

I Ciclo de Conferencias **ISACA - CV "Rafael Bernal"**

Auditoría, Seguridad y Gobierno de las TIC

IT-GOVERNANCE

Antoni Bosch i Pujol, CISA, CISM
antonи.bosch@uab.es

www.eae.es
<http://idt.uab.es>
www.isacabcn.org

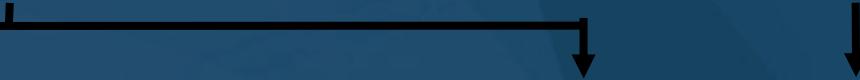
I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- **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)



I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- **¿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?**

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: $(Total \times 100) / (5 \times Importancia\ Total) =$ $(Importancia\ Resultados \times Influencia) / 5 \times Importancia\ Resultados$			

I Ciclo de Conferencias ISACA - CV "Rafael Bernal" Auditoría, Seguridad y Gobierno de las TIC	
<ul style="list-style-type: none"> • Evalúe su IT-Governance para cada uno de los ítems siguientes en una escala de 1 (muy en desacuerdo) a 5 (muy de acuerdo): 	
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.	
x 2 = TOTAL	

I Ciclo de Conferencias ISACA - CV "Rafael Bernal" Auditoría, Seguridad y Gobierno de las TIC	Performance	Resilience
81 - 100		
61 - 80		
41 - 60		
21 - 40		

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- ¿Qué decisiones se han de tomar?

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Principios IT	
Arquitectura IT	
Infraestructura IT	
Aplicaciones de negocio	
Inversiones y prioridades	

Las 5 AREAS

(Font IT Governance Institute Cobit 4.1, USA 2007)



<p>I Ciclo de Conferencias ISACA - CV "Rafael Bernal" Auditoría, Seguridad y Gobierno de las TIC</p>	
Responsabilidad	
Estrategia	
Adquisición	
Performance	
Cumplimiento	
Recursos Humanos	

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- ¿Quién las ha de tomar?

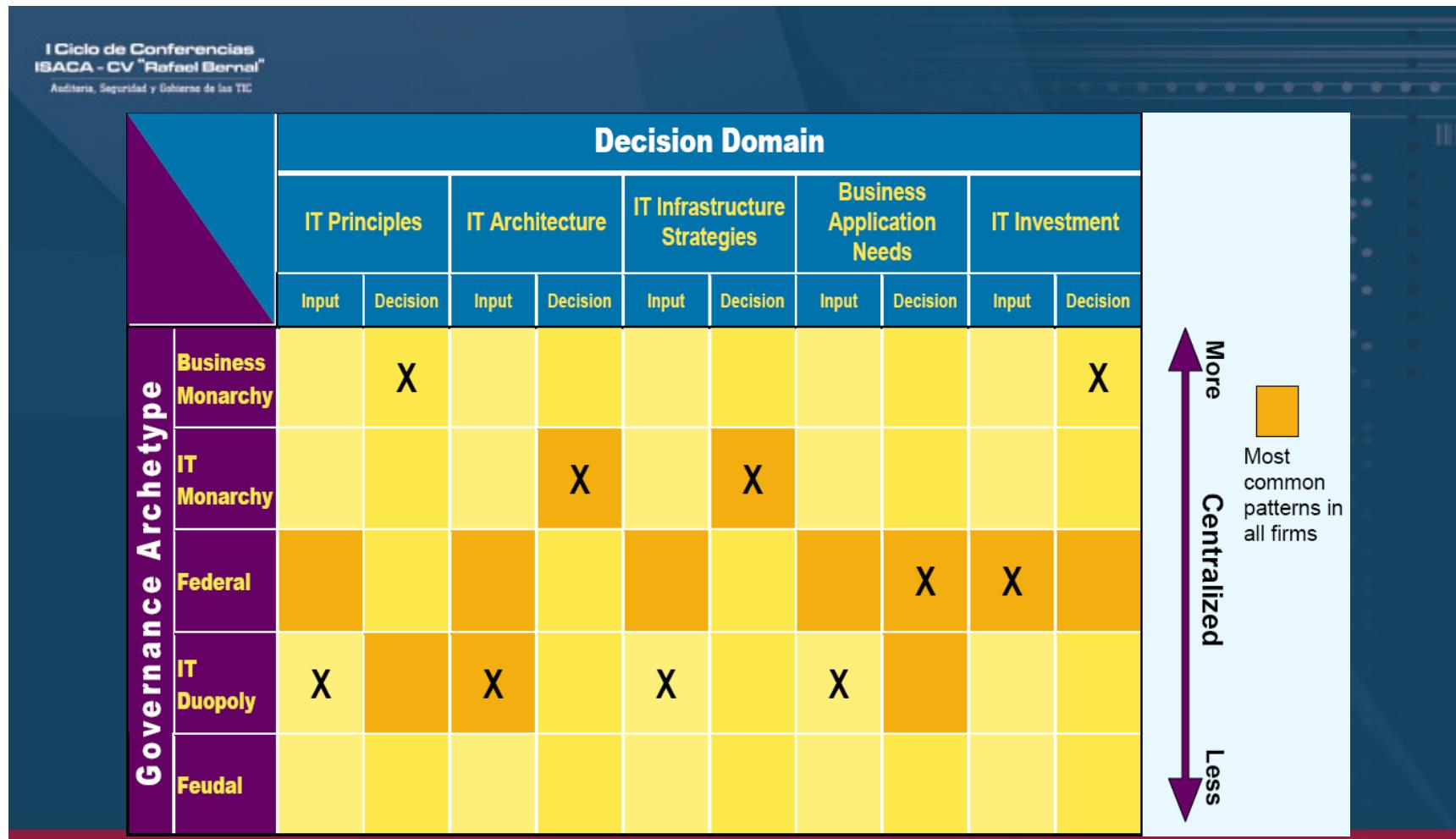
I Ciclo de Conferencias ISACA - CV "Rafael Bernal" Auditoría, Seguridad y Gobierno de las TIC	
Monarquía de Negocios	A group of, or individual, business executives (i.e.,CxOs). Includes committees comprised of senior business executives (may include CIO). Excludes IT executives acting independently.
Monarquía de IT	Individuals or groups of IT executives
Federal	Shared by C level executives and the business groups(i.e., CxOs and BU leaders) — may also include ITexecutives. Equivalent of the center and states workingtogether.
Duopolio IT	IT executives and one other group(e.g., CxOs or BU leaders)
Feudal	Business unit leaders, key process owners or theirdelegates
Anarquía	Each individual user

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

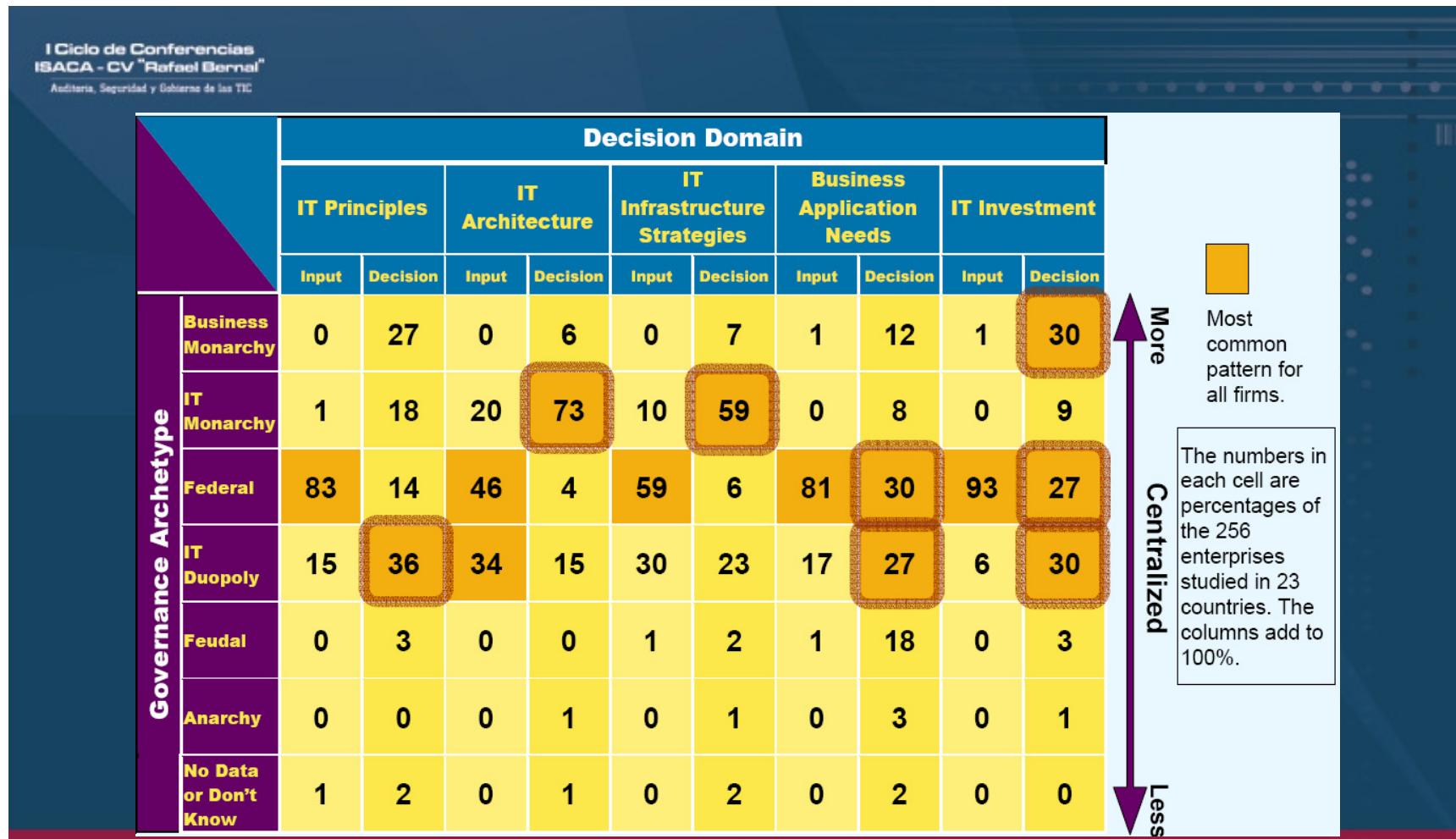
- ¿Quién provee la información?

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- Director ejecutivo (CEO)
- Director financiero (CFO)
- Ejecutivos del negocio o Directores áreas funcionales.
- Director de Sistemas de Información (CIO)
- Propietario del proceso de negocio
- Jefe de operaciones
- Arquitecto en jefe
- Jefe de desarrollo
- Jefe de administración de TI (para empresas grandes, el jefe de funciones como recursos humanos, presupuestos y control interno)
- La oficina o función de administración de proyectos (PMO)
- Cumplimiento, auditoría, riesgo y seguridad (responsabilidad de control sin responsabilidad operacional)

