En la misma dirección

Uniendo al Gobierno, Riesgo y Cumplimiento (GRC)

Diciembre 2010

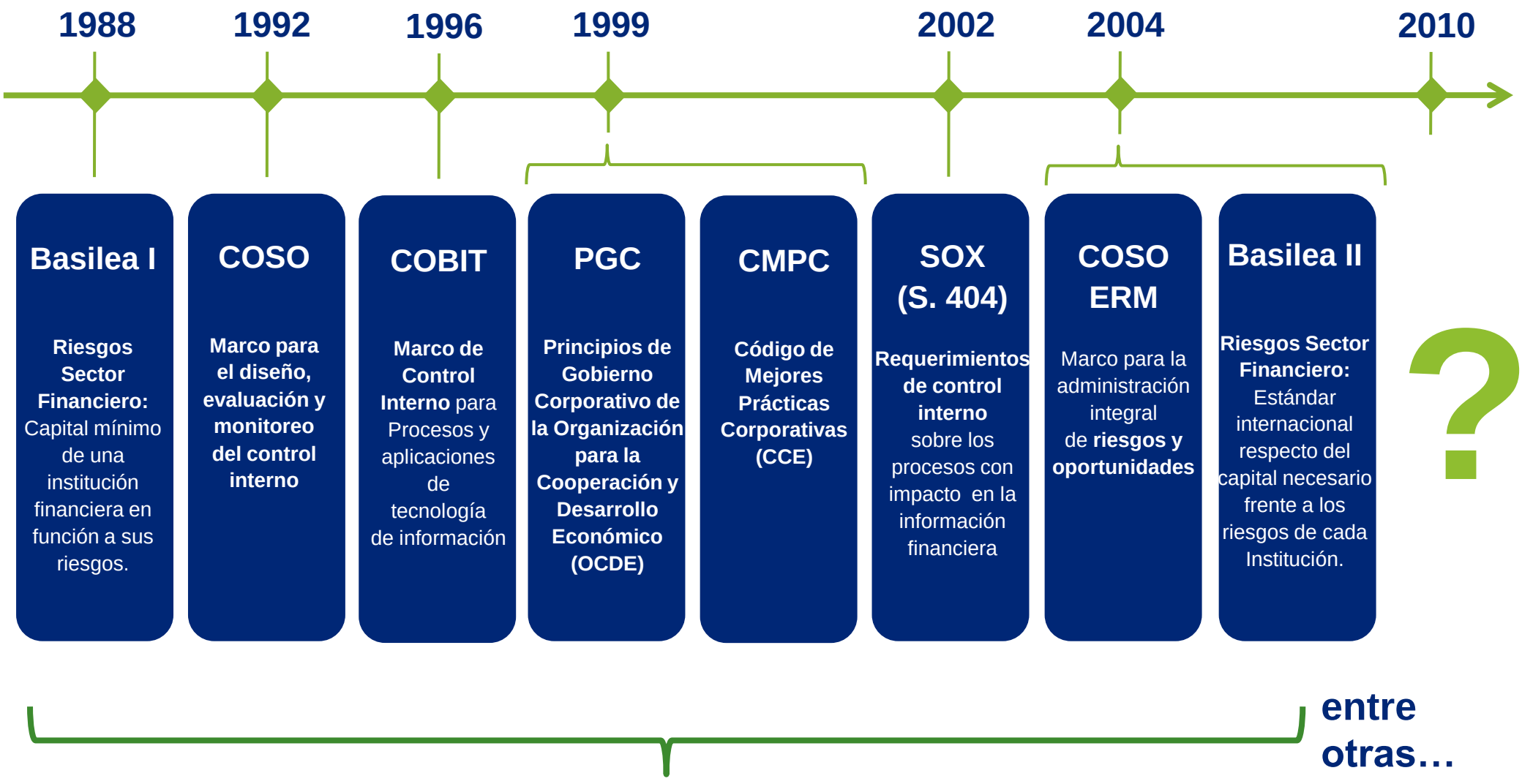
Agenda

El debate de hoy se centra en un modelo de Gobierno riesgo y cumplimiento integrado y automatizado que permita afrontar los desafíos y reducir los costos que trae la implementación de modelos GRC.

