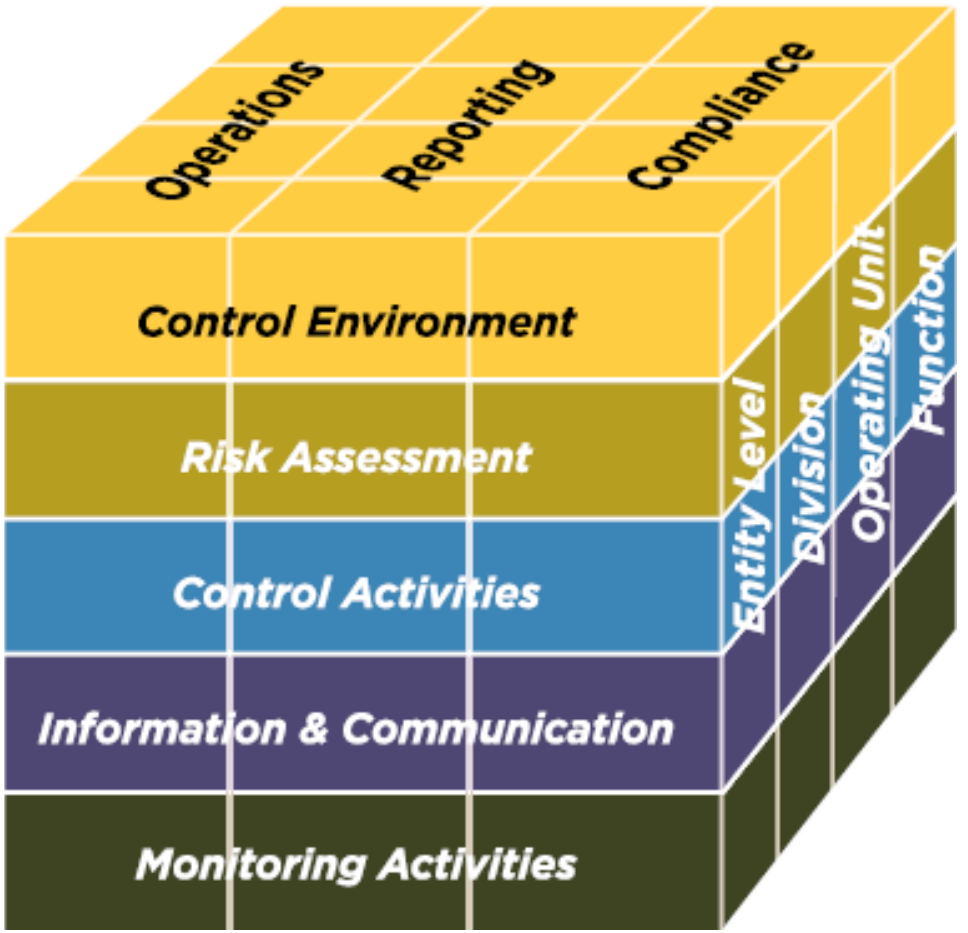
Deloitte.

COSO

Evaluación de Riesgos



Enterprise Risk Services
Noviembre, 2015

Contenido

Componente

Evaluación de Riesgos

Principios Relacionados

1. Especifica objetivos para la identificación y valoración de los riesgos relacionados a dichos objetivos
2. Analiza los riesgos para determinar cómo deben de administrarse
3. Considera la posibilidad de fraude en la evaluación de riesgos
4. Identifica y evalúa cambios que pueden impactar significativamente la gestión de riesgos

¿Qué es el Riesgo?

Objetivos de una compañía

- Los objetivos de una compañía son proteger el valor de sus activos existentes y crear nuevos activos/valor para el futuro.
- Valor para la compañía es el valor integrado para los stakeholders en su totalidad (internos y externos).

Riesgo

- Riesgo es el impacto y la probabilidad de que una amenaza (o de una serie de eventos/ amenazas) puedan afectar de manera adversa la consecución de los objetivos.

¿Tomar riesgos es bueno o es malo?

- Dos líneas de pensamiento

Riesgos No recompensados (pérdida de valor)

- *El tomar riesgos es malo y es necesario evitarlo.*

Riesgos recompensados (creación de valor)

- *El tomar riesgos es bueno dentro de un marco/ contexto donde el riesgo sea bien administrado.*

El tomar riesgos es malo y es necesario evitarlo (Preservación del Valor)

- El mercado castiga severamente el fallar en la preservación de los activos existentes (sin premio / el riesgo es malo)
- ***Bottom-up*** *y foco en las operaciones, reporte y cumplimiento.*
- *La gran mayoría de los esfuerzos para administrar el riesgo se* ***enfocan en los activos actuales*** *y se realizan aisladamente.*
- *El manejo tradicional del* ***riesgo es probabilístico*** *– habitualmente no se trata el riesgo en los extremos.*
- ***Riesgo sin retribución****, por ejemplo: no es atractivo el tomar riesgo cuando se compara con la desventaja que implican las pérdidas en las que se puede incurrir.*

El tomar riesgos es bueno (Creación de Valor)

