



SEGURINFO

VI Congreso Internacional de Seguridad de la Información

“Compartiendo experiencias y visiones en Seguridad de La Información”

12 de Agosto 2009 - Casa Piedra - Santiago de Chile

Governance, Risk & Compliance (GRC)

Gobierno Corporativo, Administración de Riesgos y Cumplimiento Regulatorio

José Lagos – Deloitte

Dario Rojas – E&Y

Rafael Ruano – PwC

Adrián Mascheroni - Accenture





SEGURINFO

VI Congreso Internacional de Seguridad de la Información

“Compartiendo experiencias y visiones en Seguridad de La Información”

12 de Agosto 2009 - Casa Piedra - Santiago de Chile

Governance, Risk & Compliance (GRC)

El GRC es una nueva filosofía de negocios. Las organizaciones deben seguir una gobernabilidad corporativa, deben contemplar retos y superar los obstáculos existentes, sin descuidar las influencias internas y externas.

¿Es esto complejo?

¿Existen soluciones?

En este panel los socios de las empresas Auditoras líderes, E&Y, Deloitte y PWC, nos brindarán su visión y tendencias al respecto.





SEGURINFO

VI Congreso Internacional de Seguridad de la Información

“Compartiendo experiencias y visiones en Seguridad de La Información”

12 de Agosto 2009 - Casa Piedra - Santiago de Chile

Governance, Risk & Compliance (GRC)