- Antecedentes
- ¿Qué es GRC?
- Componentes de un modelo GRC
- Evolución a un modelo GRC

Antecedentes (1)

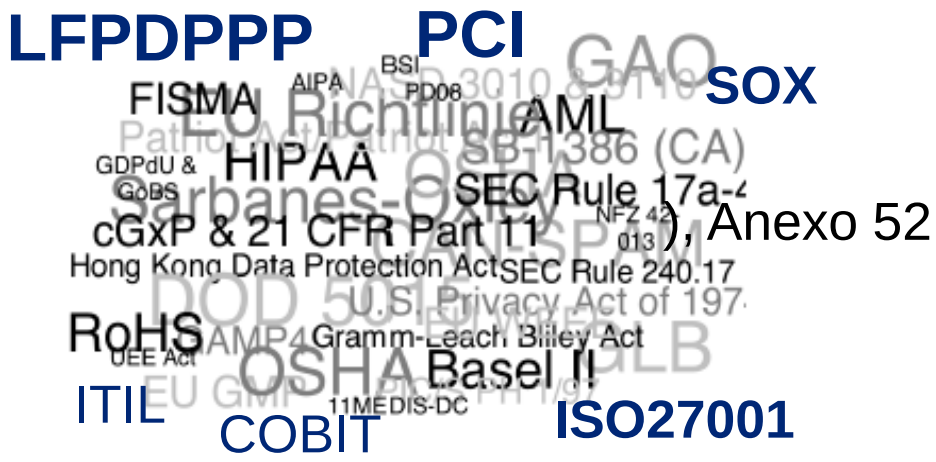
Riesgos, Control Interno y Gobierno Corporativo a través del tiempo



Soluciones adoptadas de manera aislada = SILOS

Antecedentes (2)

Las regulaciones globales y locales están creciendo en volumen y en complejidad. Como resultado, la demanda de responsabilidad legal a los Consejos de Accionistas así como a otros órganos de gobierno y, directamente a los ejecutivos se ha intensificado, a la vez que la administración de los costos asociados a la gestión de riesgo y cumplimiento continúa siendo un reto.



Retos de cumplimiento

- Requerimientos legales o de industria (ejemplo: PCI -DSS, LFPDP etc.)
- Demostrar la adopción de practicas comunes (ejemplo: COSO, ISO31000, ISO27001, ITIL, COBIT, ISO20000, etc.)
- Prácticas internas (ejemplo: políticas, procedimientos, estándares, etc.)
- Interacción con diferentes funciones y terceros (proveedores de servicio)

Incremento del espectro de responsabilidades

- Administración de riesgos
- Administración de cumplimiento
- Seguridad de la información
- Seguridad física
- Continuidad del negocio
- Recuperación ante desastres
- Protección de datos

Antecedentes (3)