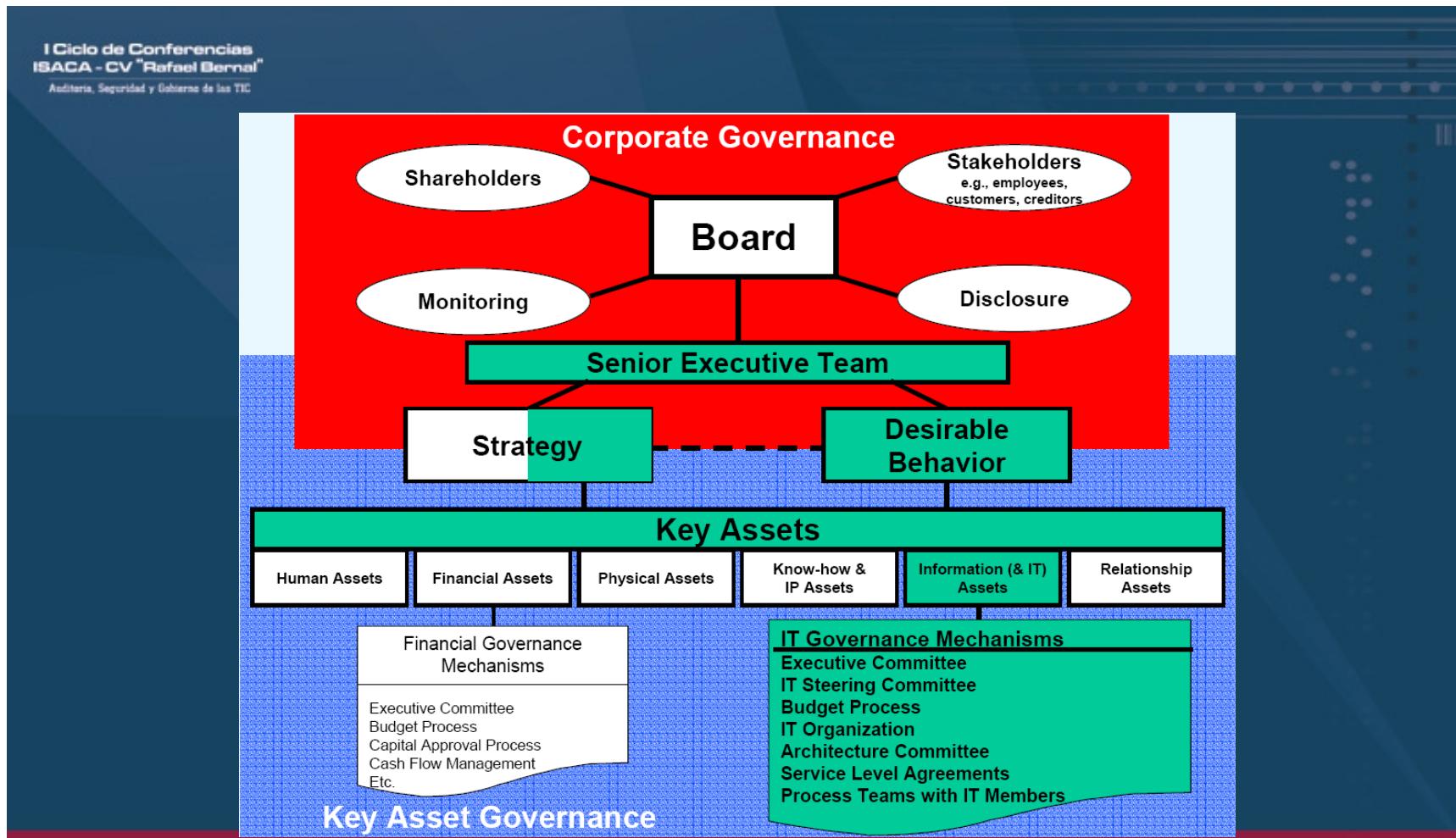


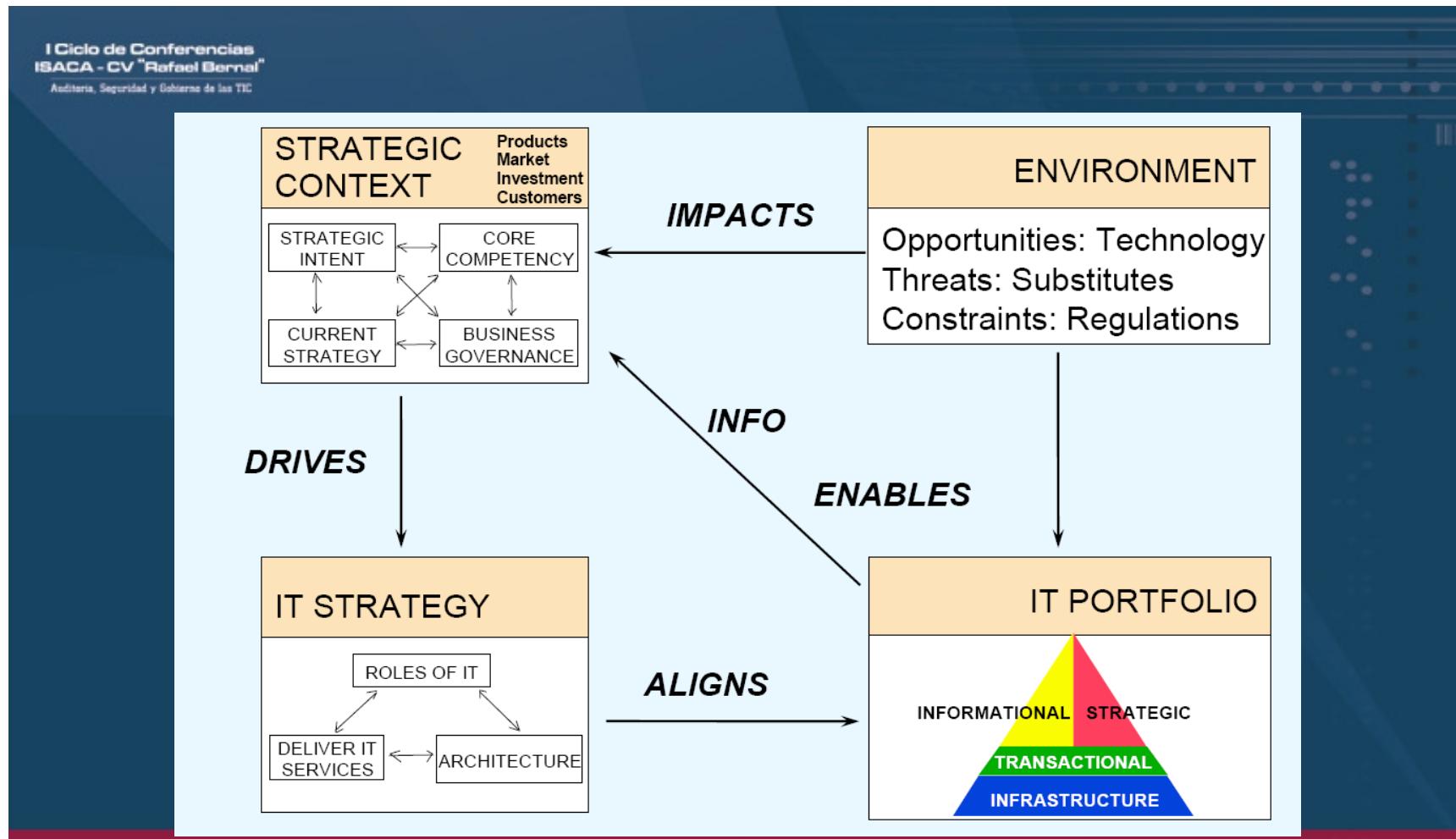
What and Who
 (Font Weill & Ross. IT-Governance.
 HBSP,2004)

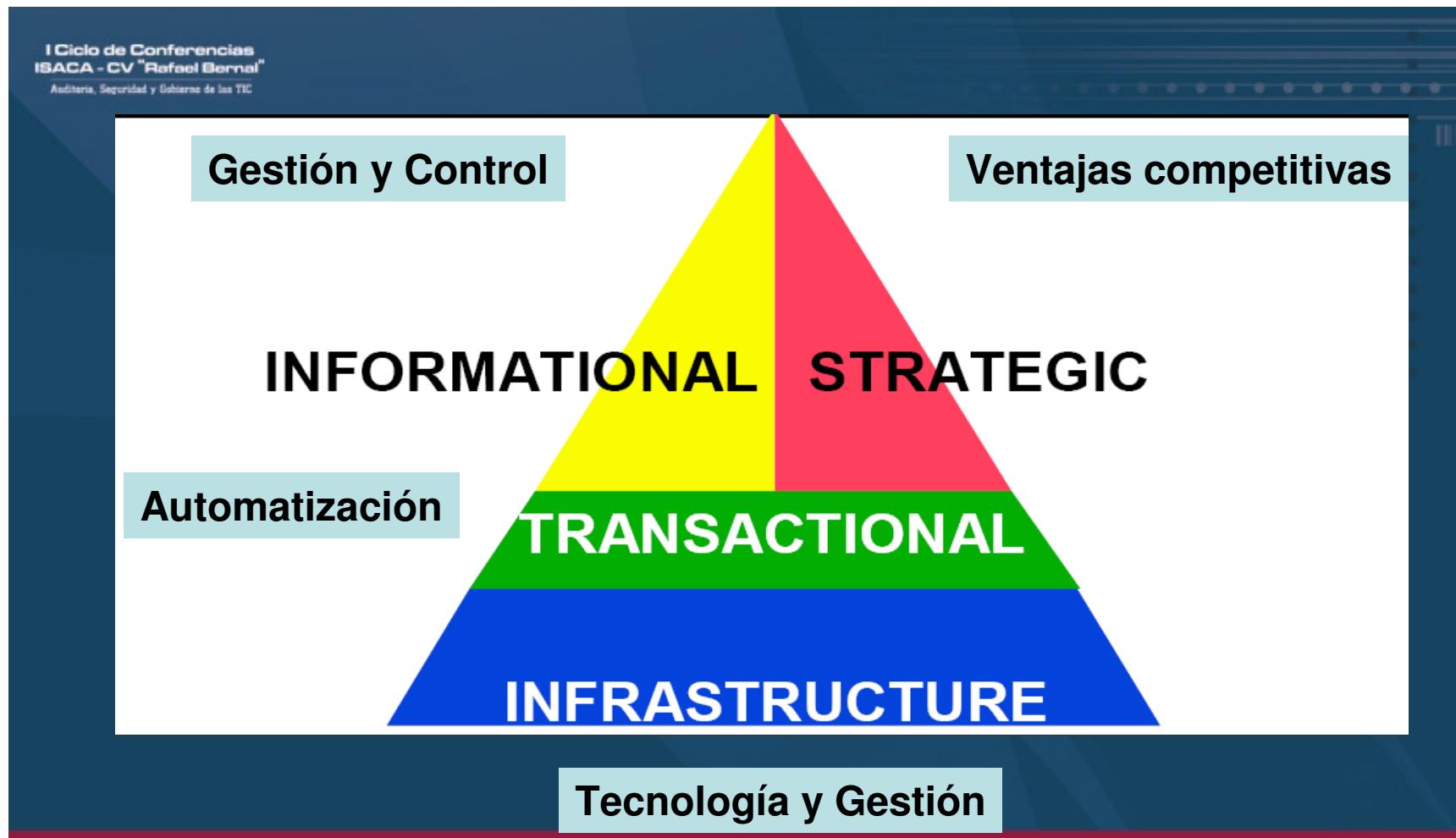


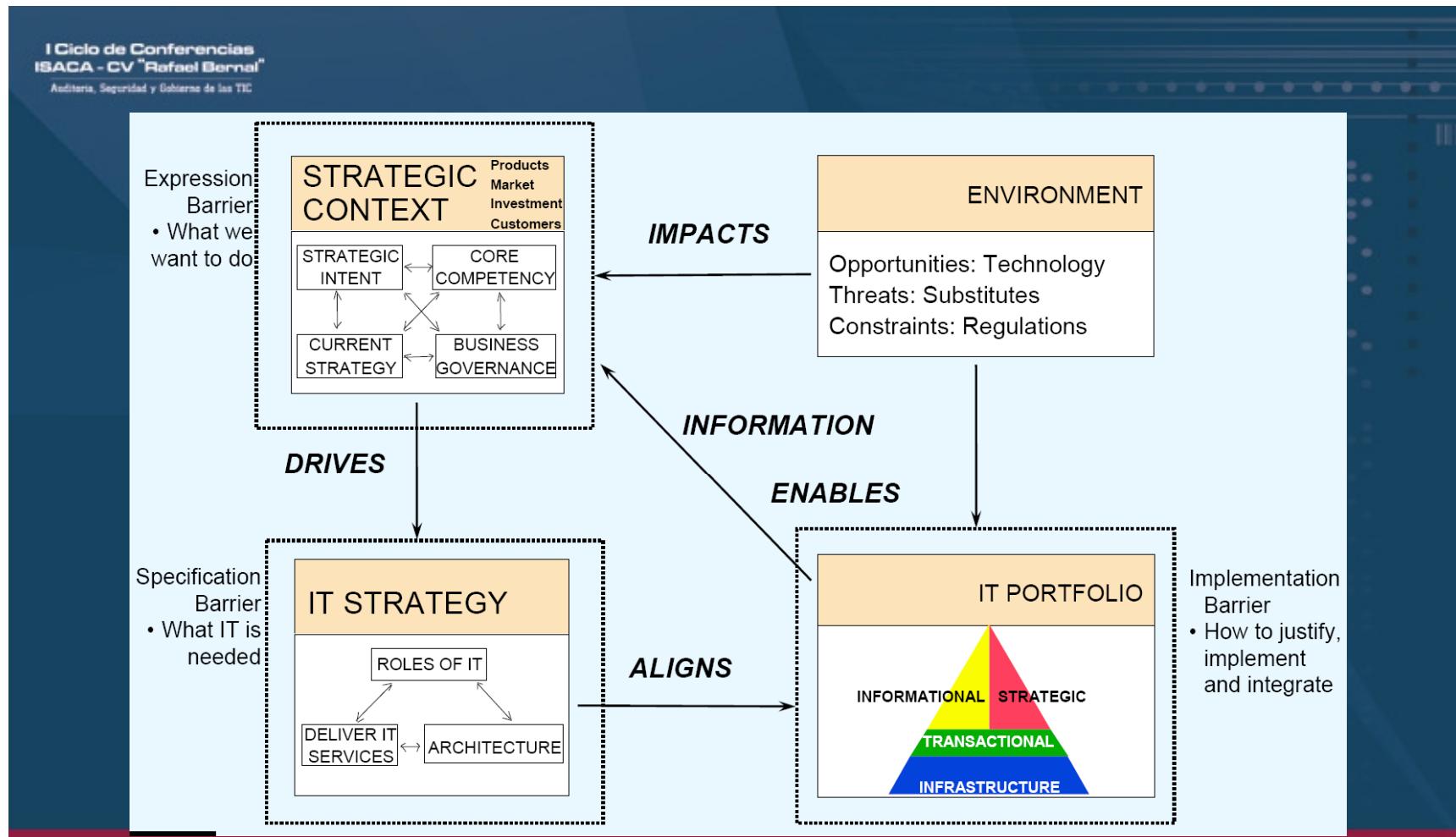
I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

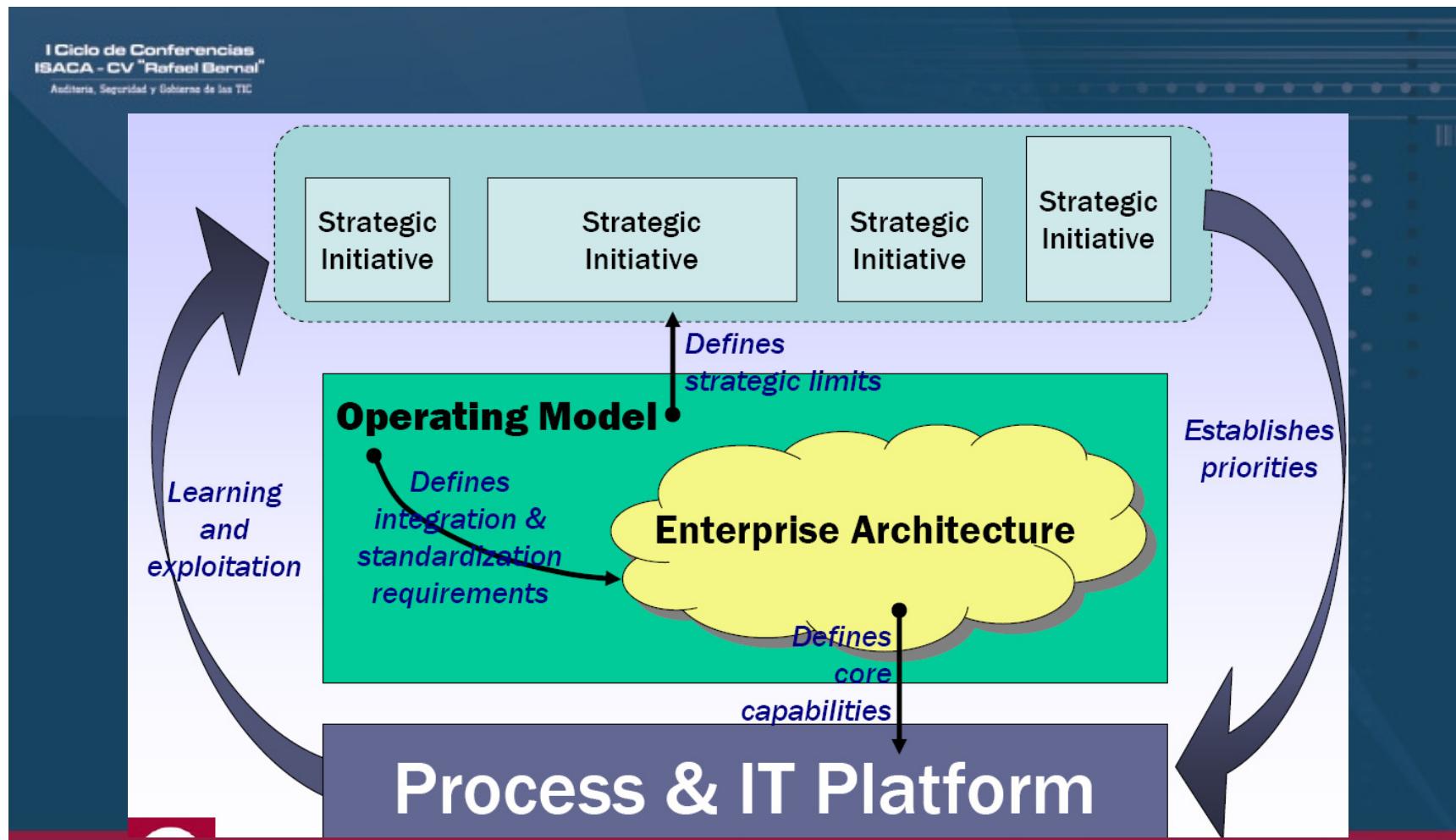
- ¿Cómo se han de tomar?

