grid of orange and white squares.

Institute of Law
and Technology

UAB



IAITG

INSTITUTE
OF AUDIT &
IT-GOVERNANCE

MUCHAS GRACIAS

Antoni Bosch-Pujol, CISA, CISM

Director Institute Audit & IT-Governance (IAITG)

Director IT-Governance (IDT-UAB)

President ISACA-Barcelona

antoni.bosch@uab.es

<http://idt.uab.es/people/curr/bosch.htm>

http://idt.uab.es/it_governance/it_governance.htm