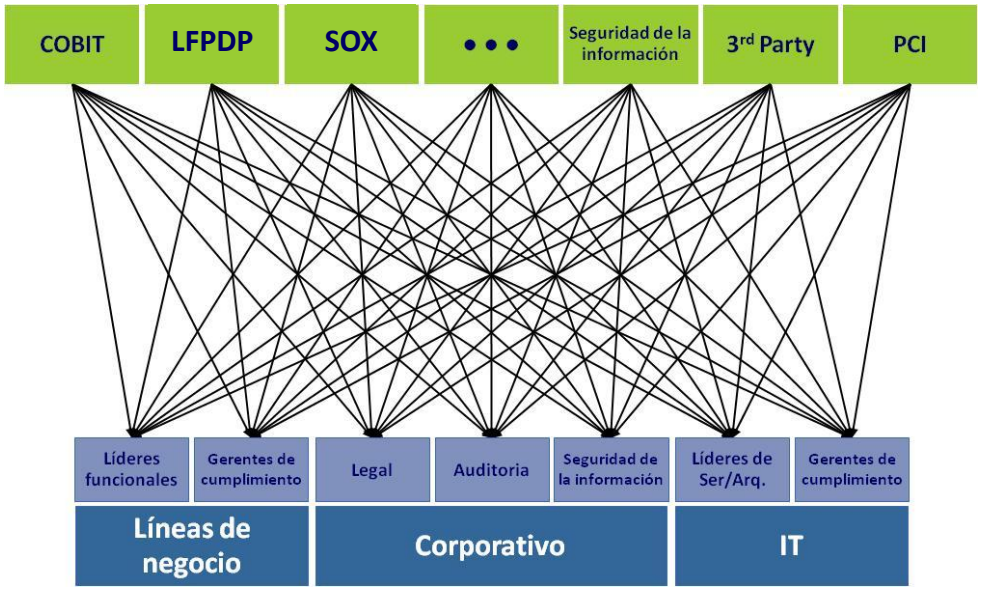
Silos

La adopción de soluciones de manera aislada deriva en la generación de silos [1].

[1] Silo: unidad o área de negocio que tiende al aislamiento debido a su giro, geografía, especialidad o función.

Antecedentes (4)

Programas en silos



Costos elevados

- Esfuerzos duplicados debido a la falta de una única fuente de riesgos y requerimiento de controles de negocio .
- Altos costos y esfuerzos extra para cumplimiento – ¿cuál es el mínimo necesario para cumplir? -
- Pensamientos sobre el peor escenario.

Ineficiencia e inconsistencias

- Las diferentes funciones ven los requerimientos, ambiente operativo, riesgos y controles de manera diferente.
- Auditoría, cumplimiento, seguridad de la información, continuidad del negocio, riesgos de TI y terceros usan un diferente proceso y herramientas para producir los mismos resultados.
- Reportes inconsistentes de riesgos
- Falta de habilidad/herramientas para realizar análisis de tendencias
- Inconsistencia en métricas y criterios
- Falta de indicadores, no existe un análisis predictivo

Antecedentes (5)

En conclusión las empresas suelen enfrentar los siguientes problemas con el **enfoque tradicional**, :

- Fragmentación en silos[1]
- Adopción de filosofías o enfoques diferentes y en ocasiones opuestos
- Desaprovechamiento de sinergias y/o mejores prácticas internas
- Duplicación de esfuerzos y/o mayor carga para ciertas áreas o funciones
- Falta de estandarización en las operaciones
- Ausencia de colaboración
- Visibilidad limitada para la toma de decisiones
- Esfuerzos de cumplimiento regulatorio aislados, reactivos y sin valor agregado

[1] Silo: unidad o área de negocio que tiende al aislamiento debido a su giro, geografía, especialidad o función.

¿Qué es GRC?

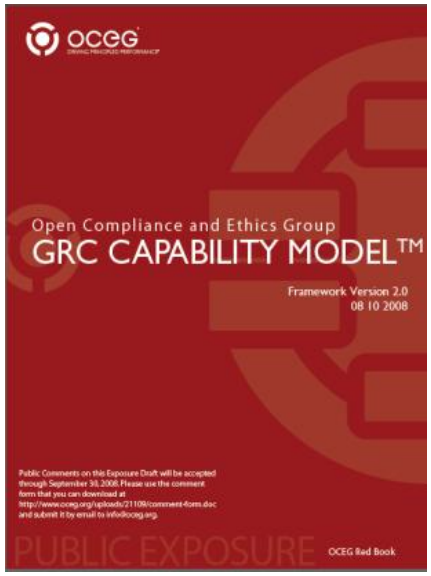
¿Qué es GRC?