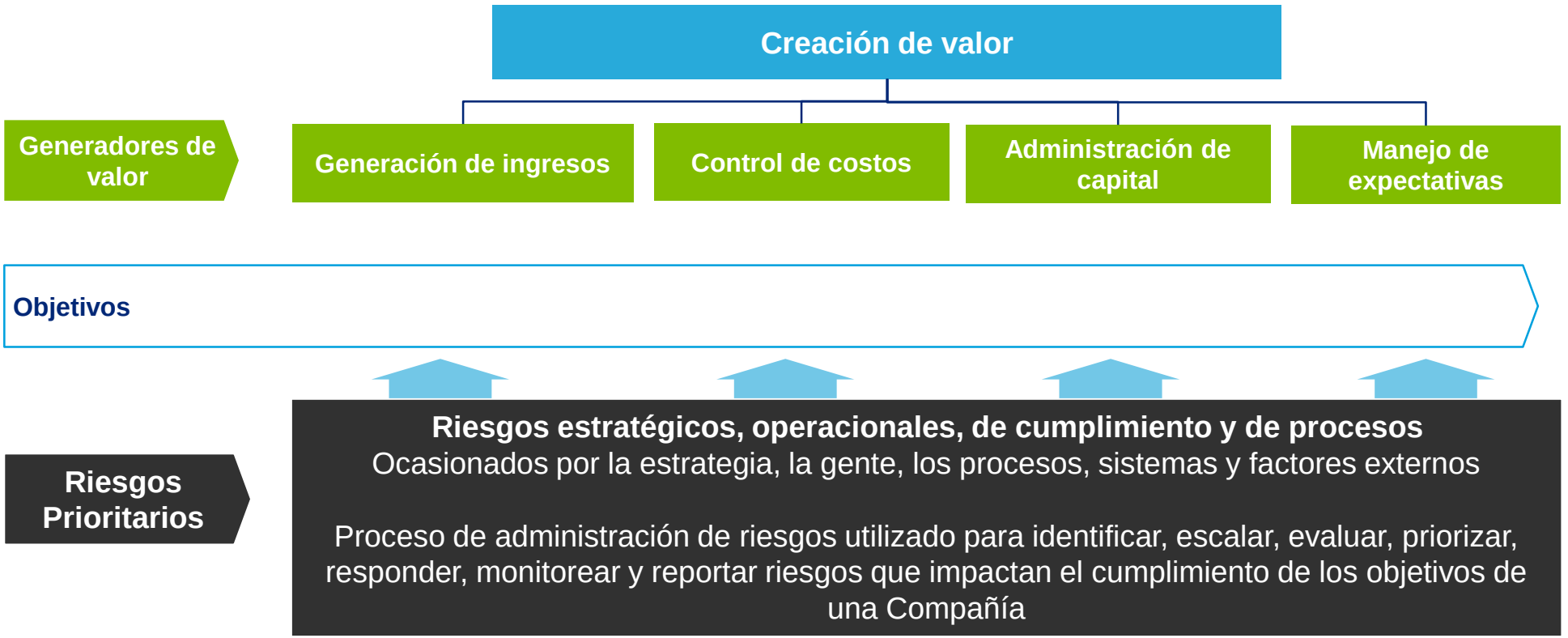
- El mercado premia la habilidad de crear y sustentar el crecimiento futuro (algunos riesgos valen la pena / son buenos)
- ***Sin riesgo, no hay retribución****. Esta es la base del capitalismo, por ejemplo: Realizar inversiones riesgosas y obtener buenos rendimientos de ellas.*
- ***Mejor entendimiento*** *de lo ventajoso de las grandes inversiones y sus riesgos para llegar al éxito y como superarlos.*
- *La dirección* ***se enfoca en riesgos críticos*** *para la estrategia de la empresa y su ejecución.*
- ***La toma de riesgos tiene retribuciones****, por ejemplo: las compañías reciben premios por tomar y administrar eficazmente los riesgos asociados con nuevos productos, nuevos mercados, nuevos modelos de negocios, alianzas, adquisiciones, etc.*

1. Especifica objetivos para la identificación y valoración de los riesgos relacionados a dichos objetivos

Asociando riesgos a los objetivos y creadores de valor

Un programa de administración integral de riesgos provee un proceso para la identificación, valoración y respuesta de riesgos que impactan el cumplimiento de los objetivos e iniciativas estratégicas de la Compañía.

La asociación entre crecimiento, riesgos y retorno ha sido identificado como el beneficio número 1 que las compañías esperan de un programa de administración de riesgos



Análisis de la estrategia

1. **Riesgo a la estrategia: ¿Qué tiene que salir bien para que una estrategia sea exitosa?**