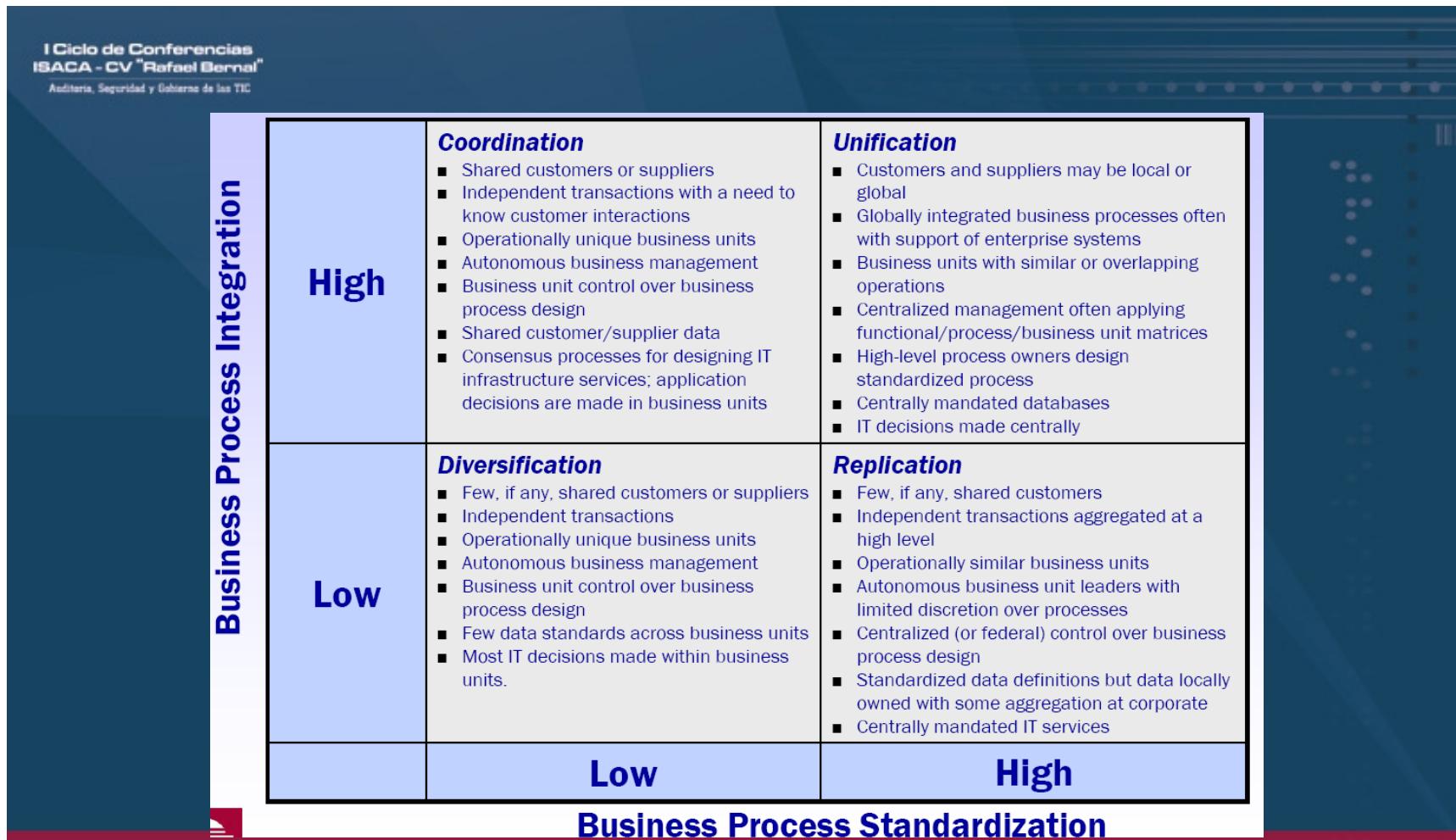


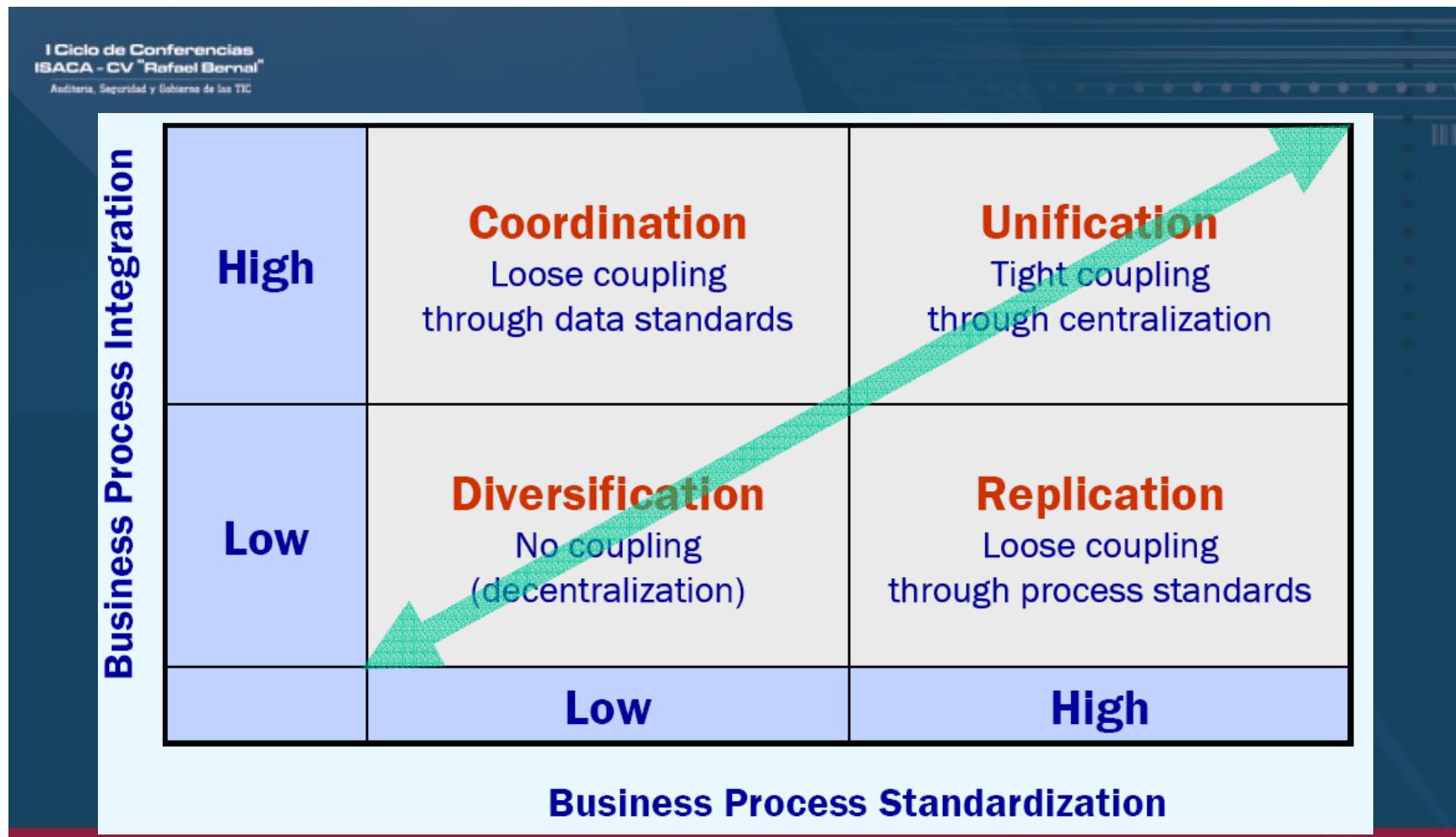




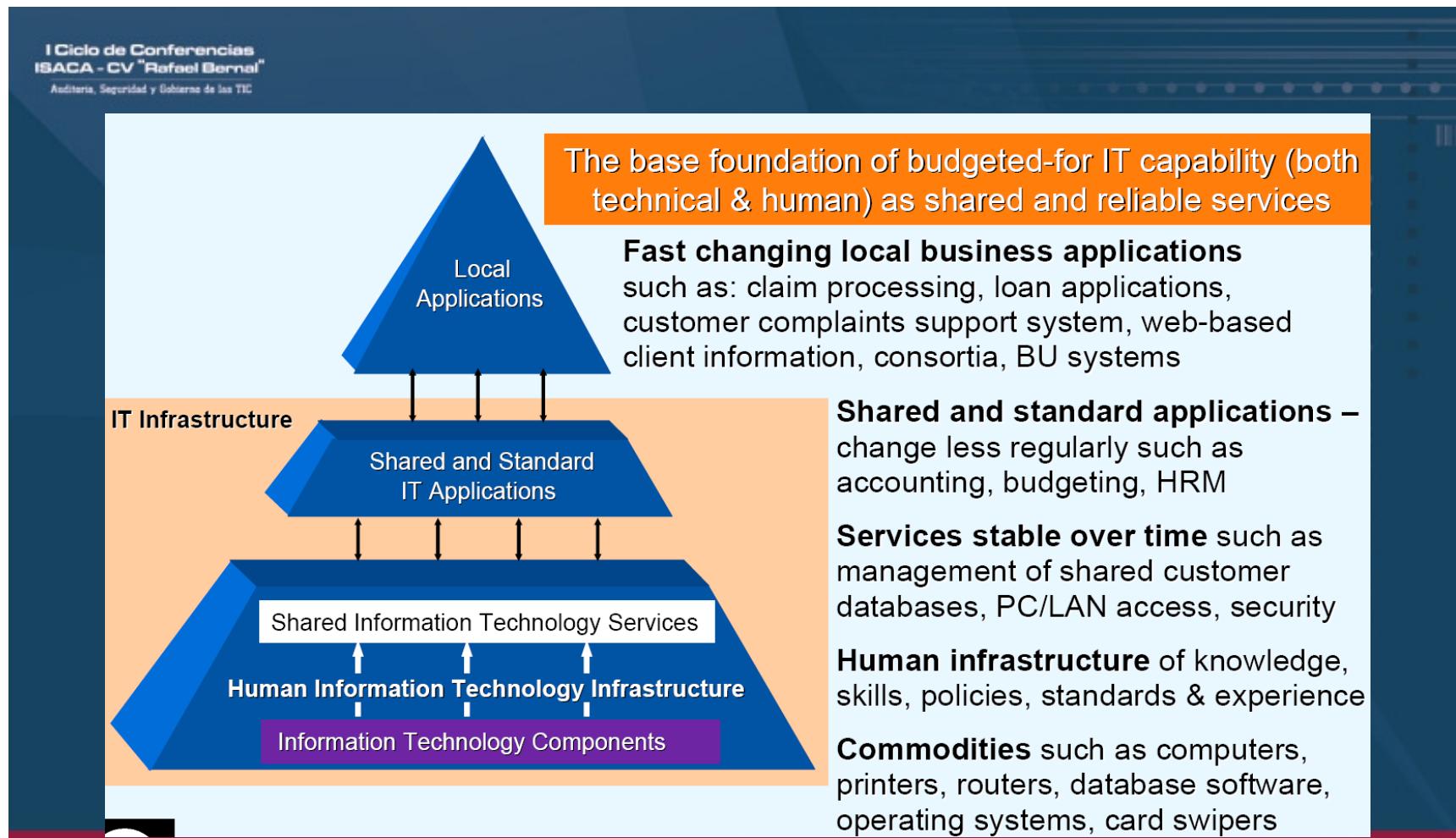








IT Infrastructure (Font Weill & Broadbent. Leverage the New Infrastructure. HBSP, 1998).



The diagram illustrates the relationship between management questions and COBIT components. On the left, three management questions are listed. To the right, three COBIT components are shown in grey boxes, each with a blue arrow pointing to a corresponding question in red.

Management's Questions	COBIT Components	Associated Question
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?