Marco de referencia

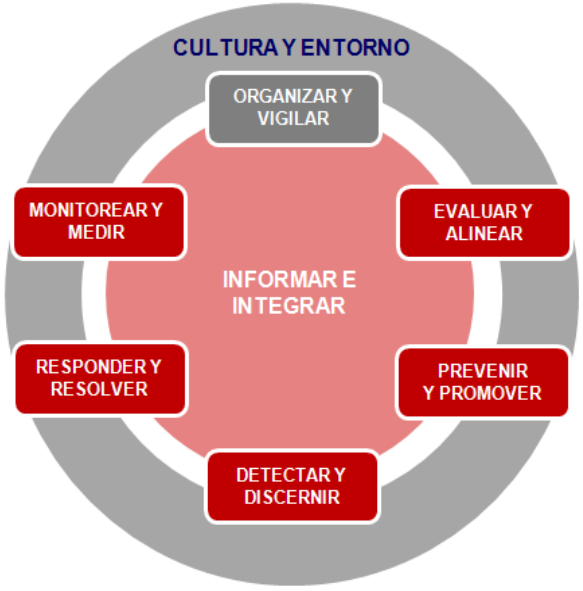
En 2008 el OCEG (Open Compliance and Ethics Group), en el que **Deloitte participa como miembro del Consejo de Liderazgo**, emitió un marco de referencia para la integración del Gobierno Corporativo, la Administración de Riesgos y El cumplimiento regulatorio.

El “GRC Capability Model” (Red Book), provee un marco conceptual para el desarrollo, implementación y seguimiento de un modelo de GRC y su herramienta tecnológica.

http://www.oceg.org/



OCEG – Red book

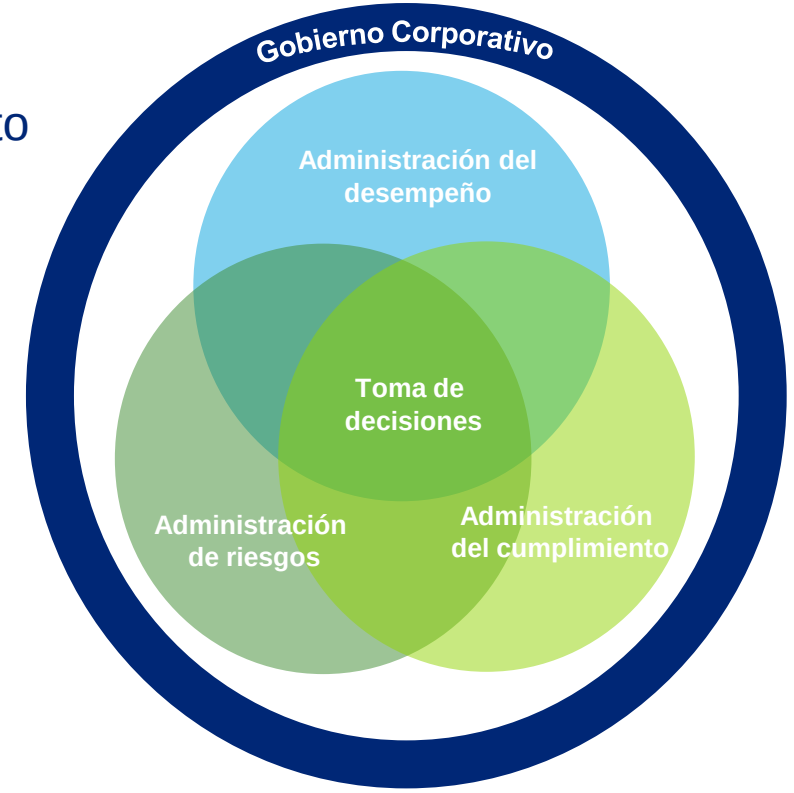


Los 8 componentes de GRC - OCEG

¿Qué es GRC?

GRC es un modelo de gestión que promueve la unificación de criterios, la coordinación de esfuerzos y colaboración entre los diferentes involucrados en la dirección de la organización; a través de:

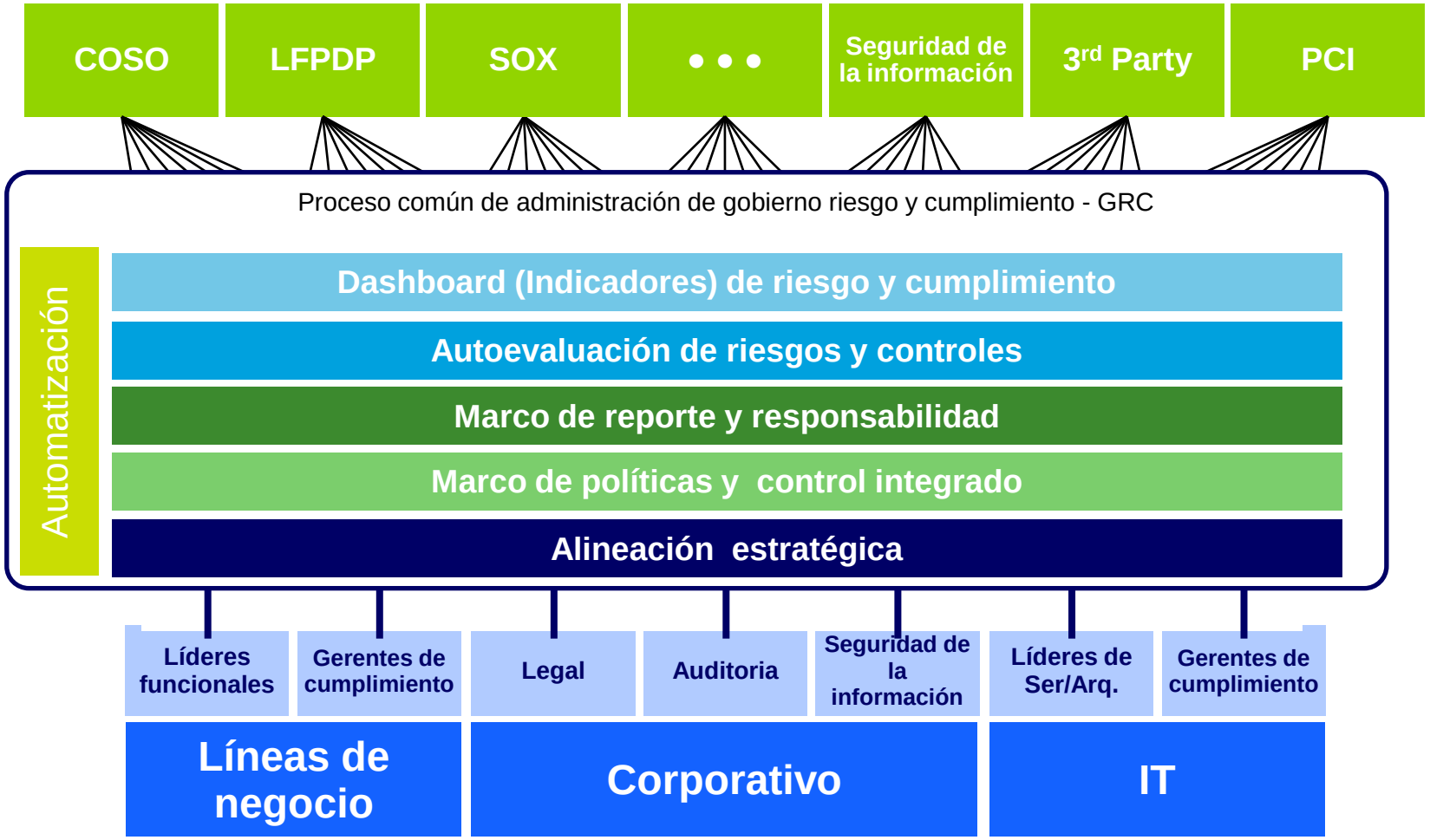
- La integración de los órganos/responsables del gobierno, la administración y gestión de riesgos, el control interno y el cumplimiento
- La asignación puntual de roles y responsabilidades del personal clave
- La formalización de los canales de comunicación
- La aplicación de un enfoque basado en riesgos
- La implementación de un programa de cumplimiento



Componentes de un modelo GRC

Componentes de un modelo GRC

Gráficamente, **los componentes** de un modelo de GRC incluyen:



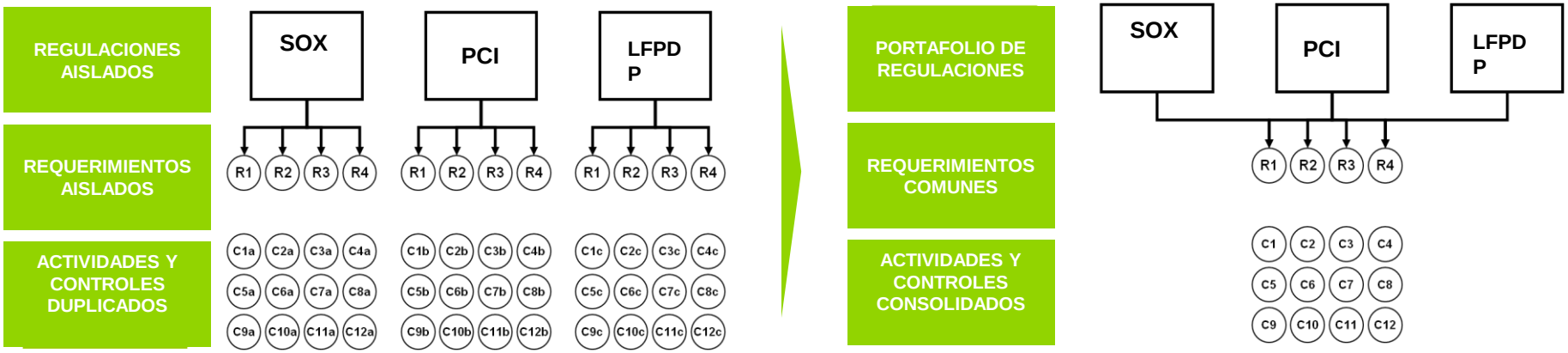
El esquema de armonización que ofrece GRC

Requerimientos sobrepuestos

El enfoque actual de cumplimiento crea múltiples programas separados o desconectados de cumplimiento, los cuales tienen que sortear las inconsistencias y la ineficiencia del manejo de requerimientos de múltiples fuentes.

Requerimientos Armonizados

La integración de requerimientos reduce costos, complejidad, inconsistencias y cargas de trabajo requerido para el cumplimiento.



Construyendo el Risk Intelligence empresarial

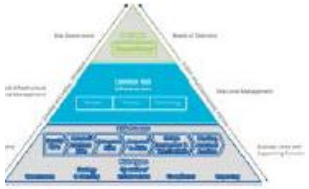
Gobernabilidad del Riesgo

Principio 1: Una definición común de riesgo enfoca a la preservación y creación del valor, es usada consistentemente a través de la organización

Principio 2: Un marco común de riesgo soportado por estándares apropiados (ej., COSO ERM, ISO, etc.) es usado a través de la organización para gestionar el riesgo

Principio 3: Roles claves, responsabilidades y autoridades relacionadas para gestionar el riesgo son claramente delimitadas dentro de la organización

Principio 4: órganos del gobierno (ej., Consejos de Accionistas , comités de auditoría, etc.) tienen apropiada transparencia y visibilidad en las prácticas de la organización en la gestión de riesgos para cumplir con sus responsabilidades



Infraestructura y gestión del riesgo

Principio 5: La dirección ejecutiva tiene la responsabilidad de diseñar, implementar y mantener un programa eficaz de los riesgos

Principio 6: Una infraestructura de gestión de riesgo común se utiliza para apoyar las unidades de negocio y funciones en el desempeño de sus responsabilidades de riesgo

Principio 7: Ciertas funciones (Ej., Auditoría interna, gestión del riesgo, conformidad, etc.) ofrecen garantías objetivas, así como supervisan e informan sobre la eficacia del programa de riesgo de la organización

