Integrando CobiT, ITIL E ISO-27000 como parte del gobierno de TI

Héctor Acevedo Juárez

hacevedoj@scitum.com.mx

CISSP, CGEIT, CISA , ITIL y MCSE

Presentación

- ¿Quién es Héctor Acevedo?
- ¿Y la audiencia?
- ¿Qué expectativas tienen? ¿por qué asistir a ésta charla?

"Hemos aprendido a vivir en un mundo lleno de errores y productos defectuosos como si eso fuera necesario para vivir. Es tiempo de adoptar una nueva filosofía…"

W. Edwards Deming

Agenda

1. Antecedentes.
2. El Gobierno de TI.
3. CobiT, ITIL e ISO-27000 en el Gobierno de TI.
4. Recomendaciones y conclusiones.

Scitum Seguridad

1.- Antecedentes

No más “actos de Dios” (George Spalding)

- Es hora de librarse de la escusa del “acto de Dios” para justificar los problemas y descuidos de TI.

- La próxima vez que alguien le diga “el sistema está caído” (que se traduce como “ocurrió un acto de Dios sobre el cual no tenemos control alguno y como resultado de ello usted está completa, total y absolutamente fastidiado”).

- Su respuesta debería ser “¿POR QUÉ?”.

¿Por qué?

- Falla en el aeropuerto de Los Ángeles (2007).
  - Cientos de aviones debieron permanecer en tierra debido a un problema en los sistemas de aduanas.
  - La falla fue causada por una tarjeta de red defectuosa que eventualmente dejó inoperativa la red y los sistemas de aduanas, por lo que nadie pudo entrar ni salir del aeropuerto en ¡8 horas!

¿Por qué?

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

CIA Admits Cyberattacks Blacked Out Cities

The disclosure was made at a New Orleans security conference Friday attended by international government officials, engineers, and security managers.

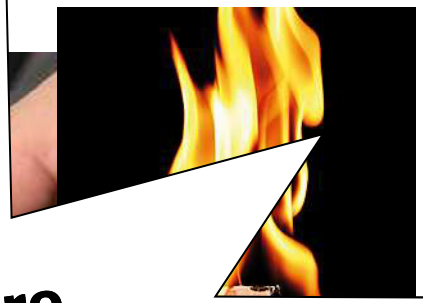
By Thomas Claburn, InformationWeek
Jan. 18, 2008
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=205901631

The CIA on Friday admitted that cyberattacks have caused at least one power outage affecting multiple cities outside the United States.

Alan Paller, director of research at the SANS Institute, said that CIA senior analyst Tom Donahue confirmed that online attackers had caused at least one blackout. The disclosure was made at a New Orleans security conference Friday attended by international government officials, engineers, and security managers from North American energy companies and utilities.

Scitum Seguridad

¿Por qué?