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

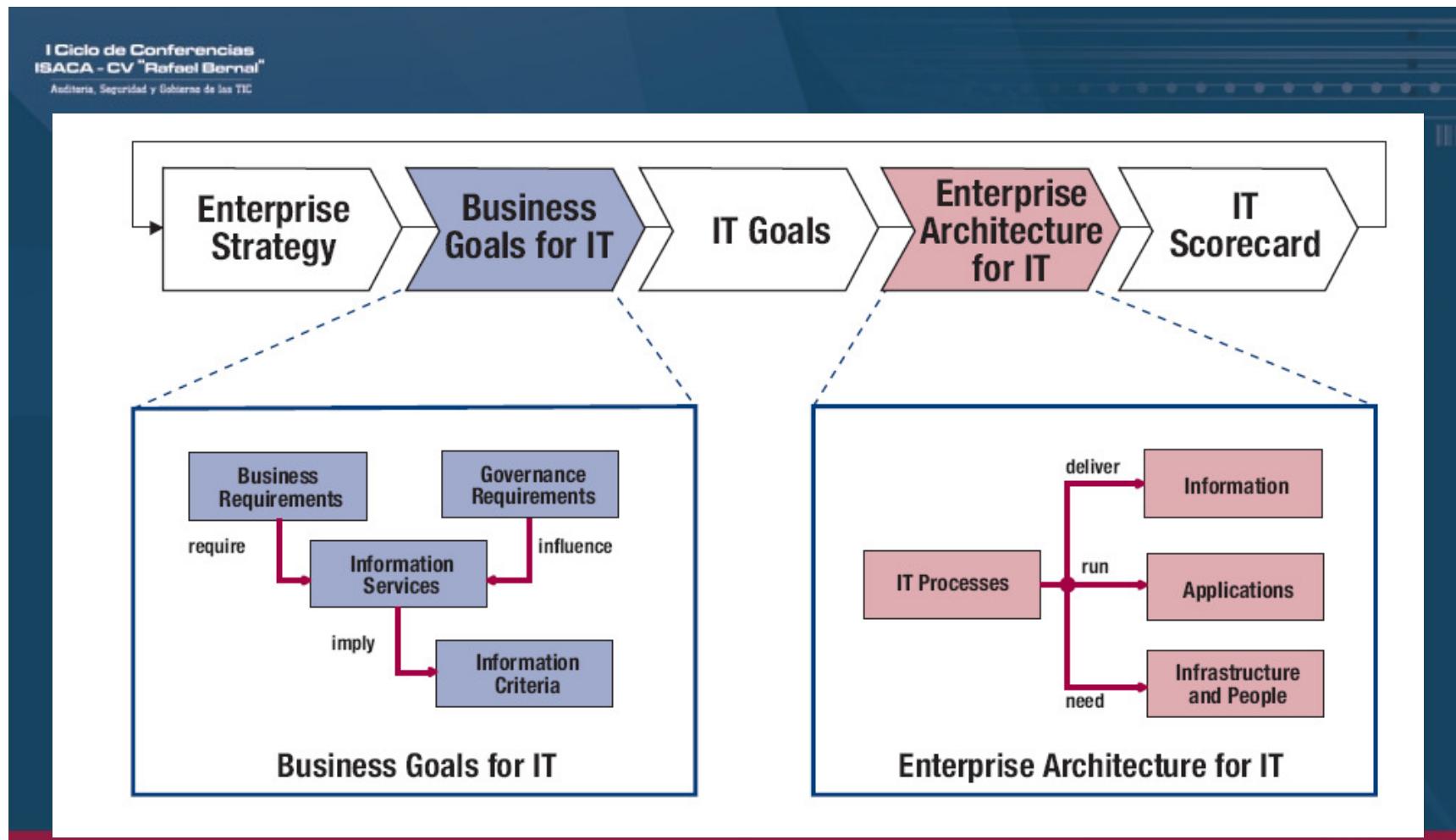
Management's Questions

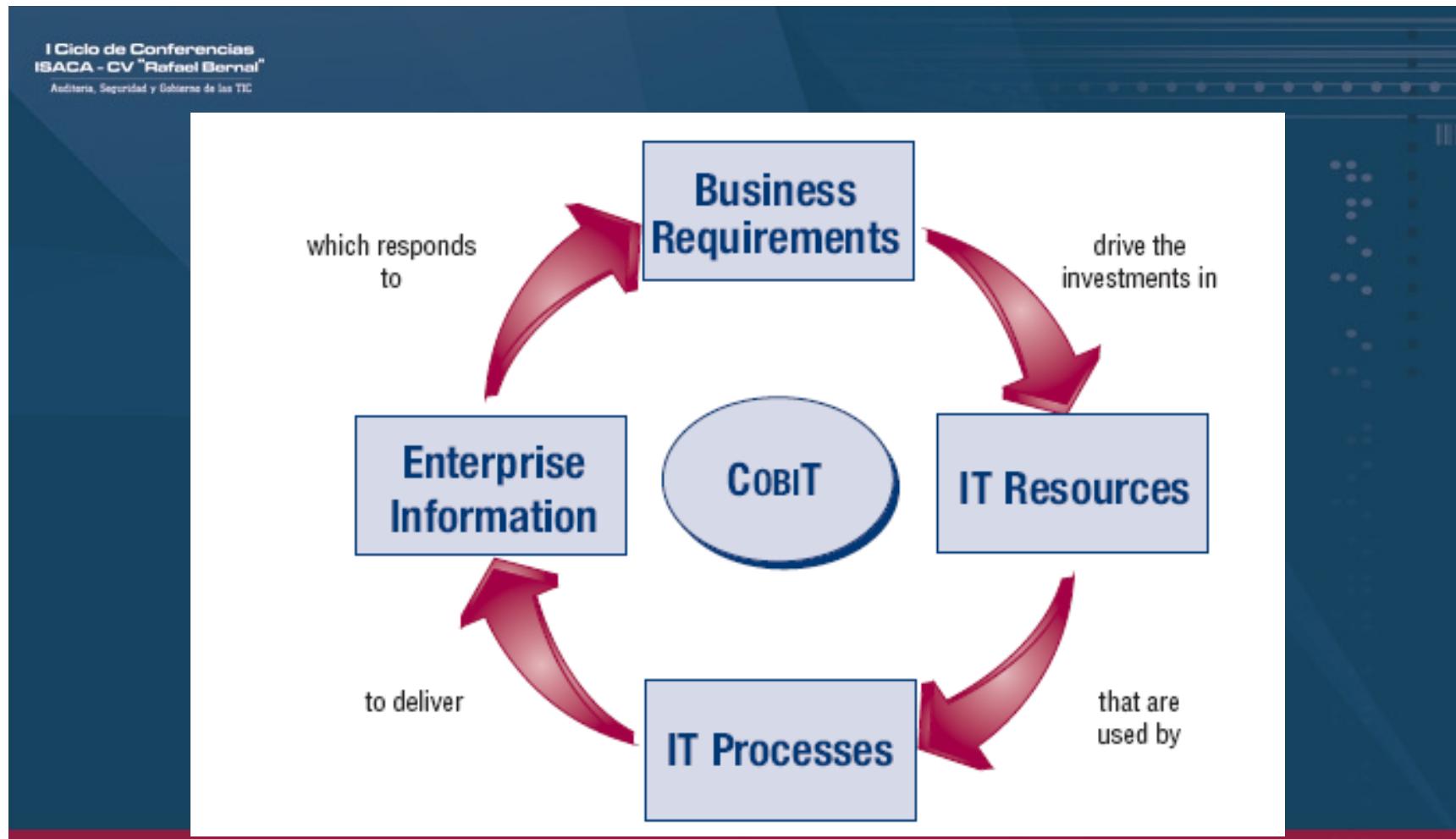
- How do responsible managers "keep the ship on course"?
- How to achieve results that are satisfactory for the largest possible segment of our stakeholders?
- How to timely adapt the organisation to trends and developments in the enterprise's environment?

DASHBOARDS → Indicadores?

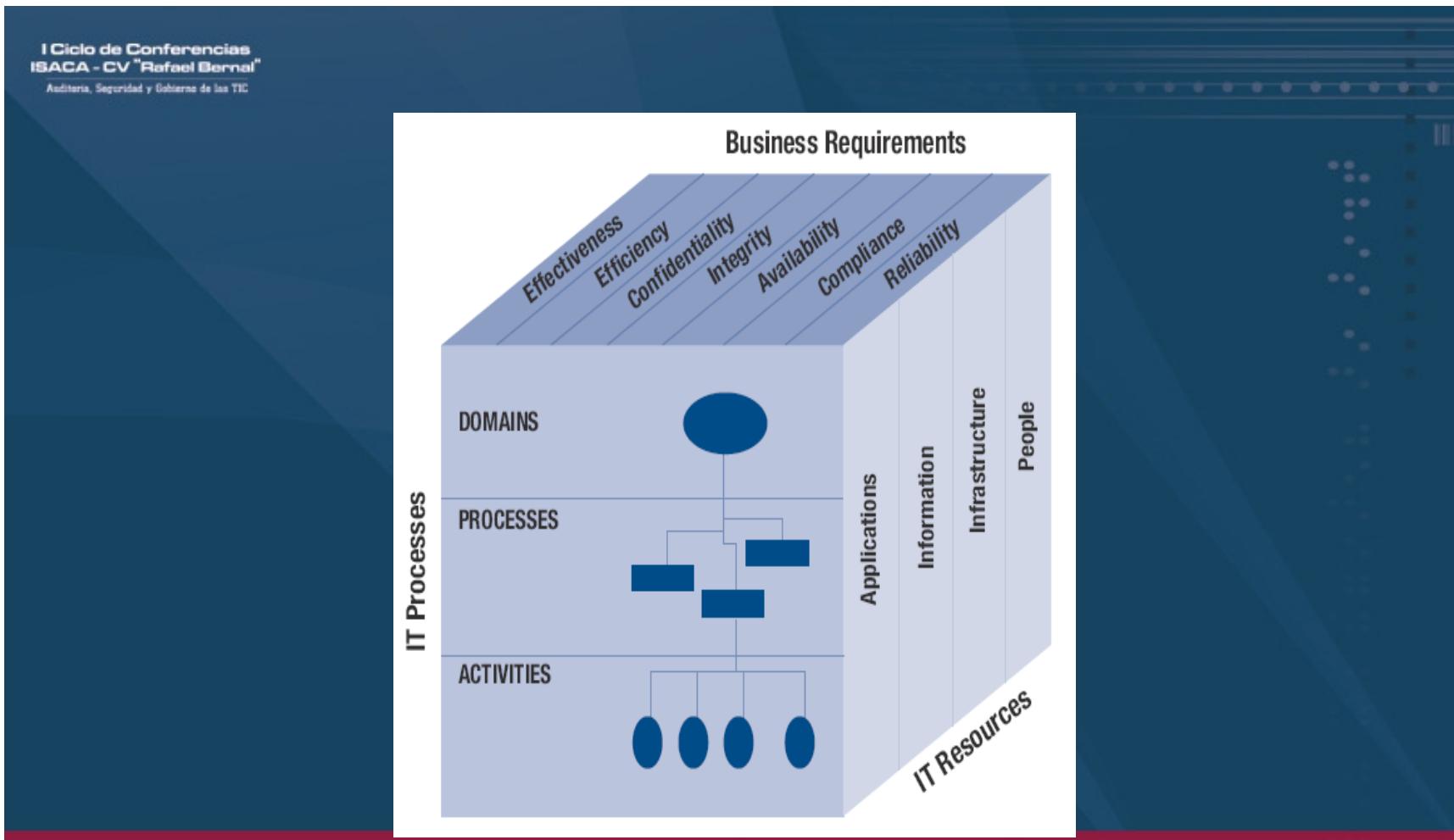
SCORECARDS → Medidas?

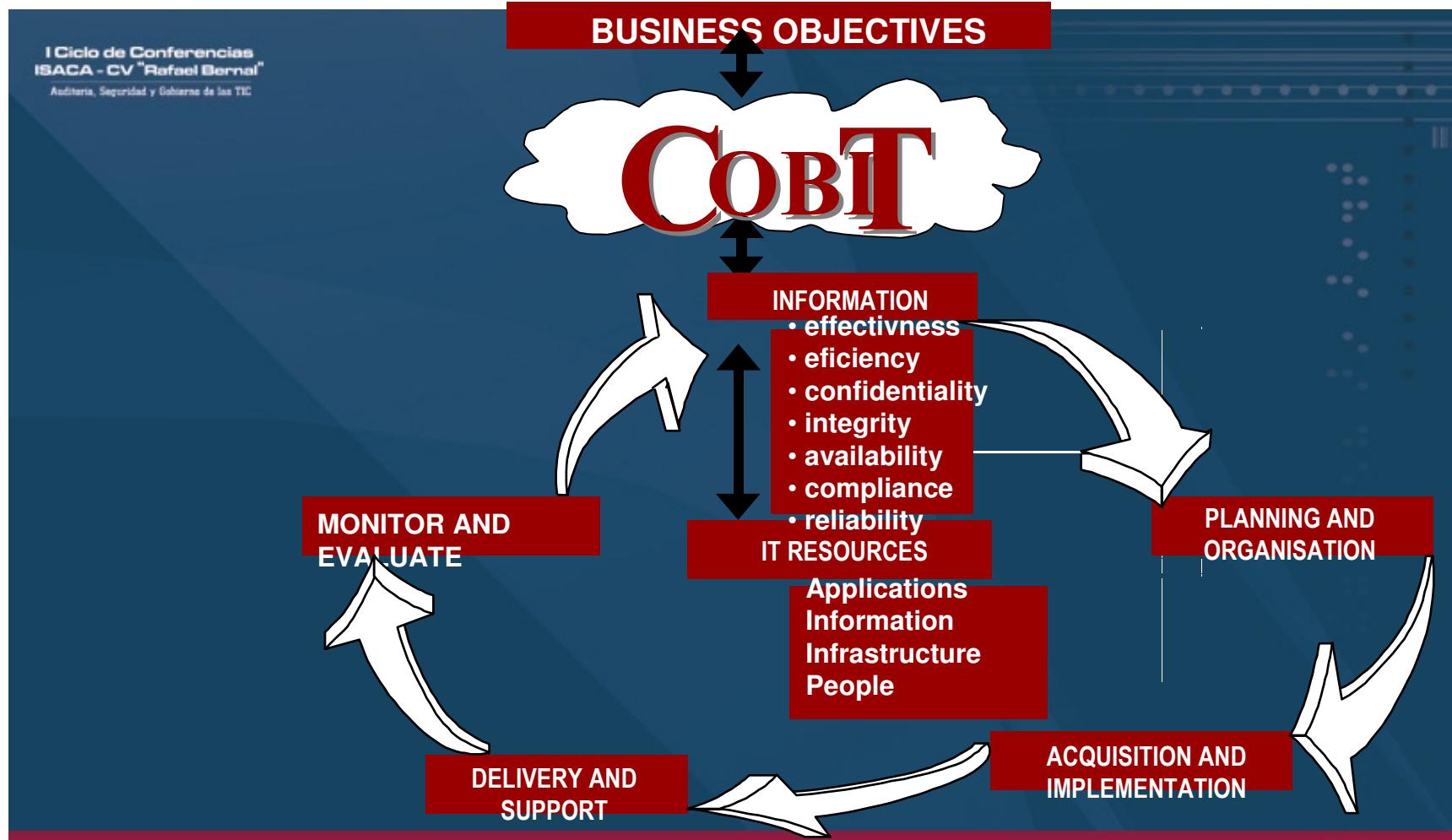
BENCHMARKING → Escalas?