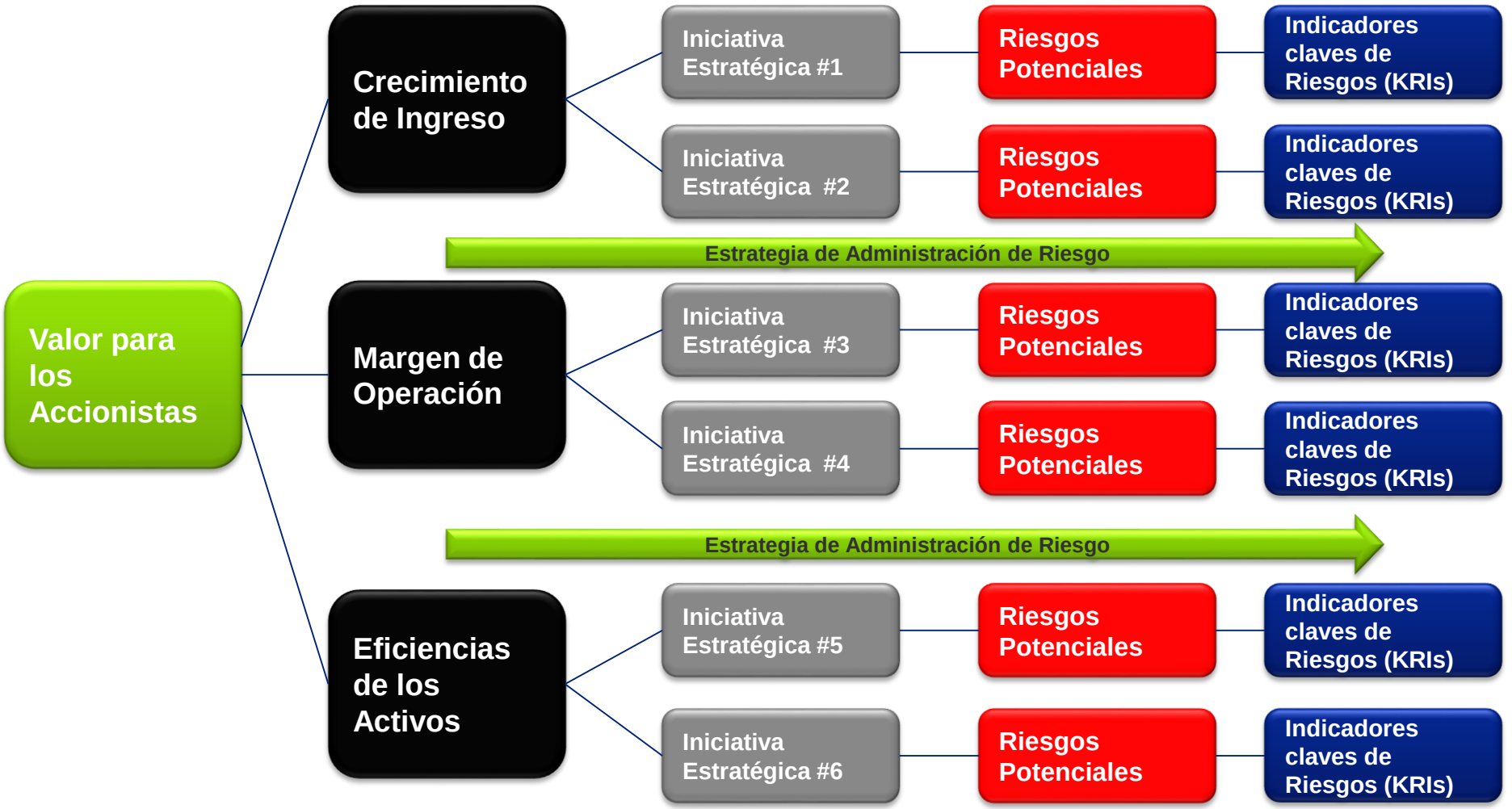
- ¿En qué supuestos se basa la estrategia?
- ¿Qué podría impedir que la estrategia sea exitosa?

2. **Riesgo de la estrategia: ¿Qué impacto podría tener esta estrategia en nuestro negocio y en otras iniciativas?**

- Consecuencias de la ejecución de la estrategia

Estrategia de Administración de Riesgos

Vinculación del Riesgo con los objetivos y la estrategia



Categorías de Riesgos

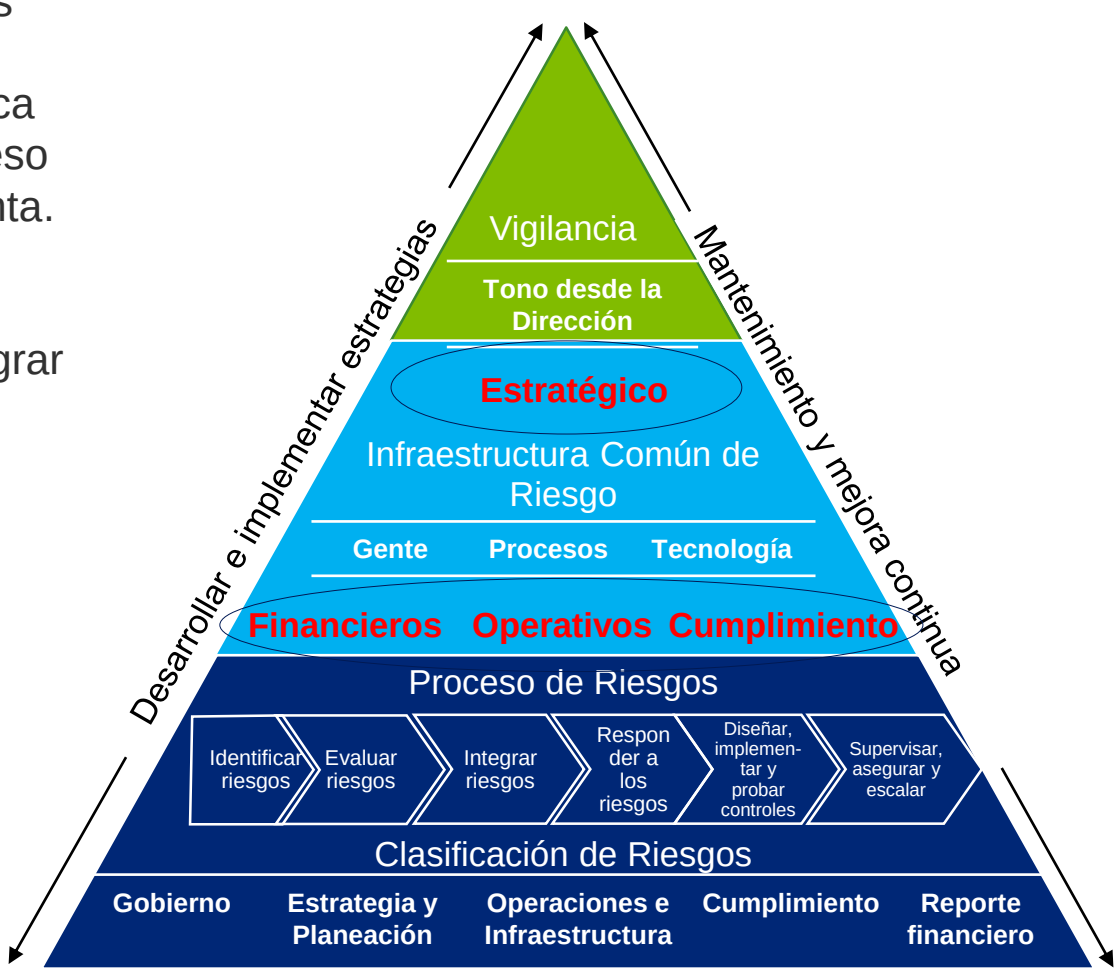
Las cuatro categorías más relevantes desde la perspectiva de un inversionista son:

1.Riesgos estratégicos – riesgos tanto **para** los objetivos estratégicos como **de** los objetivos estratégicos. La alta gerencia (C-suite) identifica los riesgos más importantes a través del proceso de planificación y obtiene aprobación de la Junta.

2.Riesgos Operativos – grandes riesgos que afectan la habilidad de la organización para lograr el plan estratégico.

3.Riesgos Financieros – incluyen información financiera, valoración, cobertura, riesgos de mercado y liquidez y riesgos de crédito en instituciones financieras.

4.Riesgos de Cumplimiento – riesgos no compensados, generalmente el foco principal para las actividades de gestión de riesgo empresarial



Administración del Riesgo basado en Valor

Valor para la Compañía

- Crecimiento de Ganancias
- Margen Operativo
- Eficiencia de activos
- Expectativas

La Administración es responsable por crear y preservar valor en la Compañía

1. ¿Cómo la compañía puede fallar en alcanzar sus objetivos de valor ?
2. ¿Qué puede causar dicha falla?
3. ¿Cuáles serían los efectos de la falla?
4. ¿Qué se está haciendo actualmente para prevenir, detectar, corregir o escalar dicha falla?
5. ¿Cuál es nuestra vulnerabilidad a dicha falla?

Riesgos de la Compañía

- Gobierno
- Estrategia
- Capital
- Operaciones
- Infraestructura (Reporting/ Compliance)
- Factores Externos