Fraude

Lavado de dinero

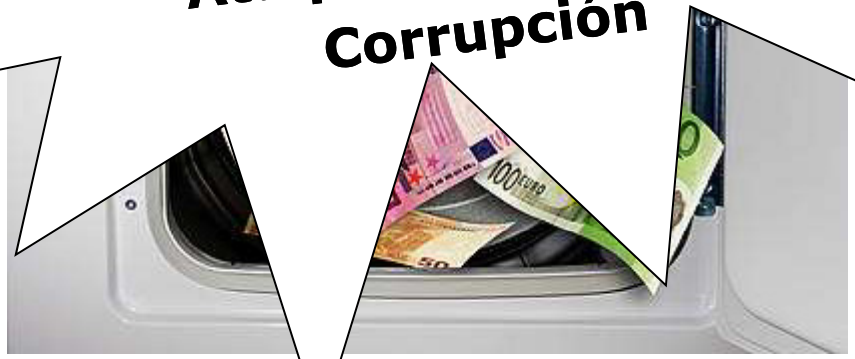
Fuga de información

Falta de elementos para fincar responsabilidades

Robo de identidad

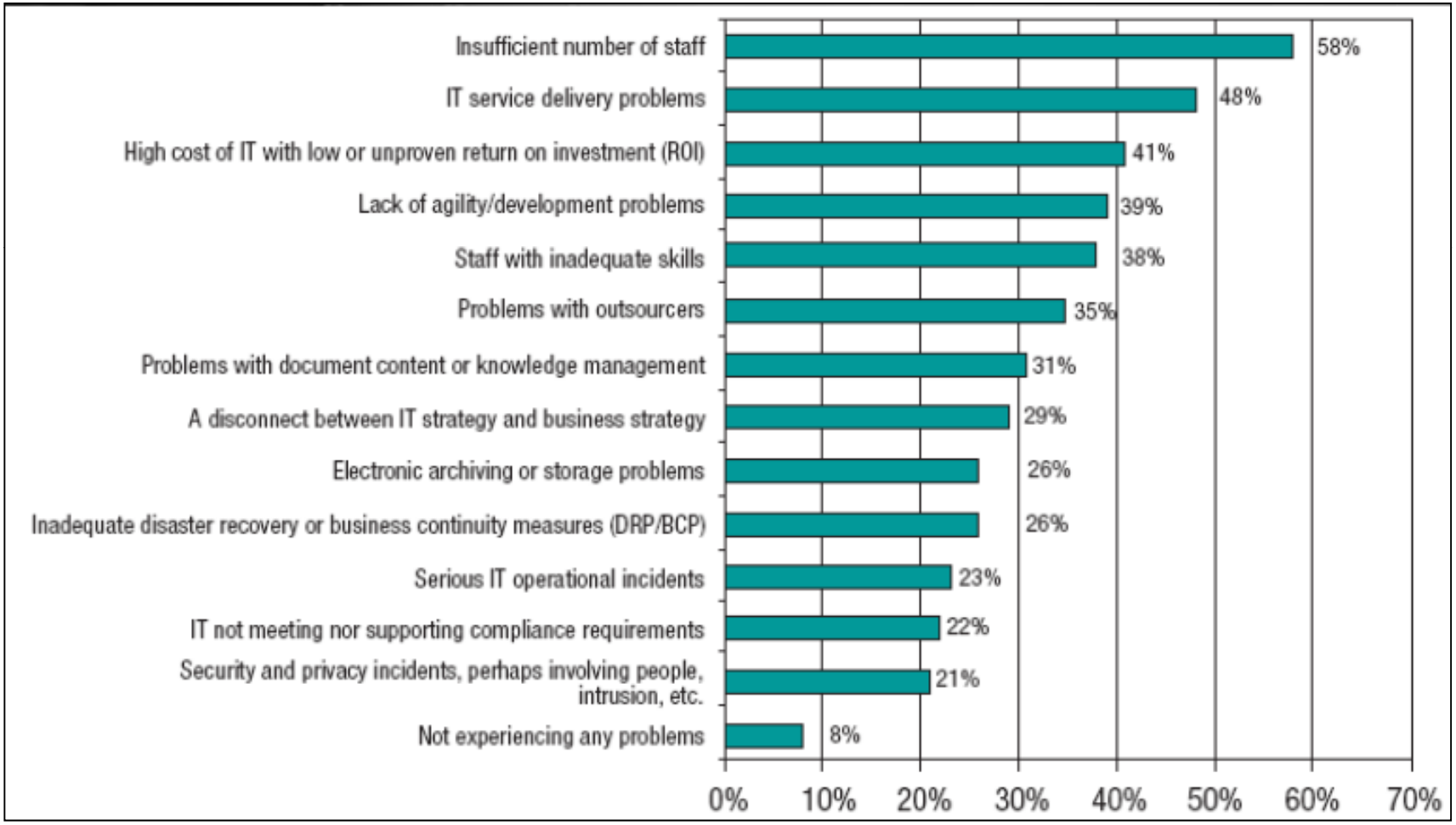
Ataques mediáticos

Corrupción



Scitum Seguridad

Problemas relacionados con TI



Fuente: ITGI – IT Governance Global Status Report 2008

Scitum Seguridad

¿Qué espera el negocio de TI?

#6 "IT to Manage Information" shifts to "IT to Manage the Business"

IDC Analyze the Future

Business Performance Monitoring is among the top 3 business initiatives on the CEO's agenda in Latin America today

While the SW market has been growing on average 10-12%, business-related technologies are gaining in importance

- Advance analytics software will grow over 30% in 2009
- Integration and process automation middleware (IPAM) will grow 13.7%
- CRM forecasted at 11%

Top Business Initiatives for CEOs in 2009

#1 Customer Care
#2 Sales Productivity
#3 Business Perf. Monitoring
#4 Product Innovation
#5 Supply Chain Efficiency