Gobierno Corporativo, Administración de Riesgos y Cumplimiento Regulatorio

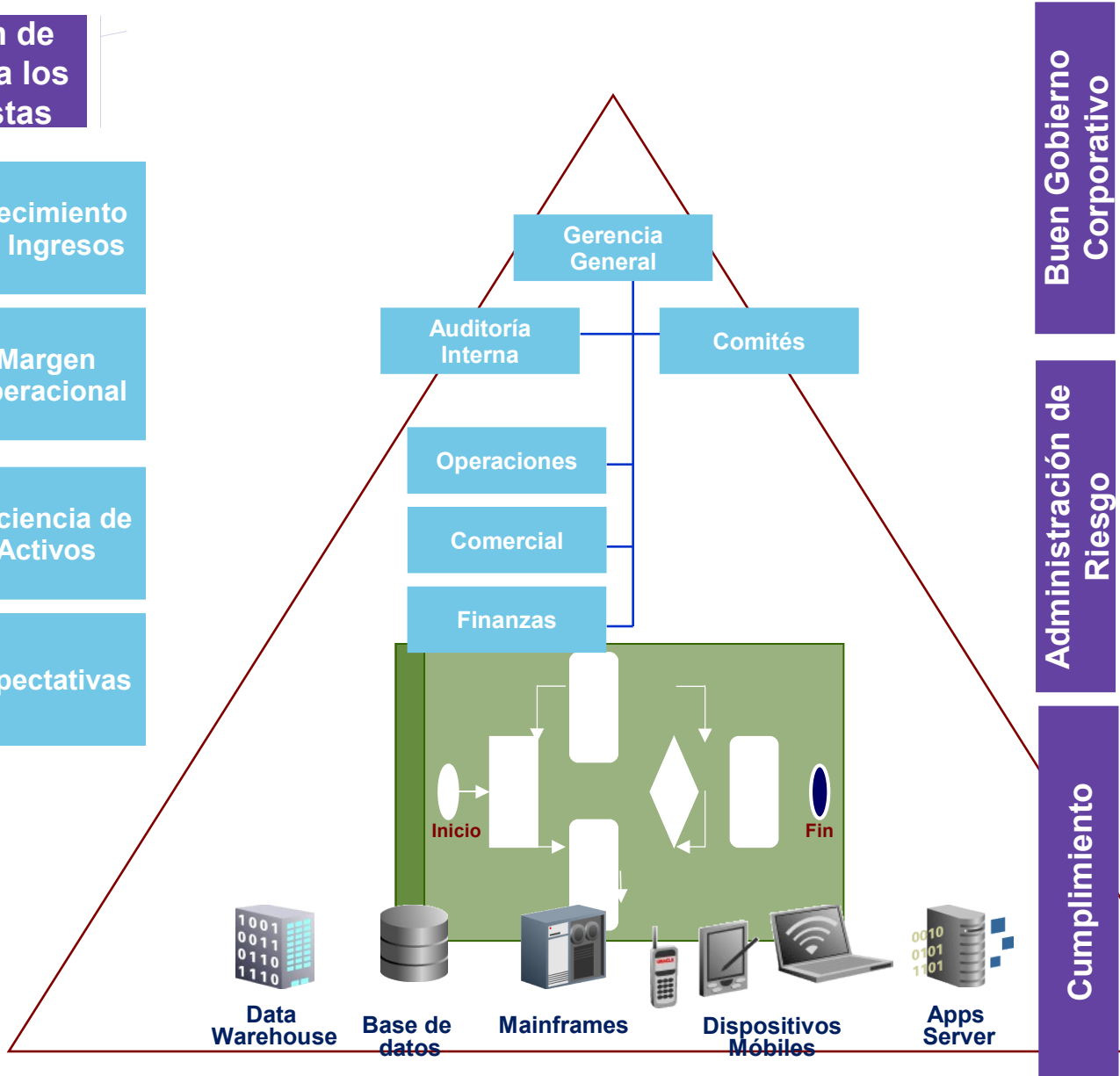
PRESENTACION PANELISTAS



Creación de Valor para los Accionistas

ESTRATEGIA y OBJETIVOS DE NEGOCIO

- Crecimiento de Ingresos
- Margen Operacional
- Eficiencia de Activos
- Expectativas



Buen Gobierno Corporativo

- Directorio y Comités
- Gestión de Riesgos
- Controles Internos
- Ética y RSE
- Comunicación

Administración de Riesgo

- Identificar
- Medir
- Mitigar
- Monitorear

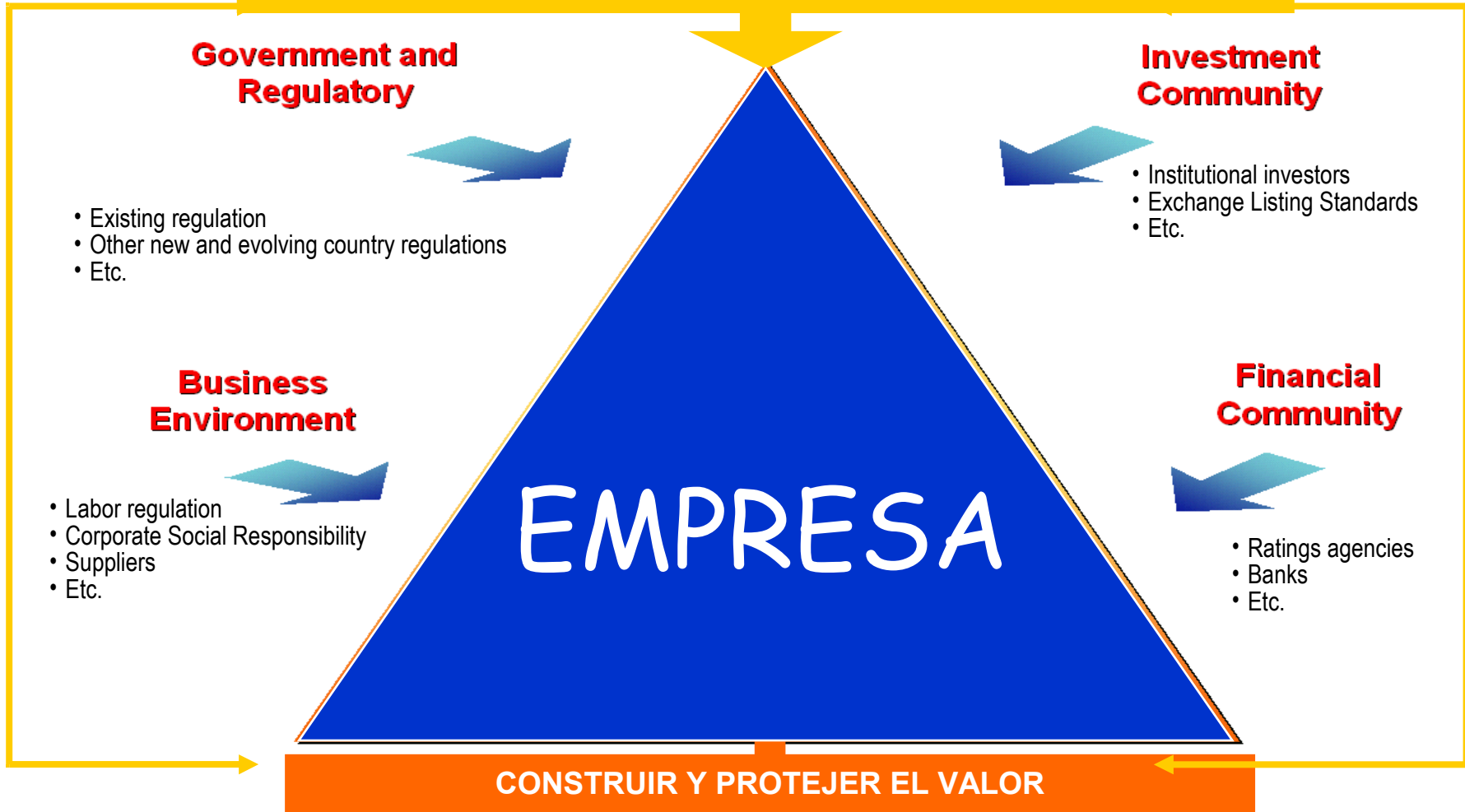
- Estratégico
- Operacional
- Financiero
- Crédito
- Ambiental