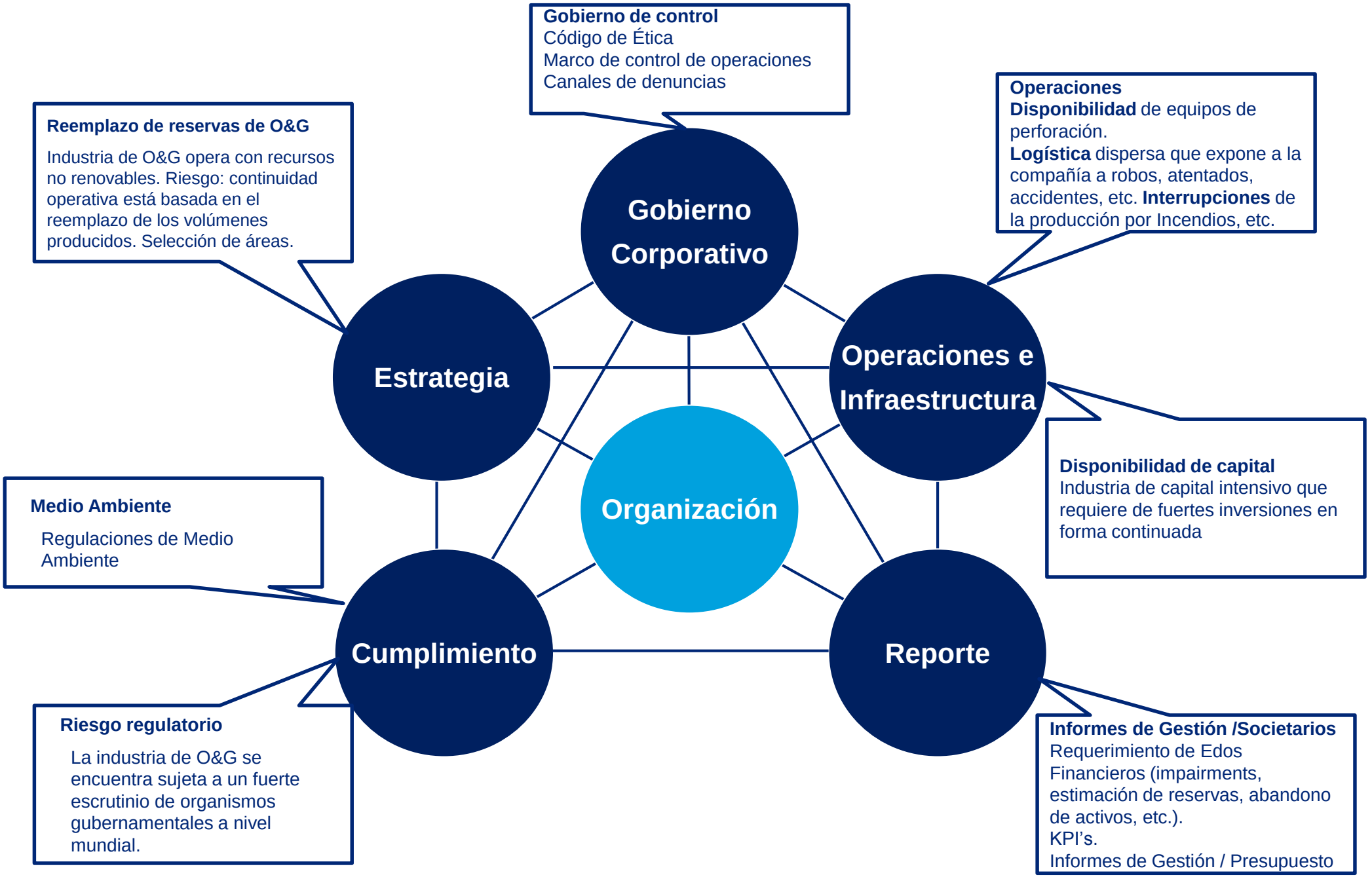
El Rol de la Alta Dirección

El **Consejo de Administración** está involucrado en el ejercicio de supervisión del Control Interno para cada uno de los cinco componentes de COSO; en cuanto a la Evaluación de Riesgos a continuación se señalan las actividades realizadas:

Componente de Control Interno	Actividades de supervisión de la Junta
Ambiente de Control	Supervisar la definición y aplicación de los **estándares de conducta** de la organización.
Evaluación del Riesgo	Desafiar a las Gerencias en la **Evaluación de Riesgos para el logro de objetivos**, incluyendo el impacto potencial de cambios significativos (ejemplo: el Riesgo de entrar en un mercado nuevo), fraude o corrupción.
Actividades de Control	Supervisar a las Gerencias en su **desempeño de actividades**.
Información y Comunicación	**Obtener, revisar y discutir información** de la Compañía relacionada con el cumplimiento de objetivos.
Actividades de Monitoreo	Evaluar y supervisar la naturaleza y el alcance sobre el **monitoreo de las actividades**, cualquier incumplimiento o falta de apego a los controles por parte de la administración (“brincarse los controles”), así como las evaluaciones de la administración y remediación de deficiencias.

2. Analiza los riesgos para determinar cómo deben de administrarse

Identificación de riesgos



Identificación de riesgos (cont.)

¿Cuáles son los desafíos en la identificación de riesgos?

- Los riesgos por definición son potenciales, en consecuencia difusos.
- Toda actividad se enfrenta a múltiples riesgos, y nunca existe la certeza absoluta de haberlos identificado en su totalidad.
- Los actores no entienden siempre lo mismo por “riesgo”: se confunde la historia con la probabilidad, y la no detección con la no ocurrencia.
- Sin saber los objetivos establecidos, es difícil hacer propuestas efectivas de gestión de riesgos y que generen valor.

10 Riesgos frecuentemente divulgados*

Ranking	Riesgos Divulgados	Menciones
1	Condiciones Económicas / Cambios	294
2	Cambios Legales/ Regulatorios/ Ambientales Adversos	288
3	Competidores y Acciones Competitivas	281
4	Interrupciones del Negocio (incluyen interrupciones de suministro y desastres naturales/ problemas climáticos)	277
5	Litigios / Problemas de Capital Intelectual	213
6	Estrategia de Fusiones y Adquisiciones / Ejecución / Integración	192
7	Estabilidad Política / Riesgo País	189
8	Cambios no Anticipados sobre la Demanda de los Consumidores/ Preferencias	187
9	Inhabilidad de Desarrollo/ Nuevo Productos de Mercado	156
10	Actividades Terroristas/ Guerra/ Malestar	149

* Riesgos divulgados públicamente en Reportes anuales (10K) de Compañías Públicas en Estados Unidos

Evaluación de Riesgos
Riesgo Inherente y Residual

- El **Riesgo Inherente** es el riesgo existente ante la ausencia de alguna acción que la dirección pueda tomar para alterar tanto la probabilidad o el impacto del mismo.

  RIESGO INHERENTE= PROBABILIDAD inh * IMPACTO inh

  - Impacto Inh: impacto de un evento, sin considerar las acciones y controles mitigantes.
  - Probabilidad Inh: probabilidad de ocurrencia de evento no deseado sin considerar las acciones y controles mitigantes.

Definidos los riesgos inherentes se deben identificar los controles mitigantes y de ahí resulta el riesgo residual:

- El **Riesgo Residual** es el riesgo que persiste luego de la respuesta de la Dirección al Riesgo.