N = 197 CEOs and Business Leaders, Nov 2008

Fuente: IDC Predictions 2009 - Opportunities Among Challenges

Scitum Seguridad

Entonces…

- ¿Cómo se maneja el RIESGO?
- ¿Qué significa tener CONTROL?
- ¿Quiénes son responsables?
- ¿Qué ha pasado cuando no hay control?
  - Quiebra de la industria del transporte aéreo.
  - ENRON.
  - Crisis financiera de octubre de 2008.
  - Y una larga lista…

Scitum
Seguridad

2.- El Gobierno de TI

El Gobierno Corporativo

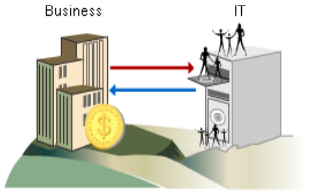
- Es un conjunto de responsabilidades ejercidas por la Junta Directiva y la Alta Gerencia con el fin de:
  - Dar dirección estratégica.
  - Asegurar que los objetivos del negocio son logrados.
  - Evaluar los riesgos y administrarlos apropiadamente.
  - Vigilar que los recursos de la organización son utilizados responsablemente.

El Gobierno Corporativo (cont.)

- El Gobierno Corporativo está relacionado con:
  - Cumplimiento regulatorio.
    - Adherencia a la legislación, políticas internas, requerimientos de auditoría, etc.
  - Desempeño.
    - Mejoramiento de la rentabilidad, eficiencia, efectividad, crecimiento, etc.
- El Gobierno Corporativo direcciona el Gobierno de TI.

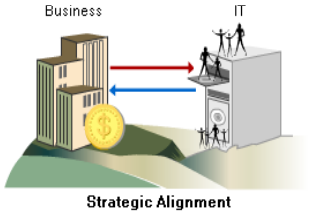
Necesidad del Gobierno de TI

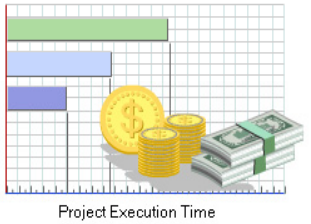
- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.



Necesidad del Gobierno de TI

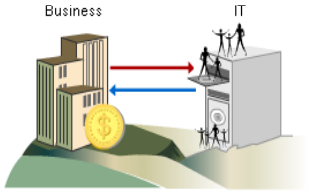
- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.
  - Lograr una buena relación valor/costo.



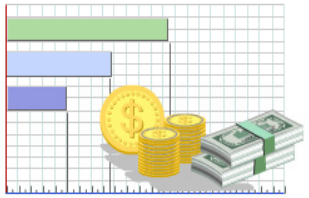


Necesidad del Gobierno de TI

- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.
  - Lograr una buena relación valor/costo.
  - Mantener la seguridad de la información.



Strategic Alignment

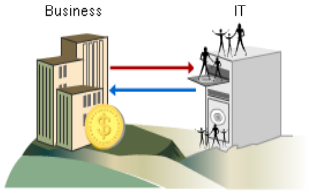

Project Execution Time

Poor Security Assurances

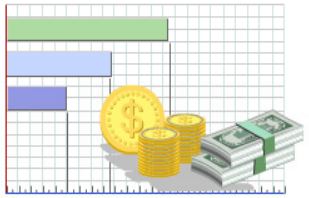
Scitum Seguridad

Necesidad del Gobierno de TI

- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.
  - Lograr una buena relación valor/costo.
  - Mantener la seguridad de la información.
  - Mantener la operación de TI.



Strategic Alignment

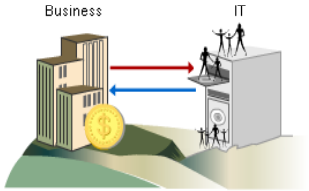

Project Execution Time

Poor Security Assurances

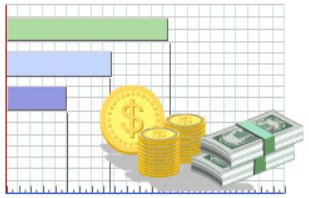
Scitum Seguridad

Necesidad del Gobierno de TI

- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.
  - Lograr una buena relación valor/costo.
  - Mantener la seguridad de la información.
  - Mantener la operación de TI.
  - Administrar la complejidad.