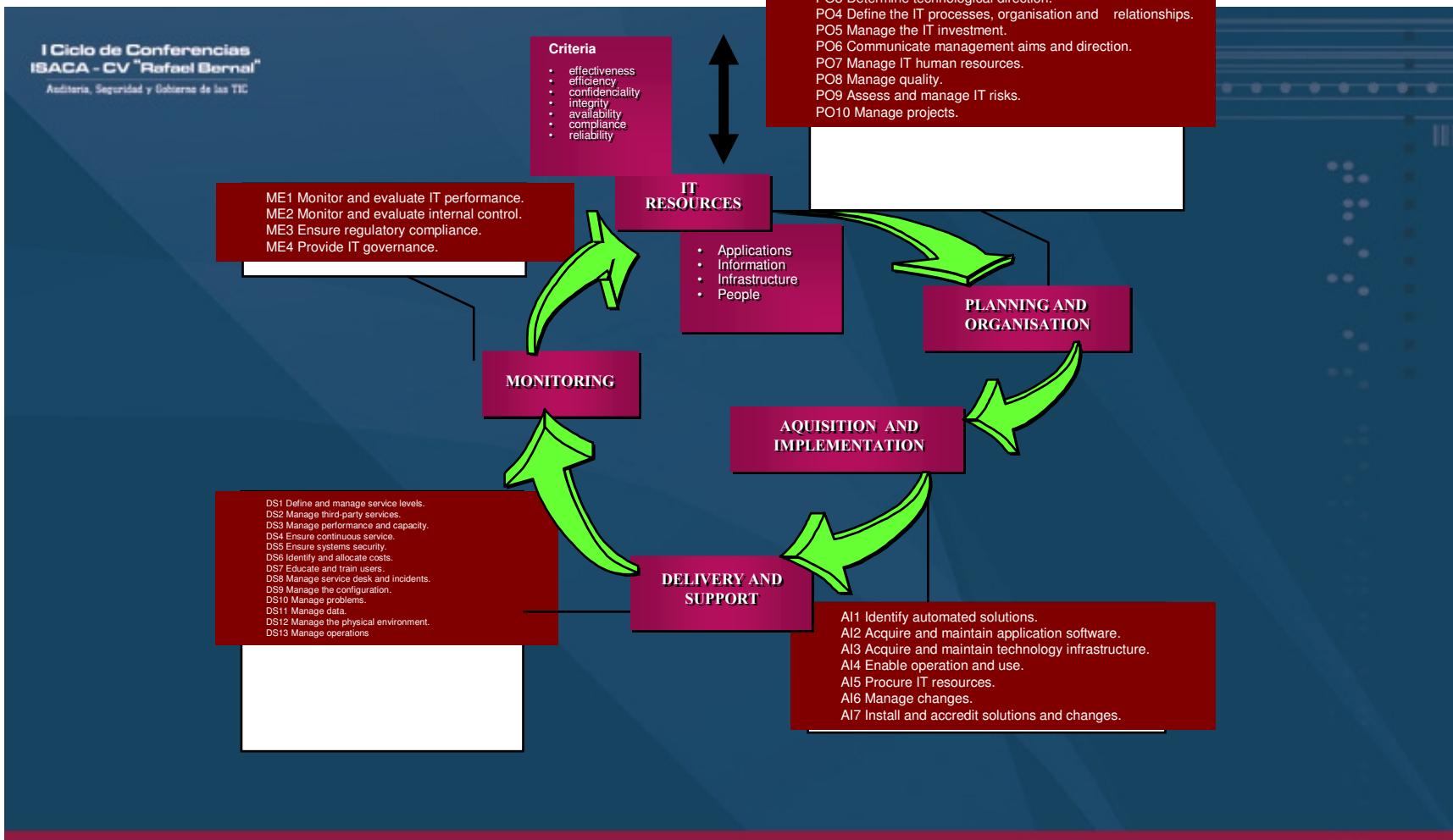


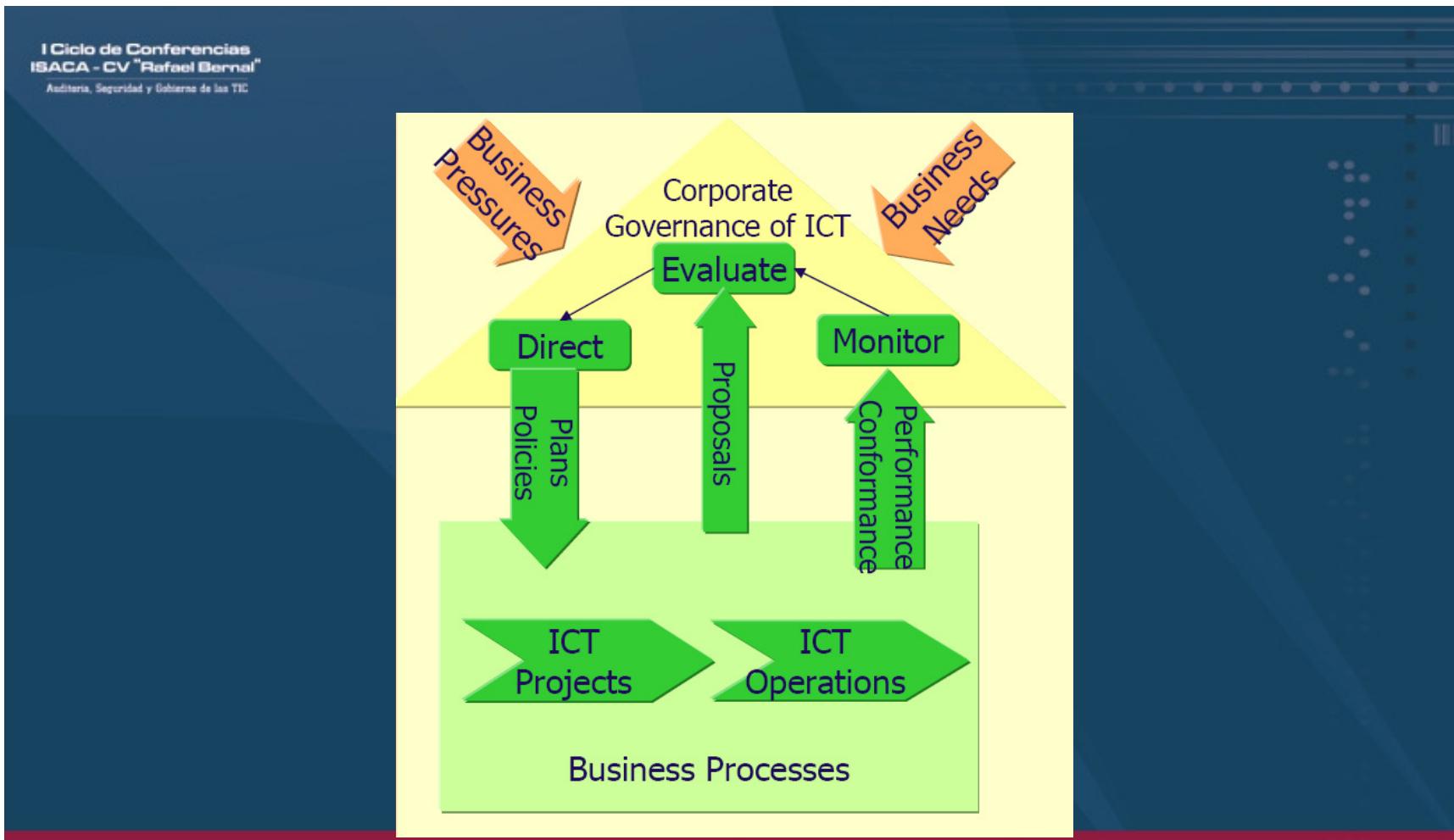


The COBIT “Cube”
(Font IT Governance Institute Cobit 4.0, USA
2005)

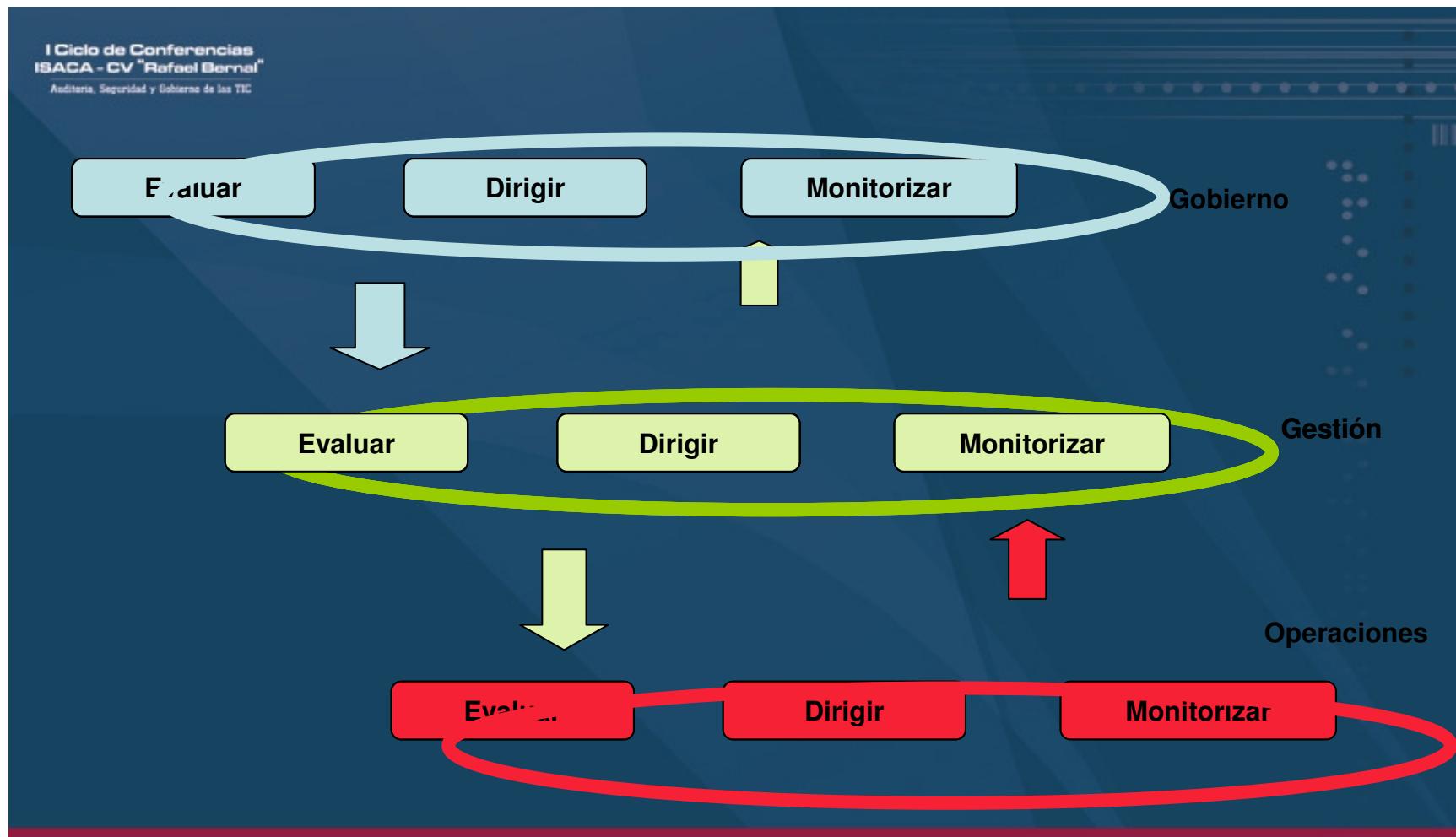








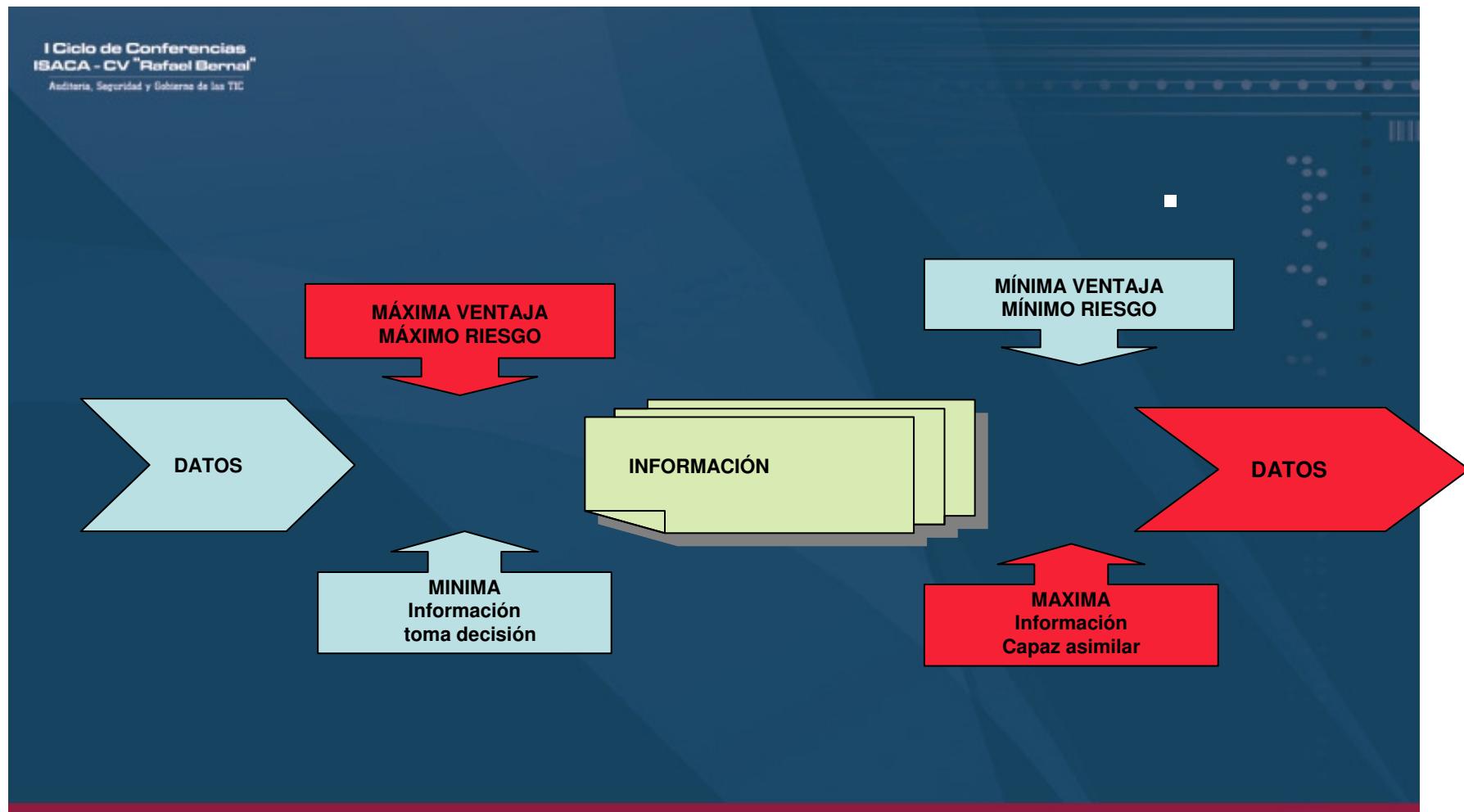
I Ciclo de Conferencias ISACA - CV "Rafael Bernal" Auditoría, Seguridad y Gobierno de las TIC			
Responsabilidad			
Estrategia			
Adquisición			
Performance			
Cumplimiento			
Recursos Humanos			