  RIESGO RESIDUAL = RIESGO INHERENTE – EFECTIVIDAD DE CONTROLES

  *o RIESGO RESIDUAL = PROBABILIDAD res * IMPACTO res*

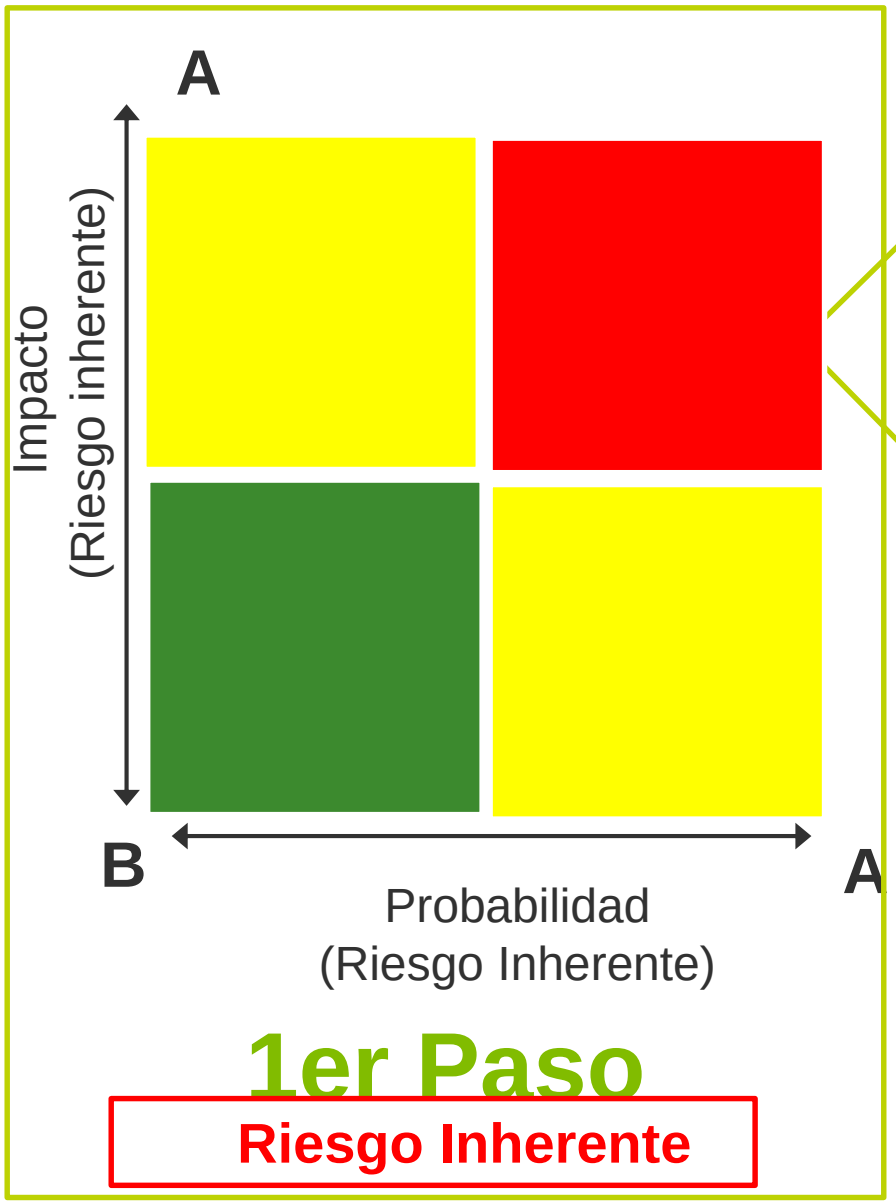
Evaluación de Riesgos
Riesgo Inherente y Residual (cont.)

- La Evaluación del Riesgo se aplica primero al Riesgo Inherente.
- Una vez que se desarrollaron las respuestas a los riesgos, la Dirección considera el Riesgo Residual.
- Las iniciativas efectivas de ERM requieren que se evalúe el Riesgo Inherente y el Residual.