Strategic Alignment


Project Execution Time

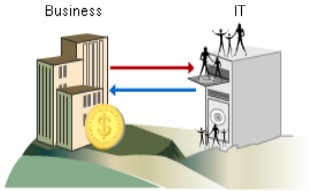
Poor Security Assurances

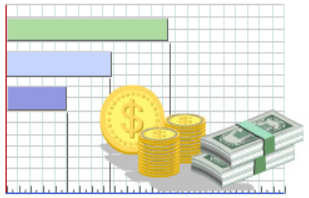
Handling External Relationship

Scitum Seguridad

Necesidad del Gobierno de TI

- El Gobierno de TI surge por la necesidad de:
  - Alinear TI con el negocio.
  - Lograr una buena relación valor/costo.
  - Mantener la seguridad de la información.
  - Mantener la operación de TI.
  - Administrar la complejidad.
  - Cumplir con los requerimientos regulatorios y contractuales.





Scitum Seguridad

Gobierno de TI, de acuerdo al ITGI

- El Gobierno de TI es:
  - Responsabilidad de la junta directiva y la administración ejecutiva.
  - Una parte integral del gobierno corporativo y consta del liderazgo, estructuras organizacionales y procesos que garantizan que TI en la empresa sustenta y extiende las estrategias y objetivos organizacionales.

En resumen

- Se define el Gobierno de TI como la normatividad y mecanismos que instrumentan:
  - La alineación entre el negocio y TI.
  - El control para asegurar que se obtiene el máximo rendimiento de la inversión en TI.

Principales áreas del Gobierno de TI

- Alineación estratégica.
  - Se centra en garantizar el enlace entre los planes de negocio y de TI, con base en la definición, mantenimiento y validación de la propuesta de valor de TI.

- Entrega de valor.
  - Se relaciona con la ejecución de la propuesta de valor a través del ciclo de entrega, garantizando que TI entregue el beneficio prometido contra la estrategia, concentrándose en la optimización de costos.

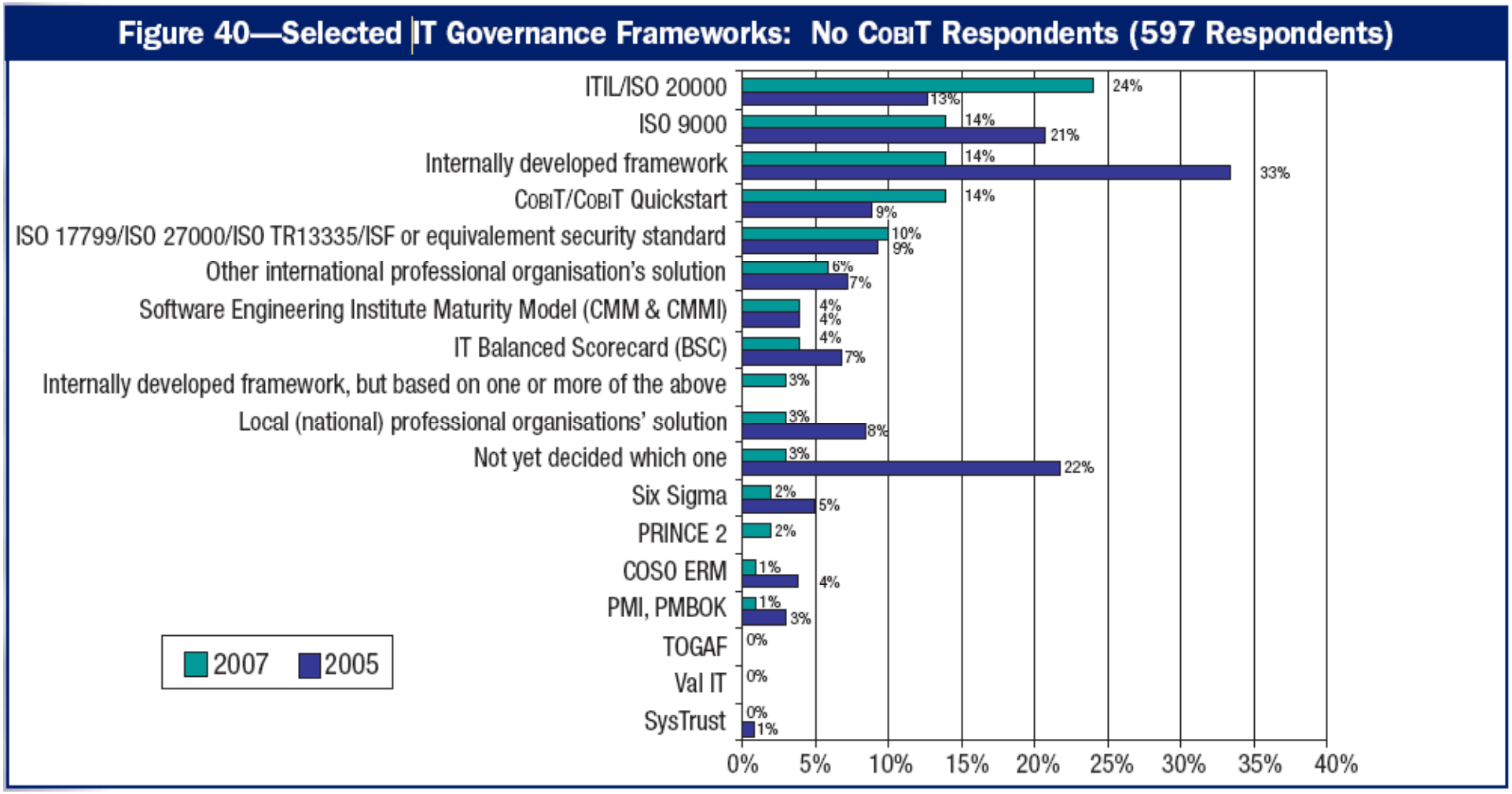
- Administración de los recursos.
  - Se relaciona con la inversión óptima y la administración adecuada de recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los aspectos clave se relacionan con la optimización del conocimiento y la infraestructura.