Cumplimiento

- Mandatorios
- Laboral
- Seguridad
- Ambiental
- Comercio Exterior
- Voluntario
- Valores
- Marca
- Políticas Internas

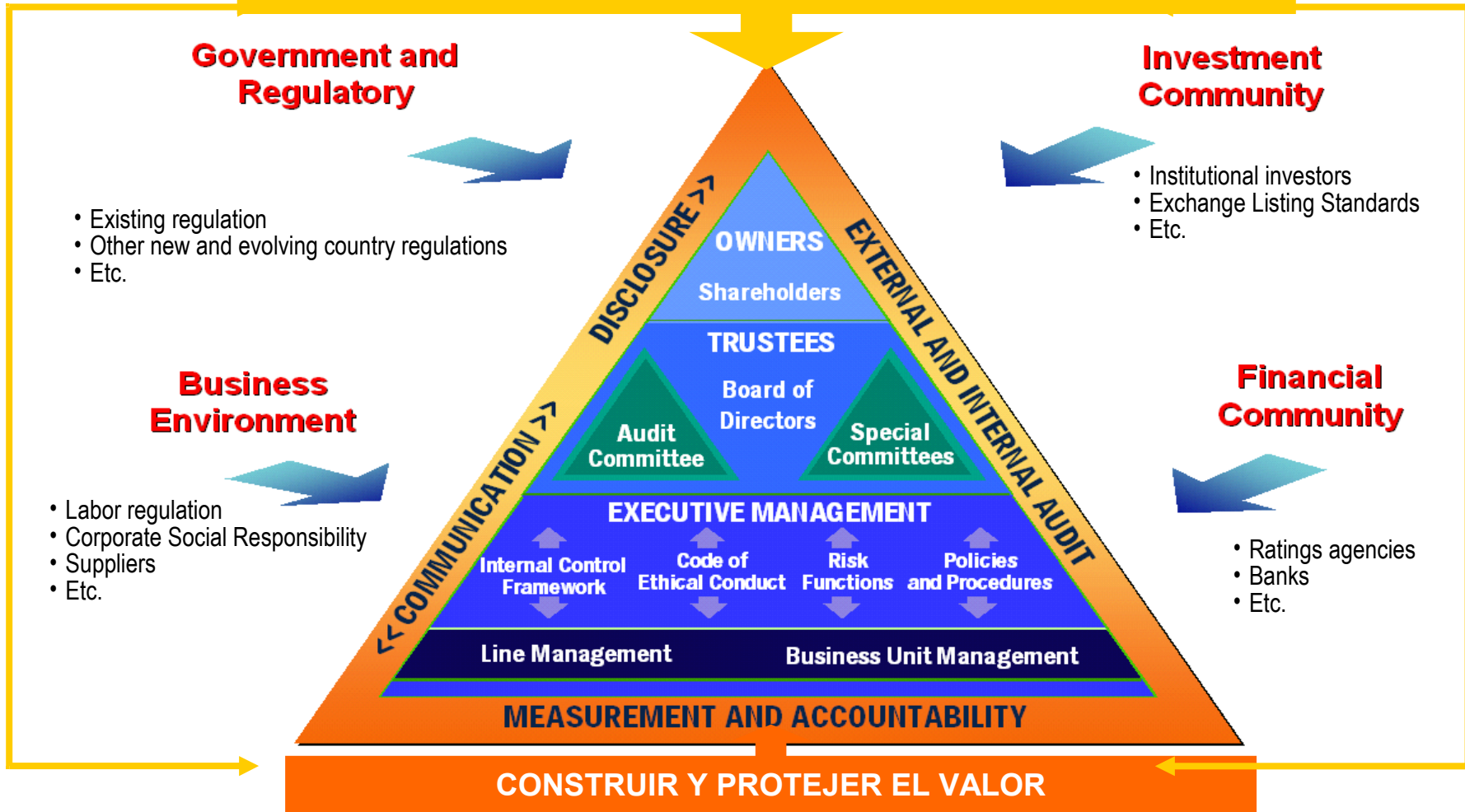
Requerimientos a la Empresa

IDENTIFICAR Y ADMINISTRAR LOS RIESGOS CLAVES DEL NEGOCIO



Gobierno Corporativo

IDENTIFICAR Y ADMINISTRAR LOS RIESGOS CLAVES DEL NEGOCIO



Atributos Claves de una Estructura de Gobierno Corporativo eficiente