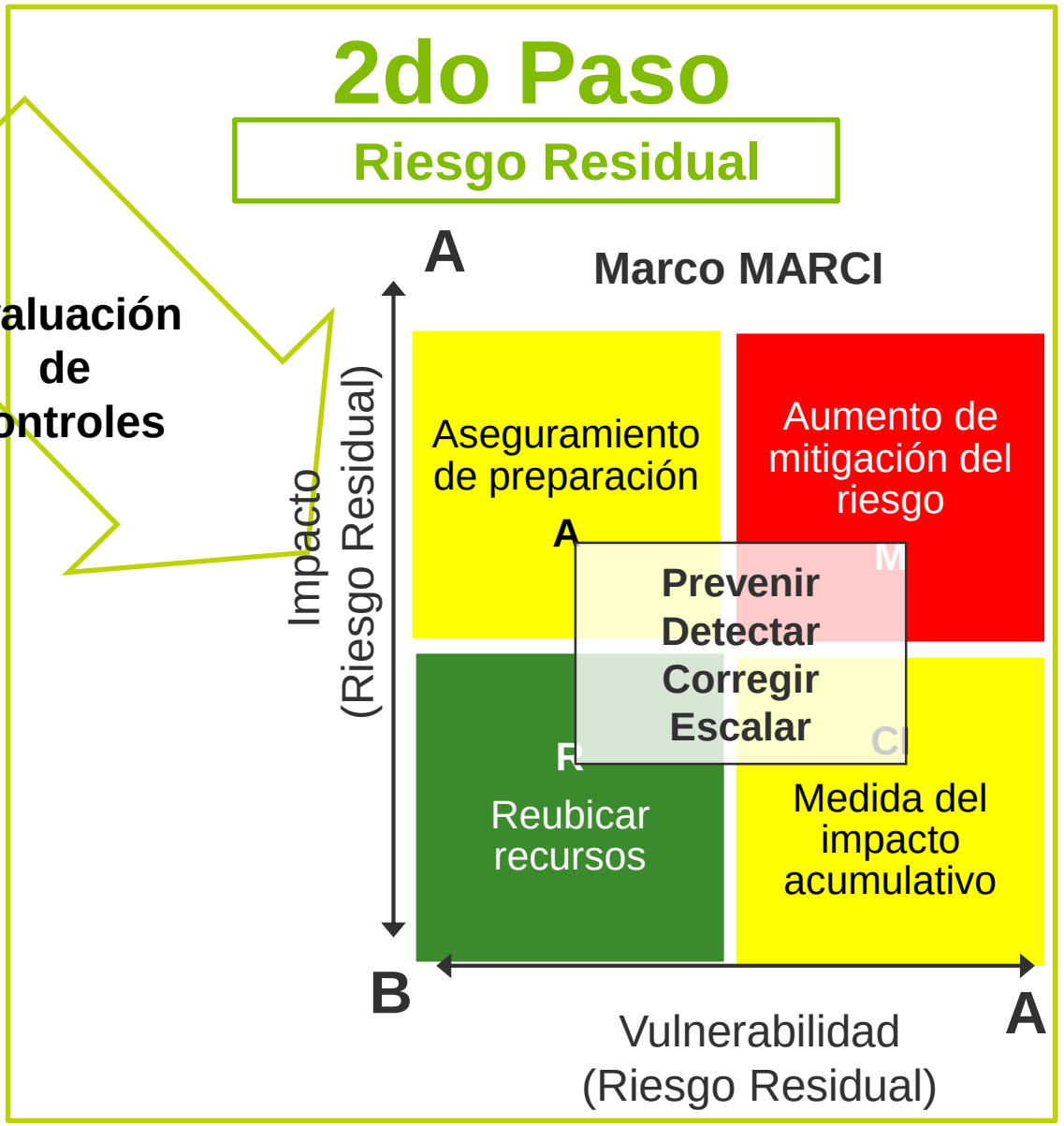
Consideraciones de Riesgo Inherente

- Las personas suelen ser demasiado optimistas sobre su habilidad para administrar el riesgo.
- Una compañía necesita asegurarse que entiende el riesgo inherente y que ha administrado el mismo de forma tal que se encuentre dentro de su perfil de riesgo (Apetito de Riesgo), es decir que acepta la vulnerabilidad.

Evaluación del riesgo
Mapeo de los riesgos inherente al riesgo residual

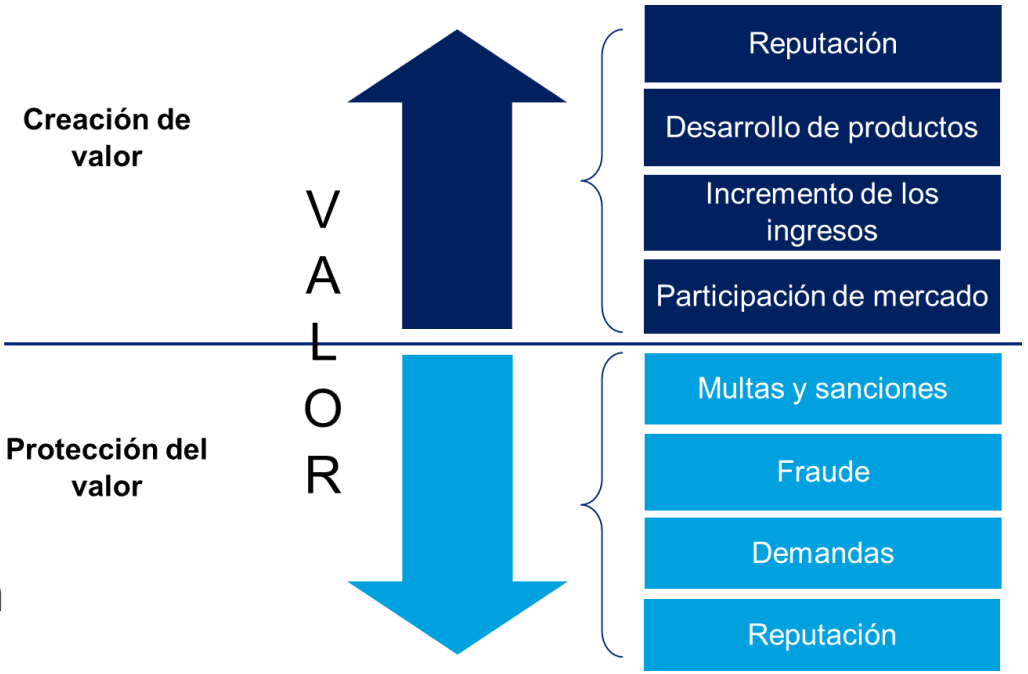


Evaluación de controles



Mantener el equilibrio— riesgo vs recompensa

- Evitar un enfoque de "una sola vista" en la protección de valor
- Se requiere una toma de riesgos "inteligente" hacia riesgos que crean valor
- Priorizar la atención en riesgos a los objetivos estratégicos
- Alinear los objetivos de administración de riesgos con las iniciativas y objetivos estratégicos



Enfoque en el costo total del riesgo—racionalizando el costo de la mitigación

- El Costo de Fallar (COF) frecuentemente es disperso, difícil de cuantificar y muchas veces se esconde por debajo de lo visible
- El COF muchas veces es mayor que el costo que implica administrar riesgos
- Racionalizar el costo y los esfuerzos para administrar riesgos debe hacerse considerando el apetito al riesgo
- El costo total del riesgo debe de ser calculado y considerarse en la priorización de las opciones de respuesta al riesgo

3. Considera la posibilidad de fraude en la evaluación de riesgos

Introducción

¿Qué es fraude?