Principales áreas del Gobierno de TI

- Administración del riesgo.
  - Requiere la concientización del riesgo por parte de la alta gerencia del negocio, un claro entendimiento de la aceptación de riesgo corporativo, un entendimiento de los requerimientos de cumplimiento obligatorio y una distribución de las responsabilidades de la administración del riesgo en la organización.

- Medición del desempeño.
  - Sigue y monitorea la implementación de la estrategia, la finalización de los proyectos, el uso de los recursos, el desempeño de los procesos y la entrega de servicios.

¿Qué están haciendo los demás?



Fuente: ITGI – IT Governance Global Status Report 2008

Scitum Seguridad

Scitum
Seguridad

3.- CobiT, ITIL e ISO-27000 en el Gobierno de TI

¿Por qué combinarlos?

- Implantar la entrega de servicios de TI sin definir previamente los parámetros a monitorear y sin planear revisiones que aseguren el cumplimiento de los objetivos del negocio y el cumplimiento regulatorio es muy riesgoso. Esto se evita combinando CobIT e ITIL.

- Si se agrega ISO-27000 a la mezcla, estaremos asegurando que la seguridad de la información se mantiene de acuerdo al estándar más relevante en la materia.

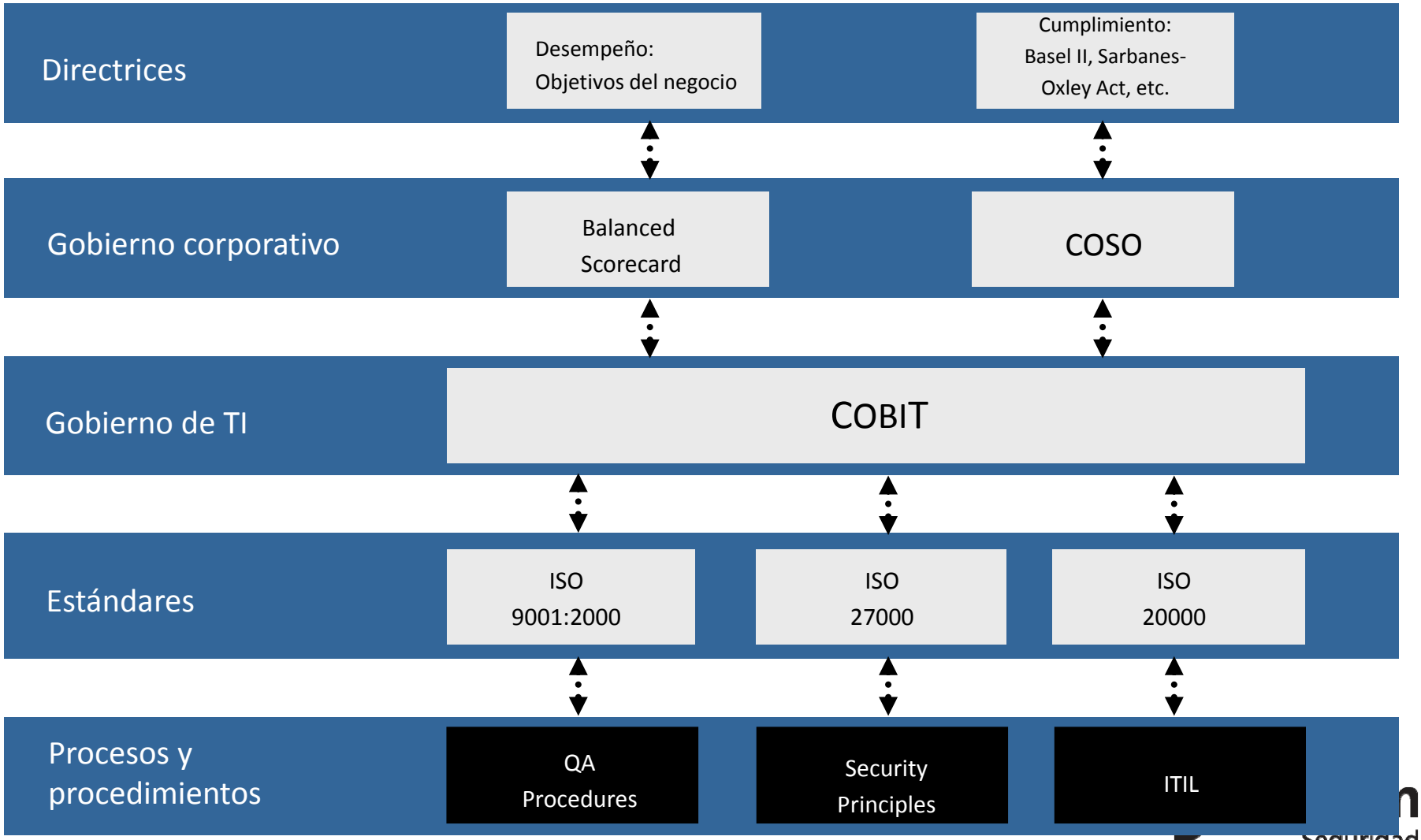
Fortalezas y debilidades

- CobiT es fuerte en controles y métricas de TI, pero no dice “cómo hacer las cosas”. Además no es tan fuerte en cuestiones de seguridad.

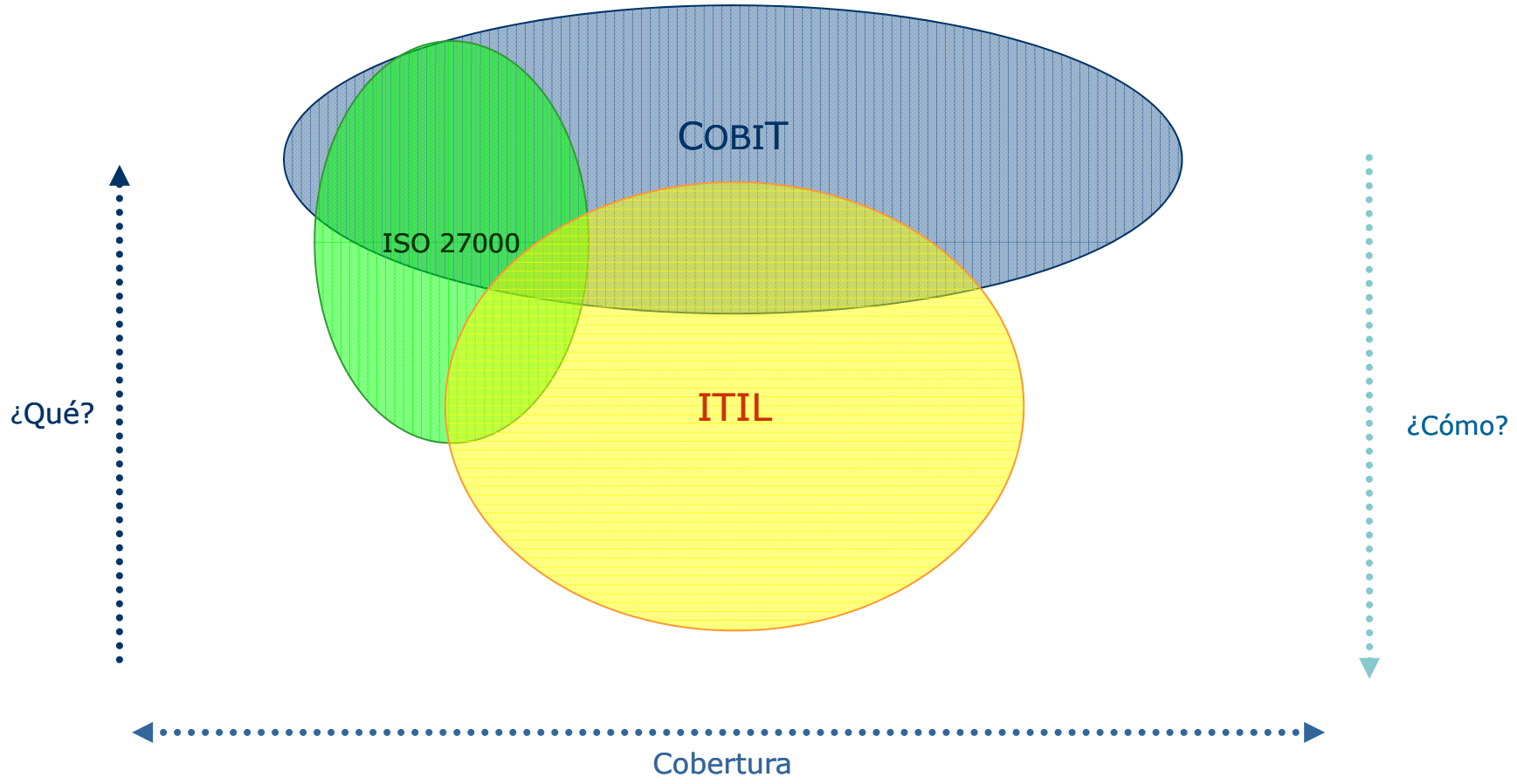
- ITIL es fuerte en procesos, pero tiene grandes limitaciones en desarrollo de sistemas y seguridad, además se enfoca mucho en el “qué hacer” (resuelto parcialmente en V3).