Propiedad del Riesgo

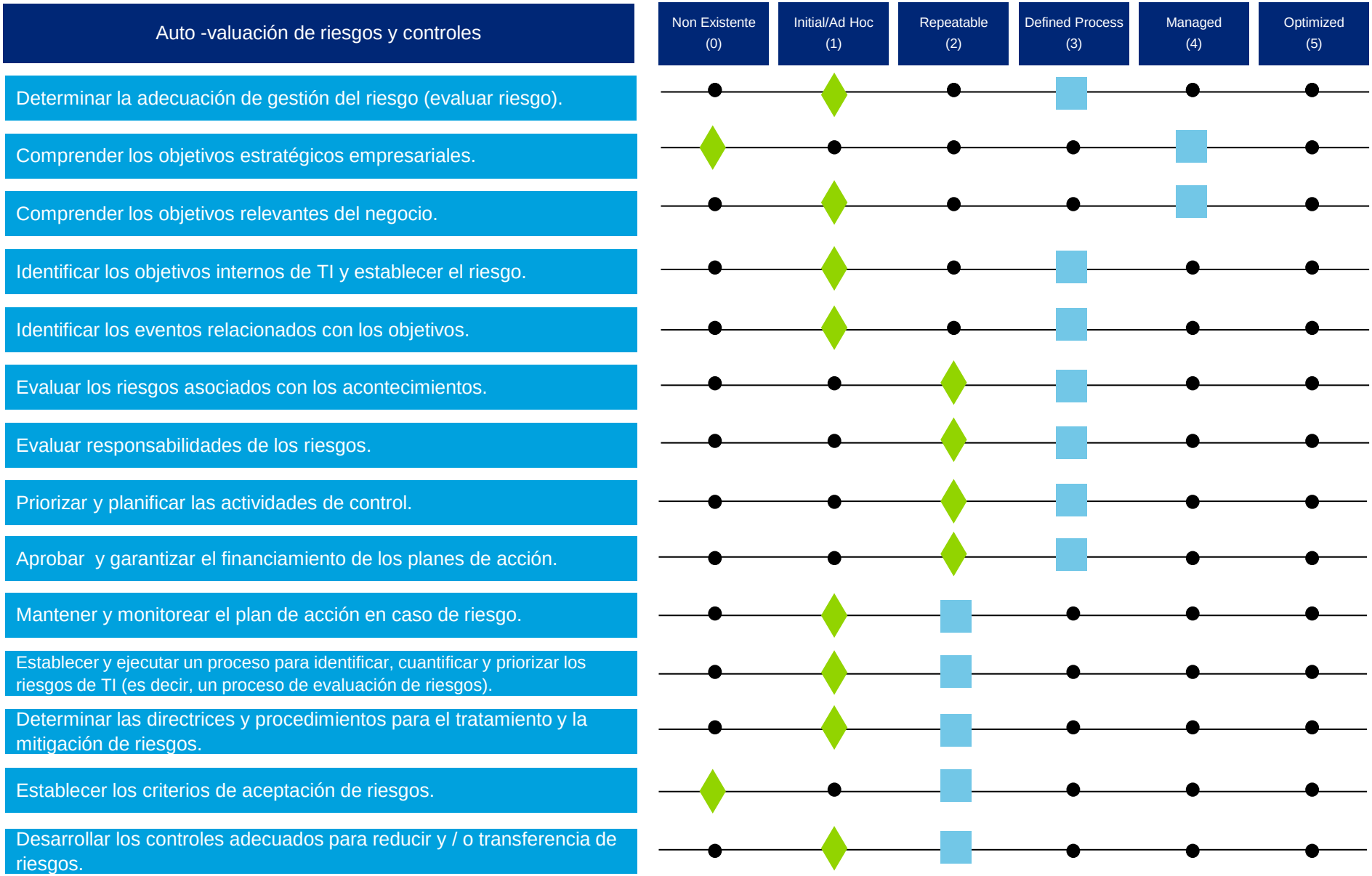
Principio 8: Las unidades de negocio (departamentos, agencias etc.) son responsables por el desempeño de sus negocios y la gestión del riesgo de acuerdo al marco del riesgo establecido por la dirección ejecutiva.

Principio 9: Ciertas funciones (Ej., finanzas, gestión del riesgo, TI, conformidad, etc.) tienen un impacto penetrante sobre el negocio y proveen soporte a las unidades del negocio de acuerdo al programa de riesgos de la organización.