Atributos Clave para un adecuada Estructura de Gobierno Corporativo

A proactive Audit committee

A Compensation committee aligning executive compensation to shareholders value

A Nominating committee ensuring effective governance of the board

A sound internal control framework

A relevant code of ethical behavior

Clear, enforced policies & procedures

Effective management of risk

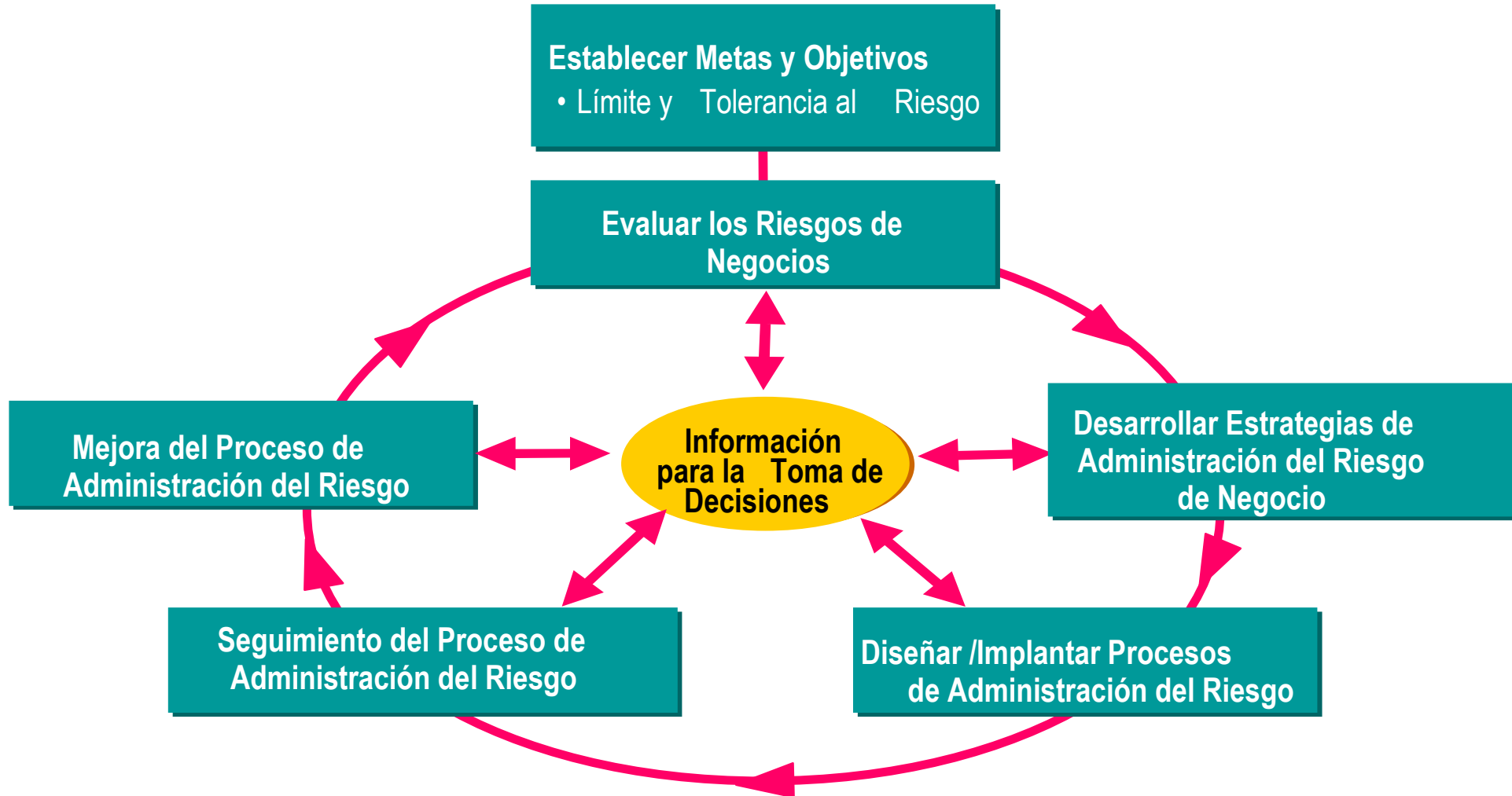
An objective, well resourced internal audit function