- ISO-27000 tiene su fortaleza principal en los controles de seguridad, aunque no detalla mucho el “cómo hacer las cosas”.

¿Dónde encaja cada uno?



¿Cómo se relacionan? (ISACA)



Scitum Seguridad

¿Cómo se relacionan?

- CobiT e ITIL tienen un buen número de procesos comunes.
- CobiT e ITIL V3 están diseñados pensando en el ciclo de vida de las aplicaciones, sistemas y servicios de TI.
- CobiT, ITIL e ISO-27000 contemplan ciclos de mejora continua (PDCA).
- Las últimas versiones de cada uno tomaron en cuenta a los otros para estar “mejor alineados”.
- CobiT e ISO-27000 consideran controles enfocados a la seguridad de la información.

4.- Recomendaciones y conclusiones

Gobierno de TI

- En estudios hechos por Gartner y el MIT quedó claro que uno de los mejores indicadores de un buen Gobierno de TI es la habilidad de la alta gerencia del negocio para explicar cómo funciona el Gobierno de TI de su organización.

- Toma tiempo lograr el buen Gobierno de TI y el proceso puede ser frustrante.

- El Gobierno de TI no es un ejercicio de una vez ni un proyecto. Es un esfuerzo continuo que requiere el compromiso de la alta gerencia para inculcar una mejor manera de lidiar con la administración y el control de TI.

Gobierno de TI

- Hacer que el Gobierno de TI sea una solución operativa requiere tratar con los retos y dificultades presentados por TI.
- Se debe concentrar tanto en mejorar el desempeño y posibilitar la ventaja competitiva como en prevenir problemas.
- Error común: dejar fuera del gobierno de TI a la alta gerencia del negocio.
- Es importantísimo que a todos los involucrados les quede claro cómo está estructurado el Gobierno de TI, y que dicha estructura contemple la perspectiva de todos los interesados.