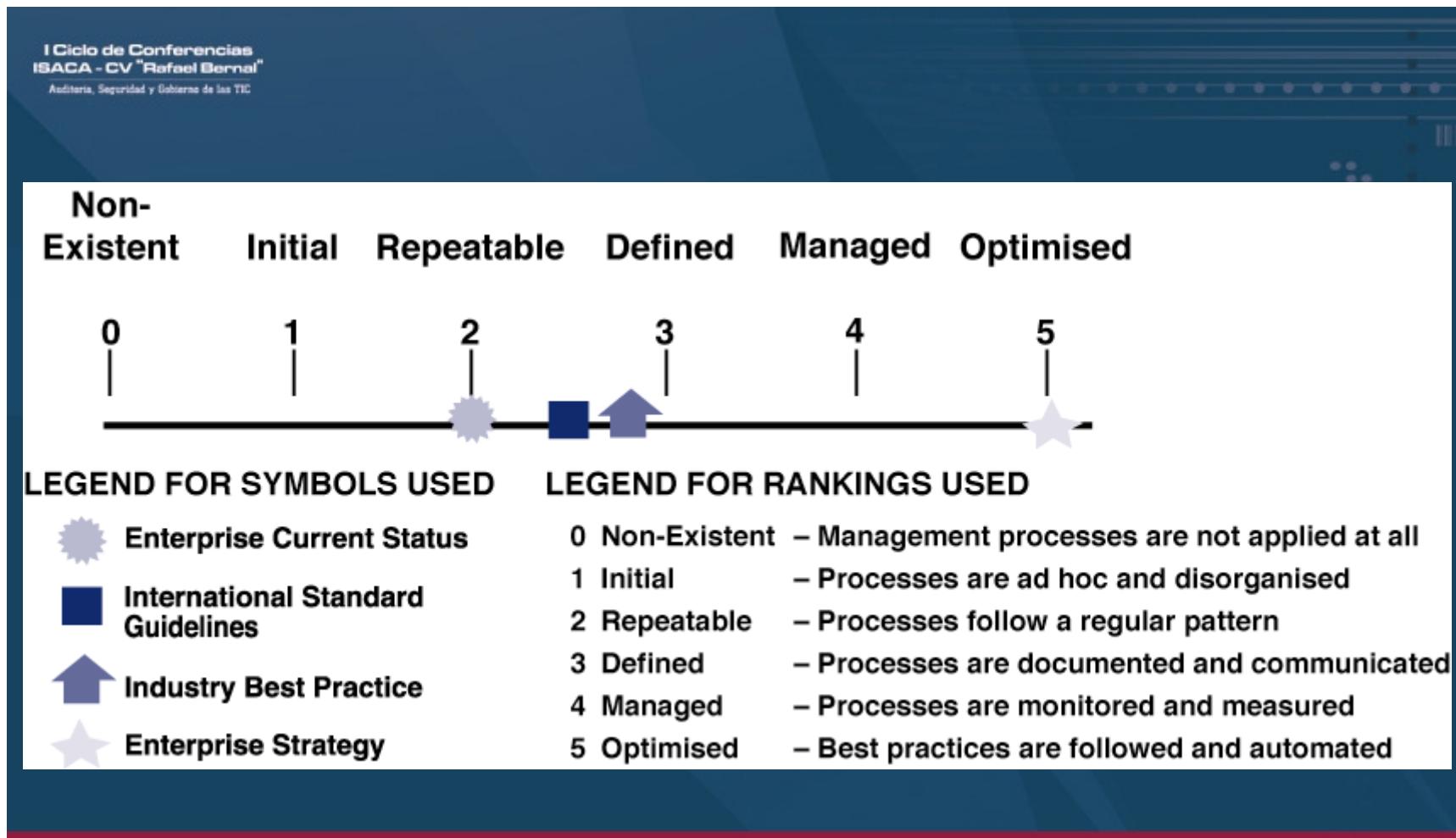


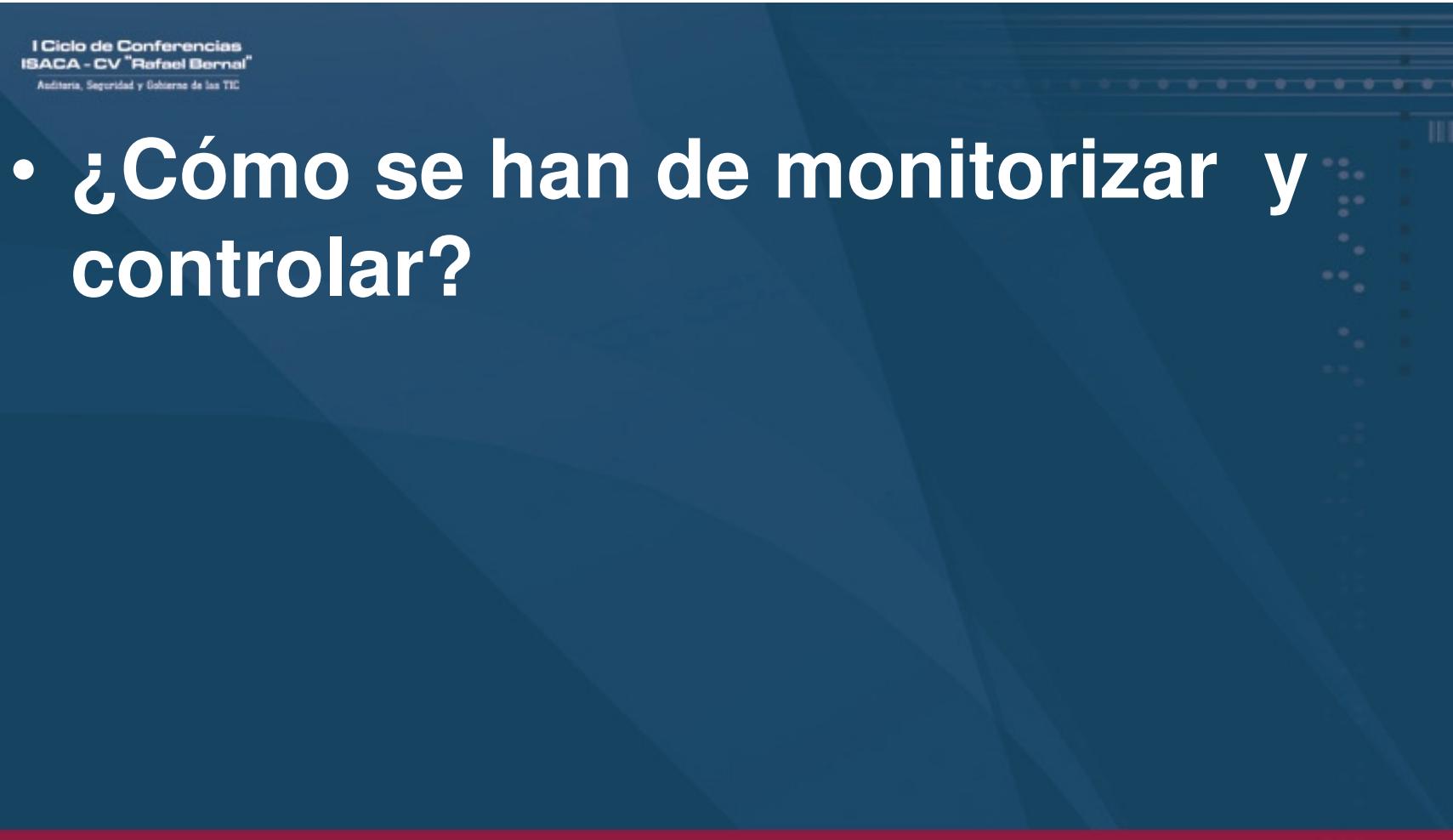
I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

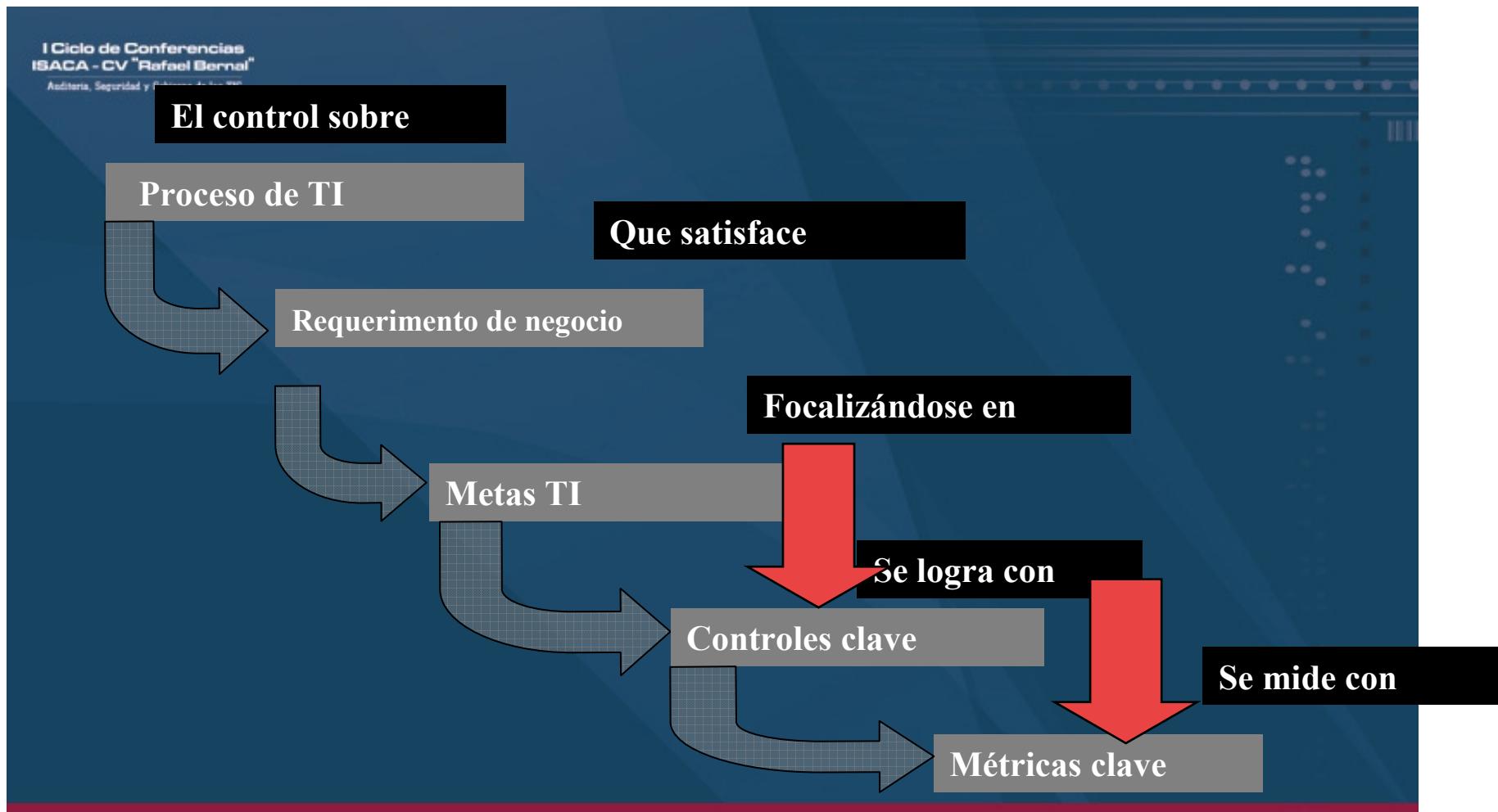
- ¿Cuándo se han de tomar?

¿Cuándo se han de tomar ?