Independent, effective external audit

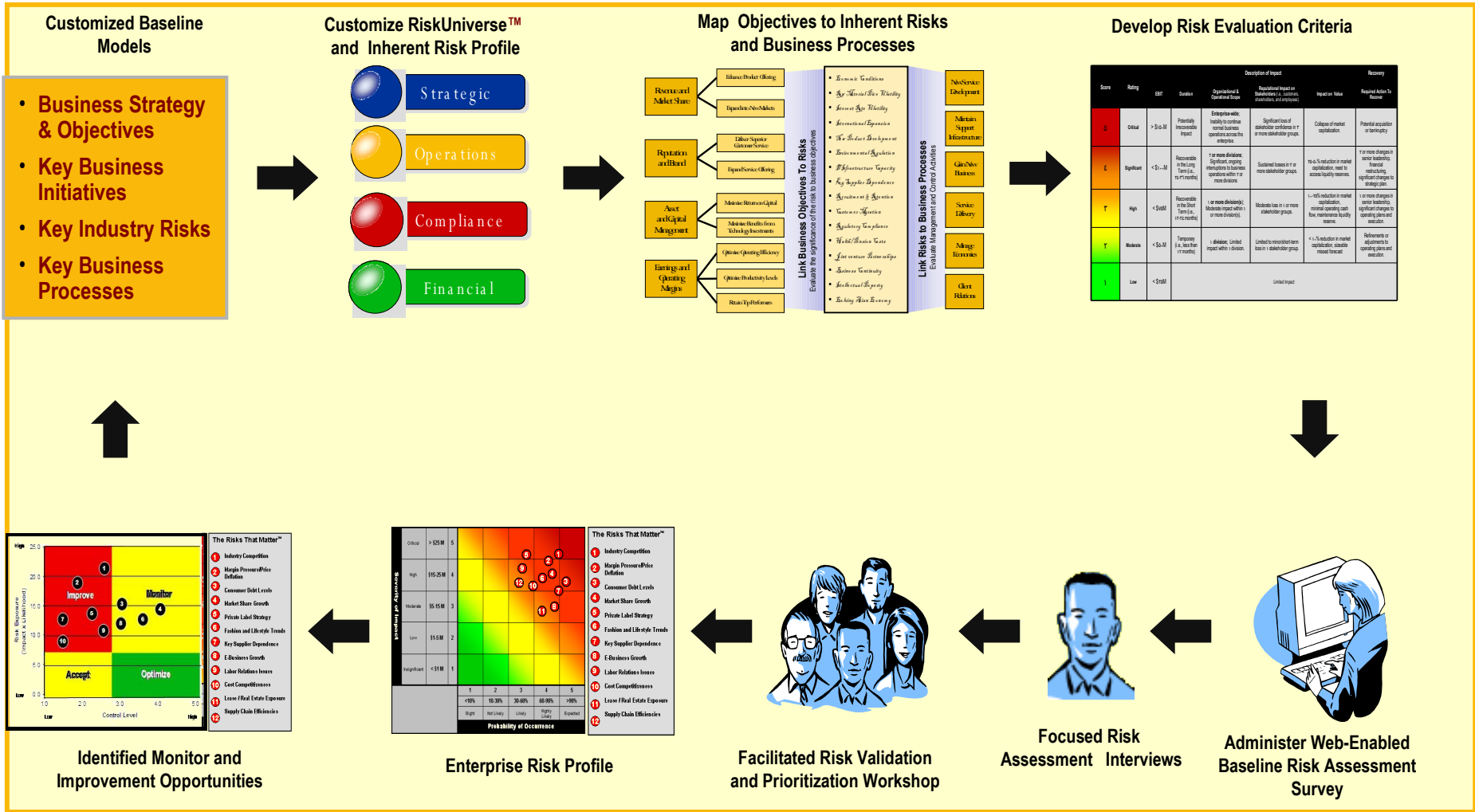
Transparent disclosure, effective communication and systems that ensure effective measurement and accountability