Evolución a un modelo GRC

Evolución a un modelo GRC

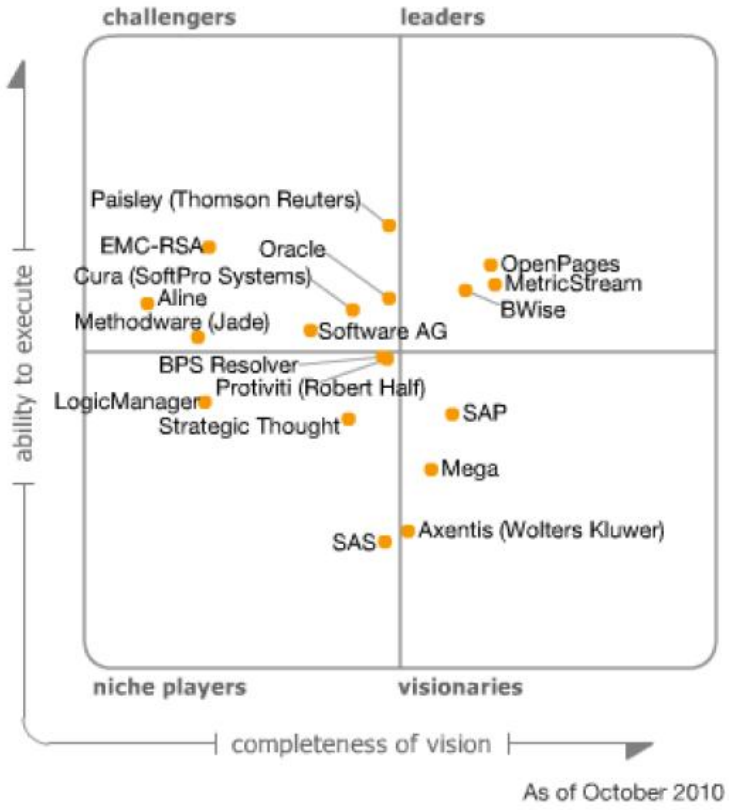
Conocer el estado actual y plantear metas permitirán la evolución al modelo



Solución GRC automatizada / Plataformas en el mercado

Gartner

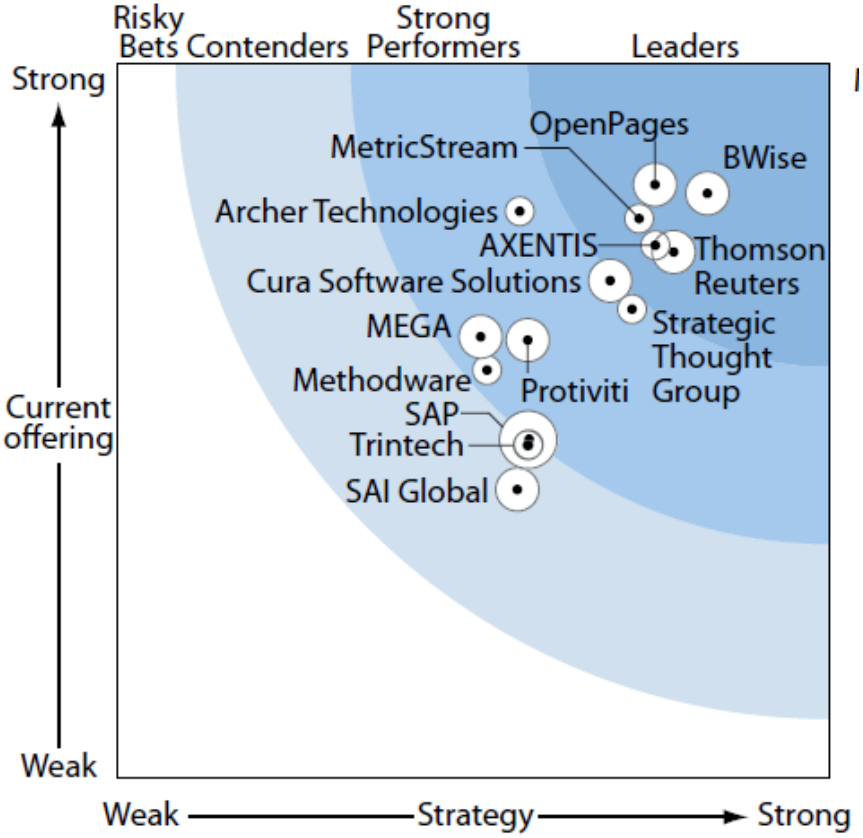
http://www.gartner.com



Source: Gartner (October 2010)

FORRESTER

http://www.forrester.com



Forrester Wave™: Enterprise Governance, Risk, And Compliance Platforms, Q3 '09