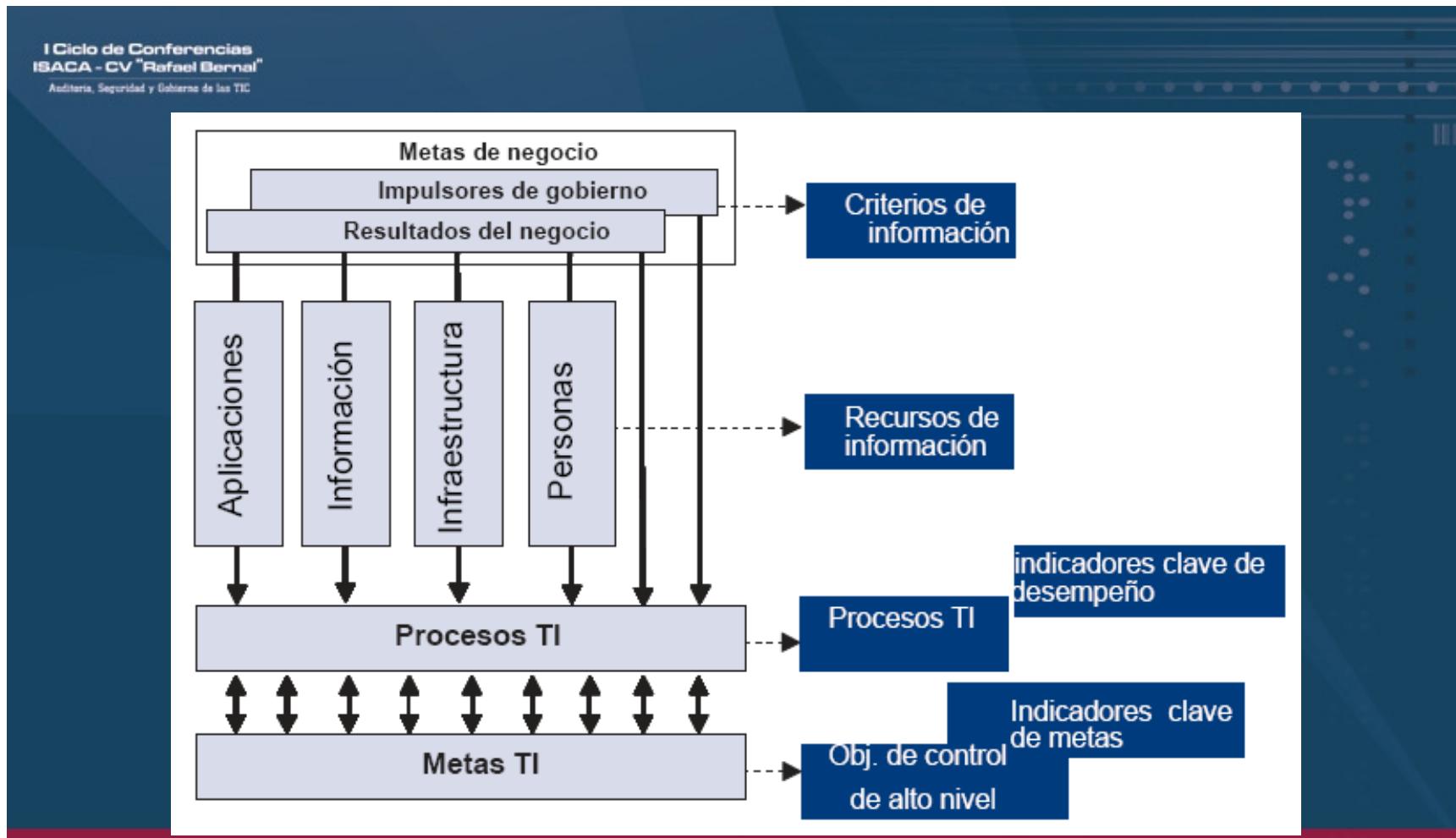


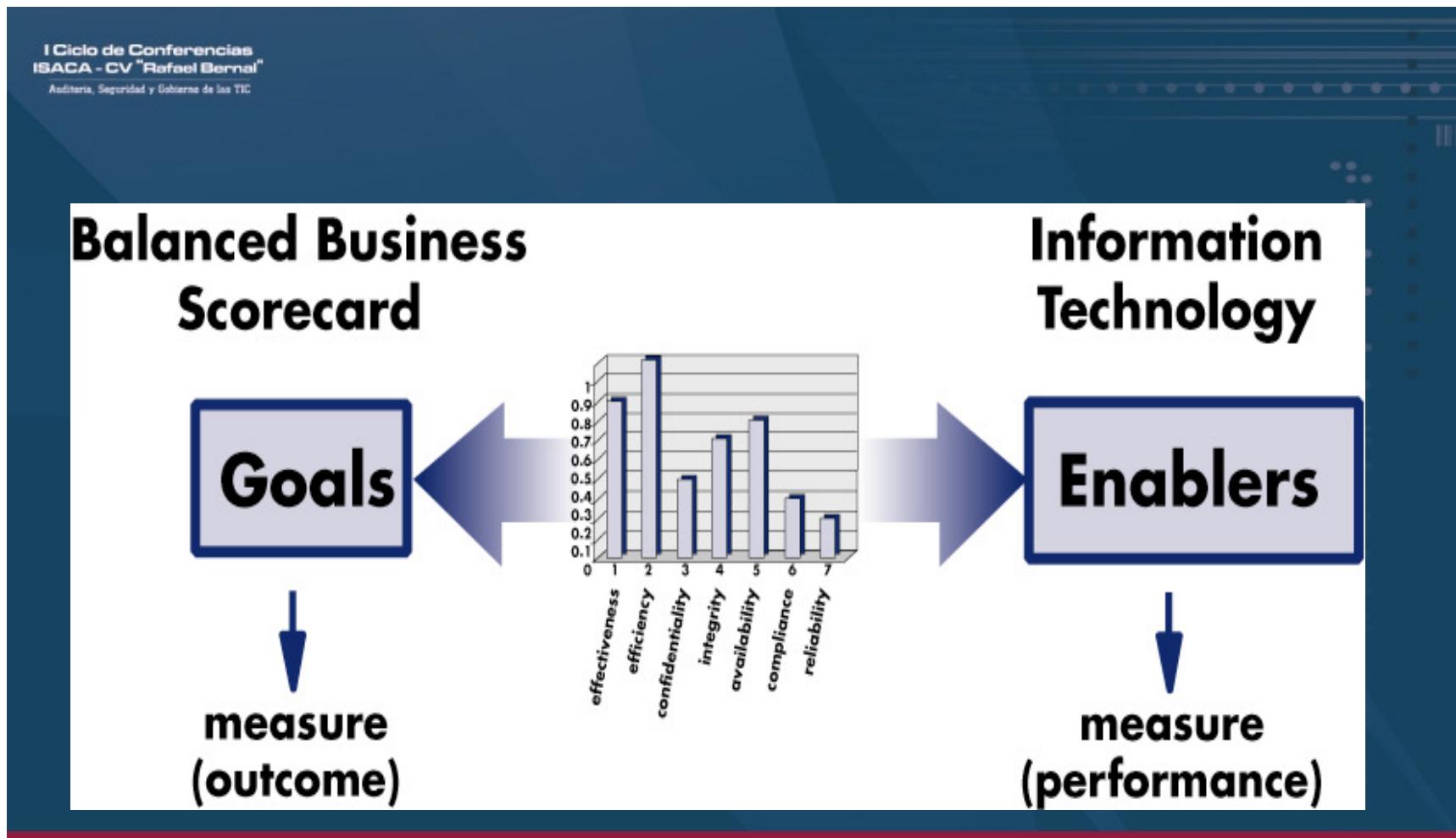


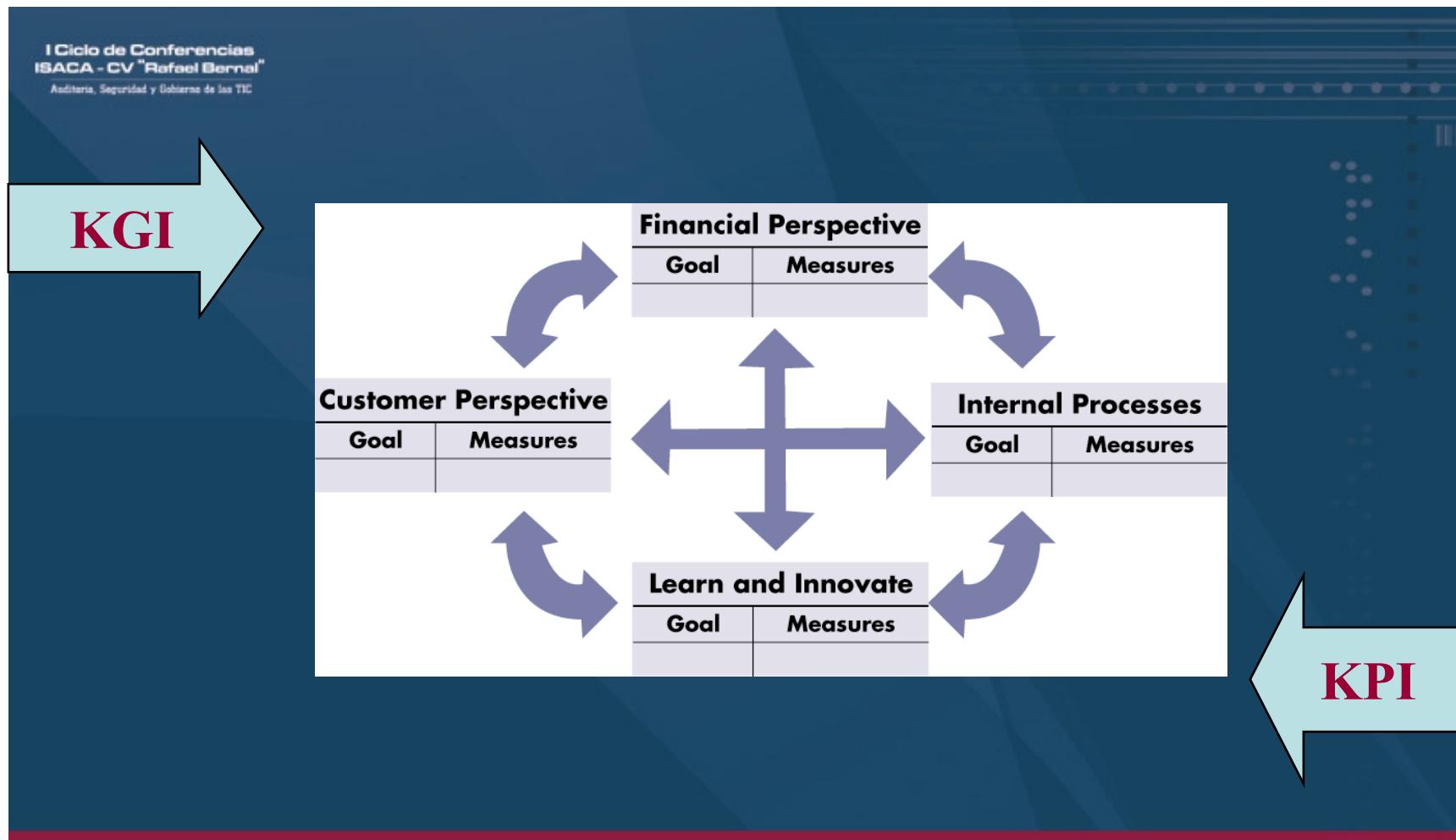




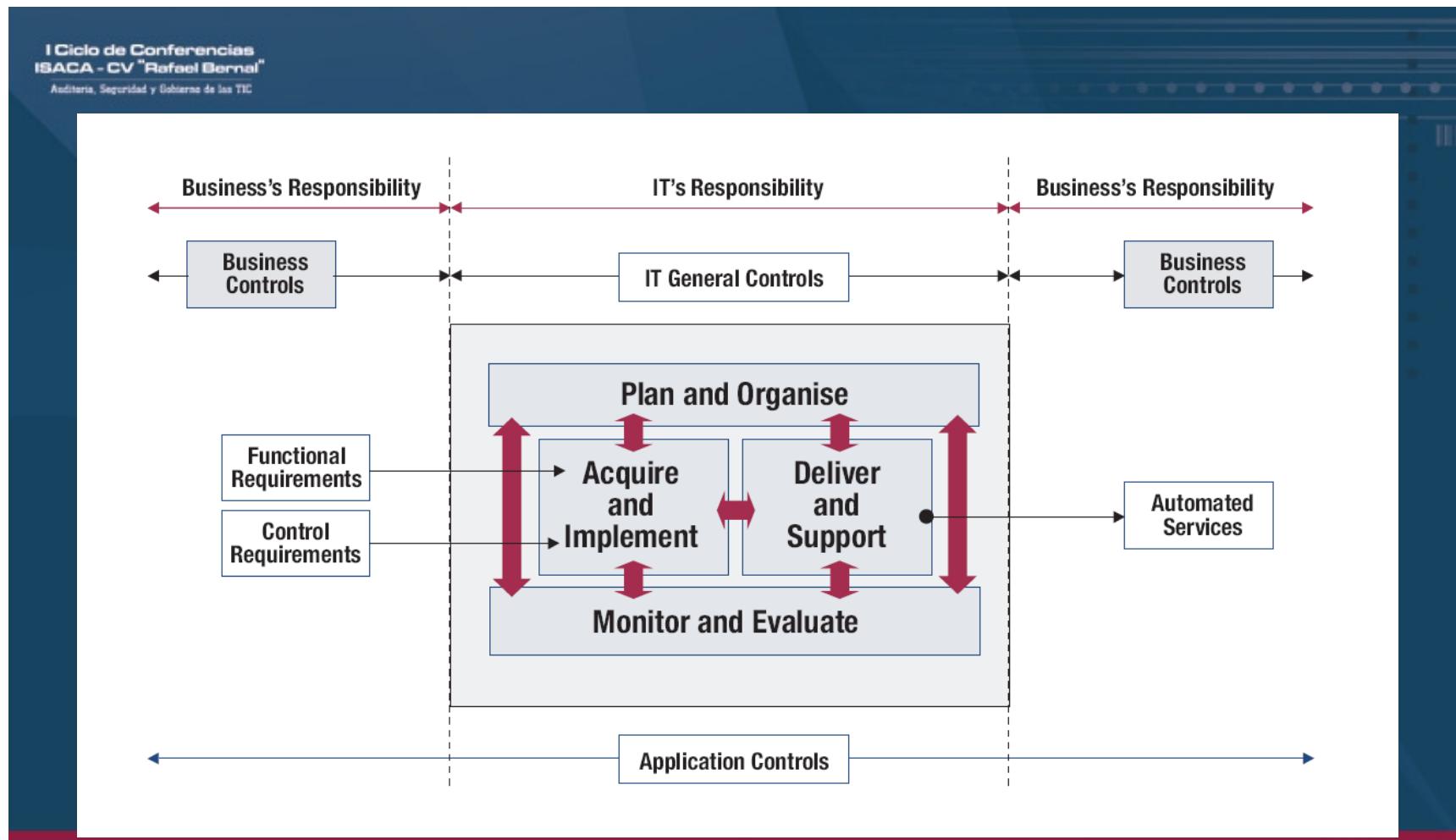
Factores Críticos de Éxito



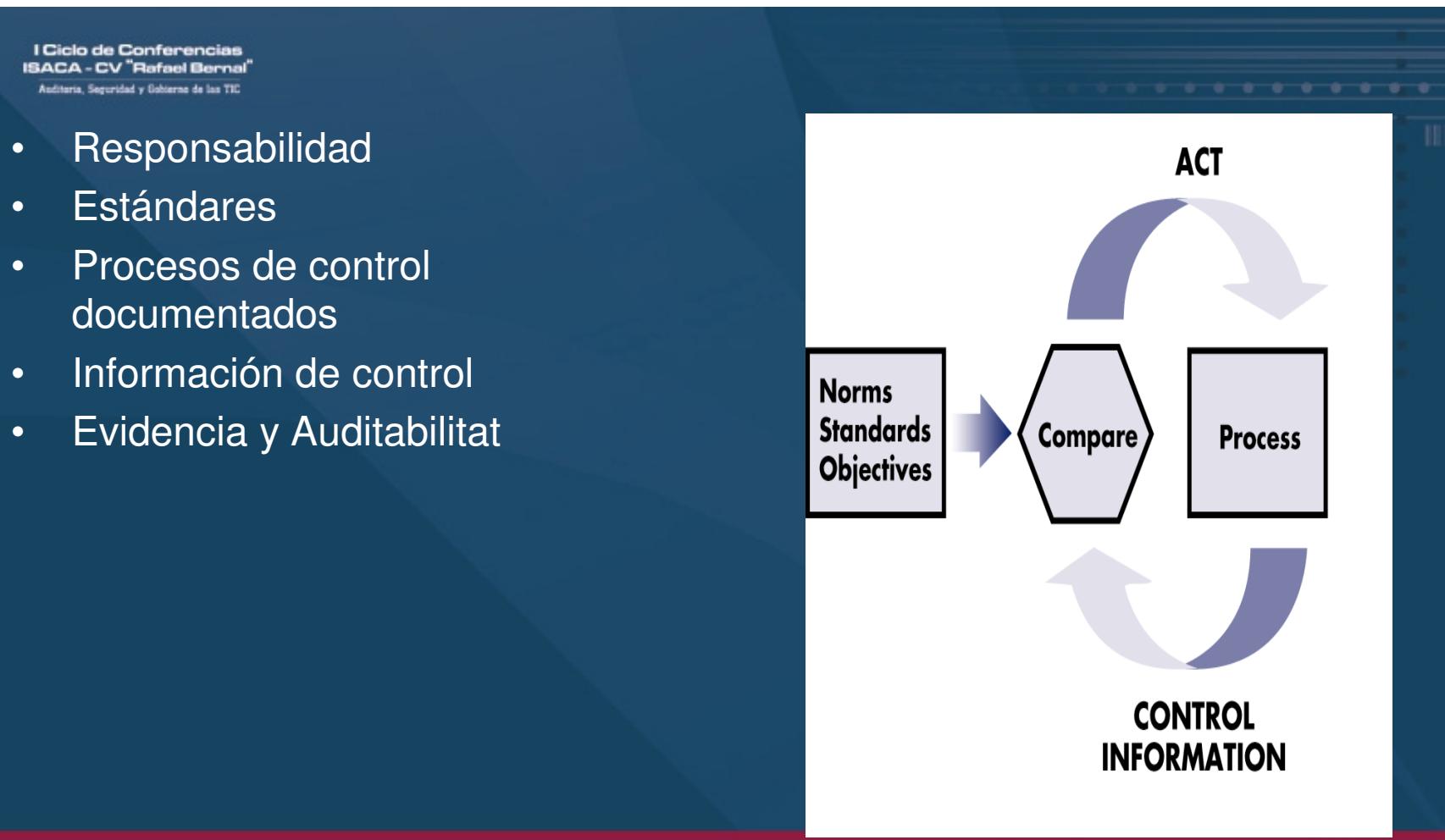


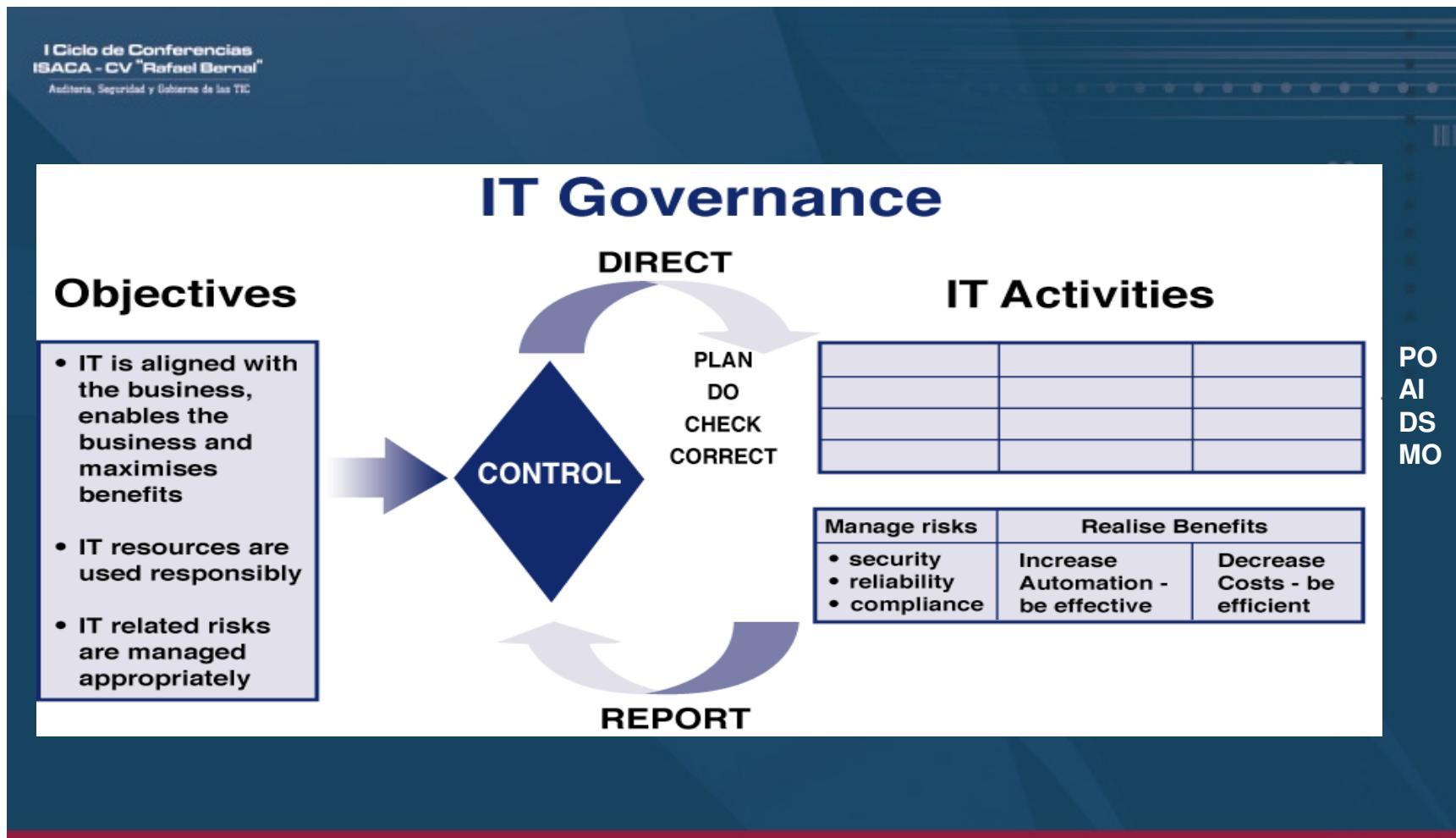


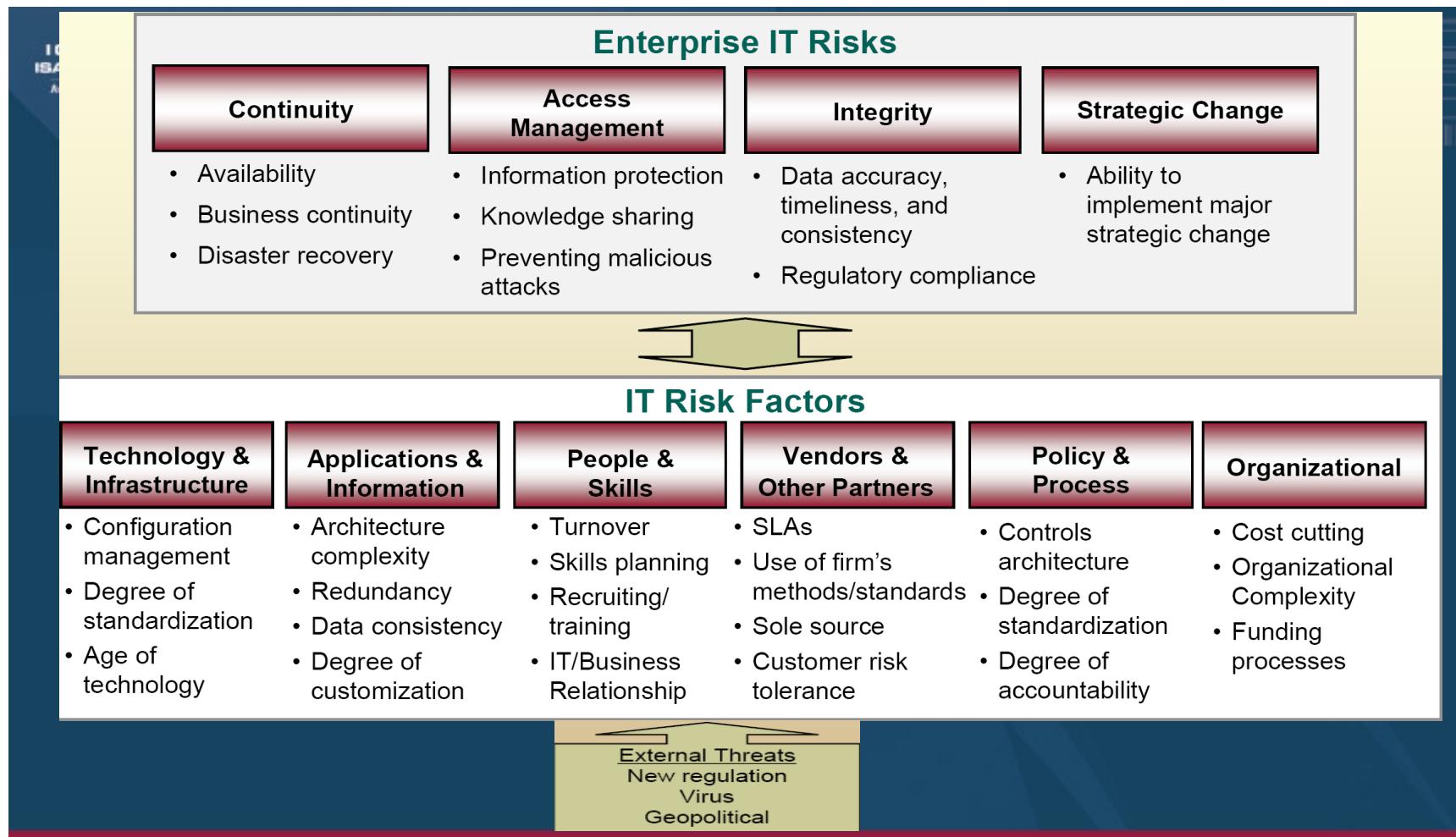
Modelo CONTROL
 (Font IT Governance Institute Cobit 4.1, USA
 2007)

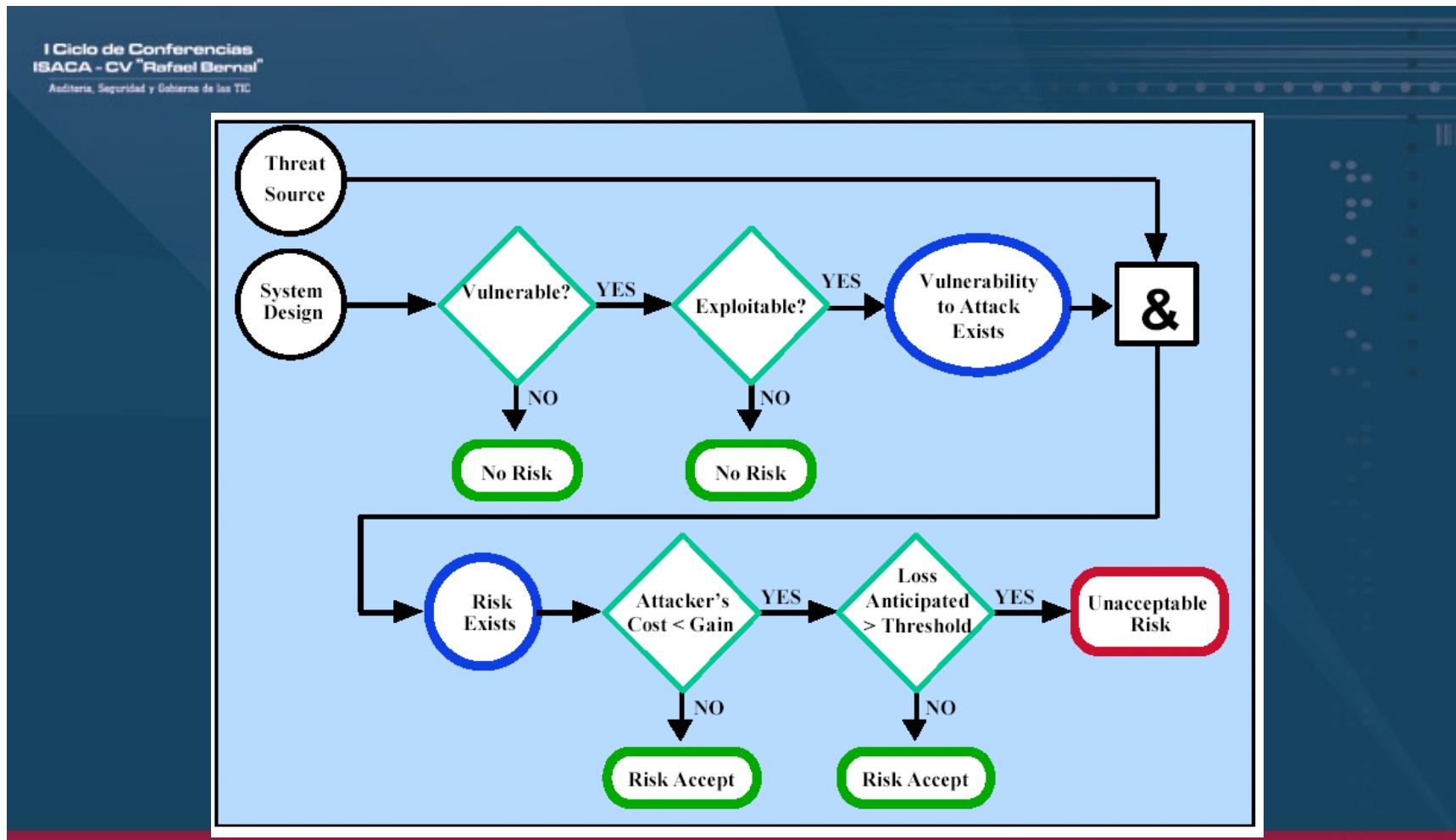


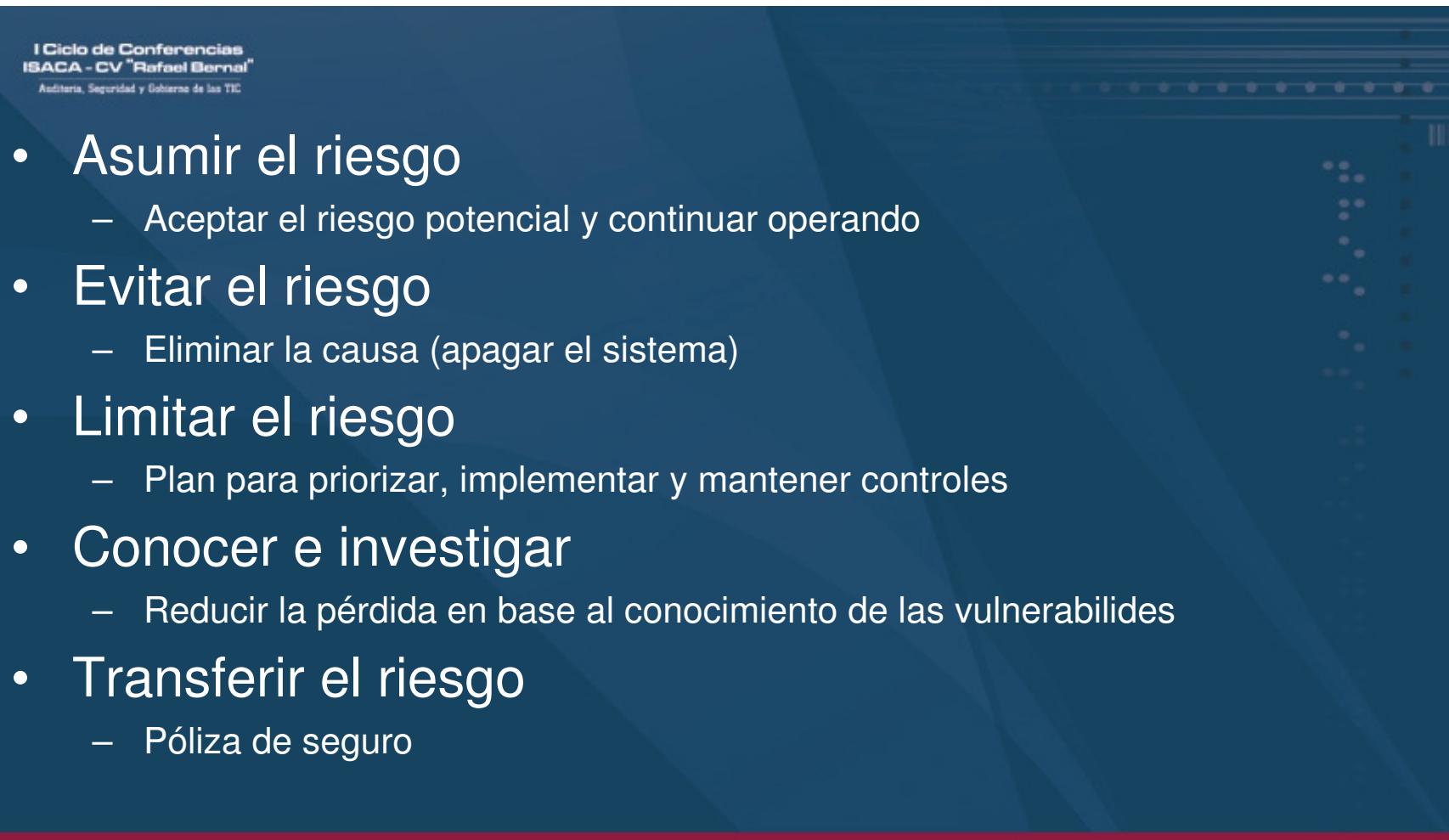
Factores Críticos de Éxito











I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- Asumir el riesgo
 - Aceptar el riesgo potencial y continuar operando
- Evitar el riesgo
 - Eliminar la causa (apagar el sistema)
- Limitar el riesgo
 - Plan para priorizar, implementar y mantener controles
- Conocer e investigar
 - Reducir la pérdida en base al conocimiento de las vulnerabilidades
- Transferir el riesgo
 - Póliza de seguro

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

- 1.- Priorizar acciones
 - Especial énfasis matriz de riesgo ALTO
- 2.- Evaluar recomendaciones de control
 - No siempre los controles recomendados son los adecuados a nuestra organización
- 3.- Analizar coste-beneficio
 - Descripción del coste y beneficio de implementar o no controles
- 4.- Seleccionar controles
 - Deben combinarse controles de gestión, operacionales y técnicos
- 5.- Asignar responsabilidades
 - Personal interno y externo
- 6.- Desarrollar un plan de acción
- 7.- Implementar los controles seleccionados
 - Reduciremos el riesgo pero no lo eliminaremos

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

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

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

EN MEMORIA DE RAFAEL

MUCHAS GRACIAS