“Corporate Governance is the system by which companies are directed and controlled, in the interest of shareholders and other stakeholders, to sustain and enhance value”.

Administración de Riesgos – Etapas



Enfoque Identificación y Evaluación de Riesgos






SEGURINFO

VI Congreso Internacional de Seguridad de la Información

“Compartiendo experiencias y visiones en Seguridad de La Información”

12 de Agosto 2009 - Casa Piedra - Santiago de Chile

Mejorando el desempeño a través de la optimización
de controles

PRICEWATERHOUSECOOPERS 

Motivadores del cambio

- **Crecientes expectativas de stakeholders**

- Mayor presión por parte del comité de auditoría, la dirección y entidades regulatorias para incorporar mejores prácticas en ambientes de gobierno y de control.
- Reducir la volatilidad y a la vez mejorar la eficiencia; predecir, comunicar y reducir sorpresas “controlables”.

- **Reducir la confusión y el costo asociado a la complejidad**

- El objetivo es reducir la complejidad de múltiples sistemas, procesos, regionalismos, requerimientos regulatorios, mercados y productos.
- Abordar deficiencias de control conocidas, fallas de control o errores en estados financieros.
- Necesidad de incorporar controles asociados a cumplimiento en la operación diaria.

- **Mantener el desempeño durante procesos de cambios significativos**

- Cambios en los requerimientos regulatorios actuales y futuros.
- Necesidad de mantenerse competitivo en periodos de crecimiento significativo y cambios estructurales mayores. (ejemplo: reducción de costos, migración a esquemas de servicios compartidos, expansión a nuevos mercados, abordaje de iniciativas de clientes, etc.).

Optimización de los controles como una extensión natural de las nuevas mejores prácticas en la integración de gobierno, riesgo y cumplimiento

Estrategia y gobierno

- ♦ Alto nivel de compromiso con la gestión global de riesgos.
- ♦ Apetito de riesgo definido en forma centralizada, cumplimiento de la taxonomía y estructuras de control.
- ♦ Identificación y respuesta oportuna a los requerimientos nuevos o emergentes.
- ♦ Aplicación de gobierno de datos y gestión estratégica de datos.
- ♦ Políticas, estándares y normas desarrolladas centralizadamente.