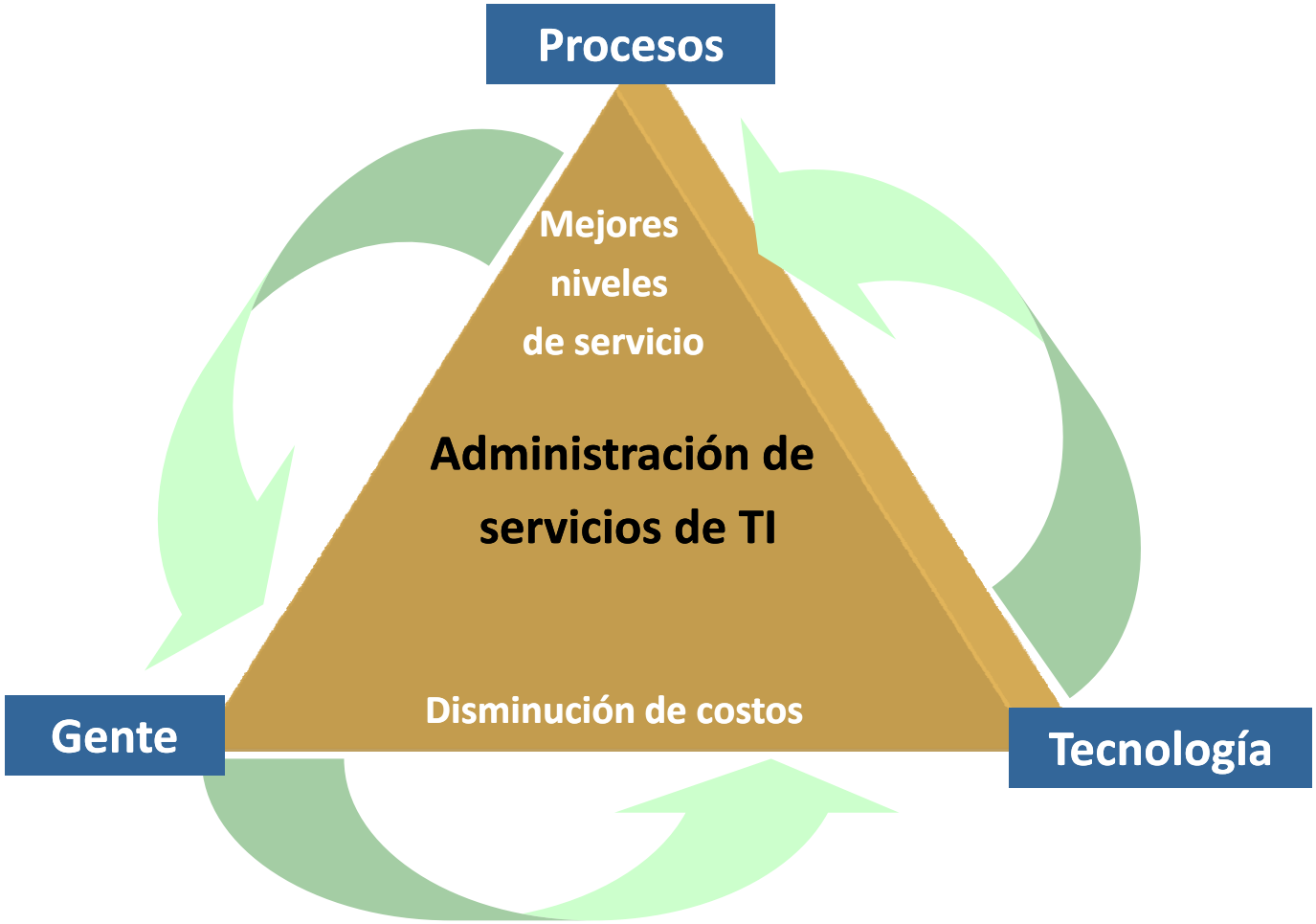
Gobierno de TI

- En el estudio “Why Governance Matters?” se concluye que un Gobierno efectivo de TI es el arma secreta para el éxito de un CIO.

- Aunque suele creerse que el Gobierno de TI consumirá demasiado tiempo y hará la vida más compleja, lo cierto es que sucede lo contario: bien hecho reduce la complejidad y hace la vida del CIO, y de todos los integrantes de TI, más sencilla.

- Una vez que el Gobierno de TI se establece adecuadamente, lo que alguna vez parecieron proyectos de TI se convierten en programas de cambio del negocio facilitados por TI.

El reto: lograr la integración eficiente de…



Scitum
Seguridad

Recomendaciones finales

- No convertir los medios en el fin.
- Dejar atrás los “las religiones”.
- Eficacia antes que eficiencia.
- El mantra del área ideal de TI: “el negocio manda y vivimos para los usuarios, no al revés”.

Finalmente, parafraseando a Esther Dyson

No dejes tu sentido común de lado, piensa primero en lo que quieres mejorar y como los estándares, mejores prácticas y marcos de referencia pueden ayudarte a hacerlo. No pienses primero en ellos…

¡Muchas gracias!

¿Preguntas?

Héctor Acevedo Juárez
CISSP, CGEIT, CISA, ITIL Practitioner y MCSE
Gerente de Soluciones de Servicios - DSA
Scitum, S.A. de C.V.
hacevedoj@scitum.com.mx
91-50-74-00 x 1654