Personas y organización

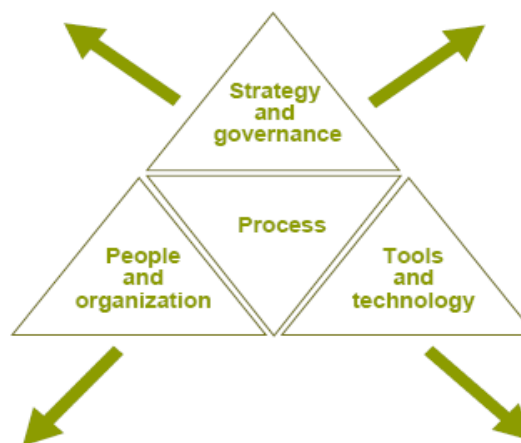
- ♦ Visión centralizada para soportar el despliegue de unidades regionales.
- ♦ Centros de excelencia para la identificación, prueba, evaluación de riesgos, diseño de regulaciones, normativas y políticas.
- ♦ Responsabilidad sin ambigüedades y claridad de roles.
- ♦ Optimización para la asignación de recursos relacionados con la gestión del riesgo.
- ♦ Entrenamiento organizacional y desarrollo del soporte a la gestión del riesgo.

Procesos

- ♦ Habilidad de capturar, editar y estandarizar jerarquías.
- ♦ Definición de los componentes estándares.
- ♦ Procesos simplificados y estandarizados.
- ♦ Visión de los controles desde adelante hacia atrás.
- ♦ Reportes basados en roles estandarizados.
- ♦ Métodos estandarizados.
- ♦ Mejores prácticas internas.
- ♦ Visión transversal de datos, procesos y controles.

Herramientas y tecnología

- ♦ Controles en tiempo real con métricas en tiempo real.
- ♦ Bases de conocimiento organizacional y desarrollo de taxonomías.
- ♦ Uso de tecnologías de workflow y gestión documental.
- ♦ Impulso de las tecnologías a través de herramientas comunes, apoyadas en procesos estandarizados.
- ♦ Capacidades de reporte multidimensional.
- ♦ Capacidades de archivado, consultas y auditoría.
- ♦ Tableros de mando.



Optimización de controles – los controles adecuados al precio correcto.

La optimización de controles es nuestra respuesta a las necesidades de los negocios de contar con los controles adecuados al precio correcto.

Los controles adecuados son aquellos que **mitigan el riesgo** del negocio en una forma eficiente y **costo efectiva**, y cuentan con el apoyo de una cultura de controles coherente y siempre monitoreada.

Los controles optimizados pueden soportar de mejor forma las funciones operacionales y de back office, ayudar a manejar la complejidad y lograr un **gobierno efectivo** de los aspectos regulatorios y de cumplimiento.

La optimización de controles es un proceso de **mejora continua**. Está construido en torno a un planteamiento basado en el diseño de controles internos de acuerdo a los riesgos identificados.

Enfoque Metodológico Accenture

Compliant User Provisioning Enterprise Role Management Superuser Privilege Management



Objetivos:

- Definir e implementar los procedimientos de provisión de usuarios y permisos para los sistemas objetivo
- Implementar herramientas Compliant User Provisioning, Enterprise Role Management y Superuser Privilege Management

Tareas principales:

- Definir procedimientos de provisión de usuarios y perfiles en Enterprise Role Management y Compliant User Provisioning
- Definir estrategia para el uso del usuario de emergencia (Superuser Privilege Management)
- Integrar RAR, CUP y ERM
- Ejecutar prueba técnica de las herramientas
- Implementar

Lecciones Aprendidas

Lecciones Aprendidas

Tratar GRC como un programa... no como un proyecto

Relevamiento

- Hacer participar, y comprometer, a las áreas de Negocio, Seguridad y Auditoría desde el primer día de proyecto con responsabilidades bien definidas
- Identificar a las personas que poseen el conocimiento técnico/funcional de las aplicaciones, e involucrarlas desde el primer día en el proyecto
- Identificar a las personas que serán las dueñas de la aplicación (p.e. Compliance) una vez implementada e involucrarlas desde el primer día en el proyecto
- Incorporar en el análisis y diseño solamente transacciones y roles en uso

Diseño

- Dedicar el tiempo necesario para validar las funciones definidas

Remediación / Mitigación

- Armar un plan de remediación / mitigación con metas a corto, medio y largo plazo y comunicarlo a todas las partes involucradas

Asegurar de contar con el equipo necesario (Hardware y Software) según recomendaciones de SAP



SEGURINFO

VI Congreso Internacional de Seguridad de la Información

“Compartiendo experiencias y visiones en Seguridad de La Información”

12 de Agosto 2009 - Casa Piedra - Santiago de Chile

Preguntas