Fraude es engañar o aprovecharse del error de una persona de manera intencionada para hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido. (1)

Existen diversos factores de riesgo que pueden propiciar el fraude en las organizaciones, por ejemplo:

(1) Fundamento Legal del Código Penal Federal, Artículo 386 al 389 y lo aplicable del Libro Segundo, Título Décimo.

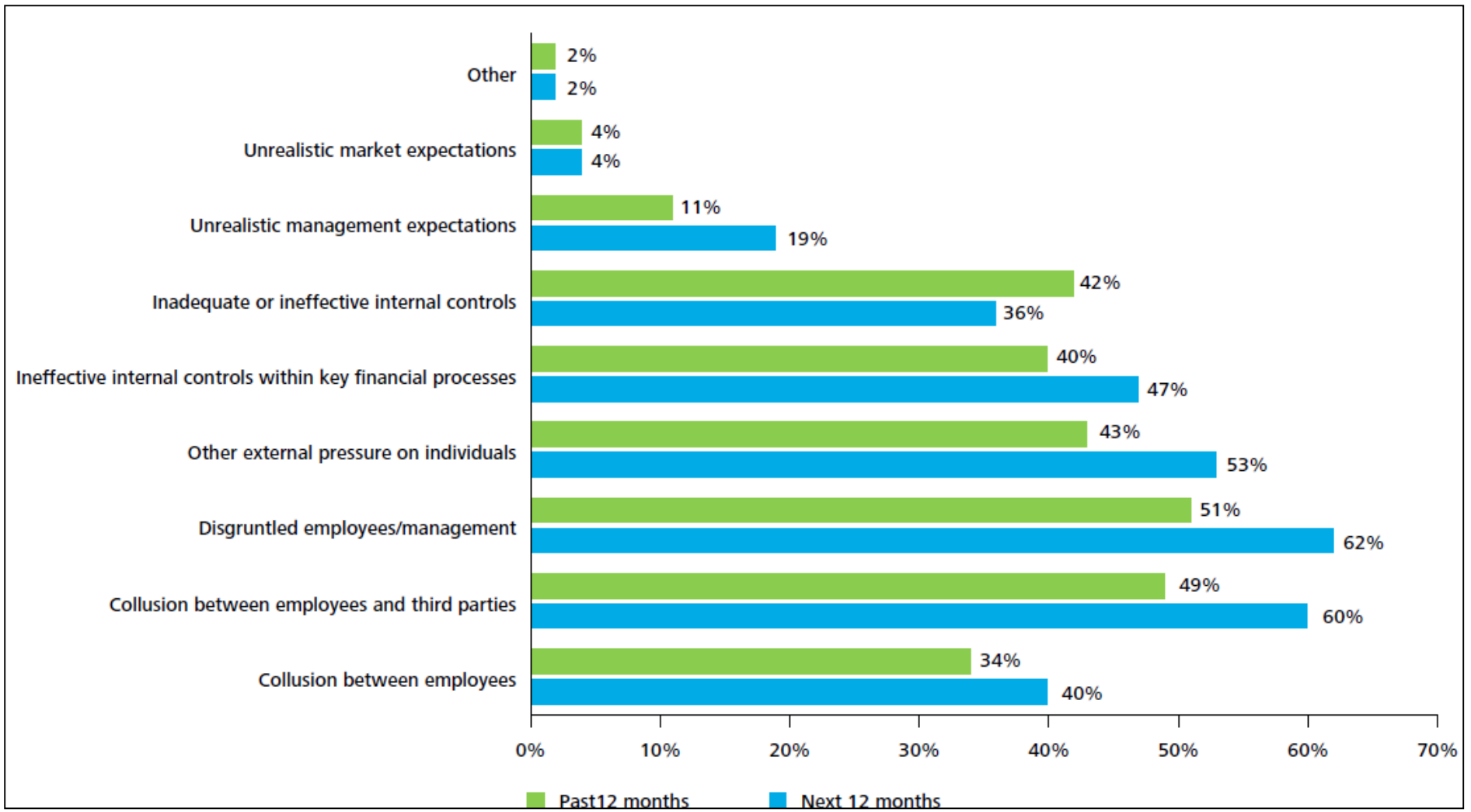
Combatir el fraude desde el origen— atacar las causas y no solo los síntomas

Compañías líderes llevan a cabo las siguientes actividades como parte de un programa formal antifraude:

- Educar a los líderes sobre las implicaciones y consideraciones de negocio de los riesgos de fraude
- Definir el alcance y objetivos de un programa antifraude
- Documentar las actividades antifraude existentes en la compañía
- Evaluar las actividades antifraude existentes en la compañía
- Identificar áreas potenciales de remediación
- Establecer y ejecutar un plan para la remediación
- Crear documentación soporte
- Conducir recorridos o "walthroughs" formales
- Capacitar sobre conciencia de fraude, evaluación de riesgos de fraude, ética y valores
- Monitorear la efectividad de los controles

Tendencias en la gestión de riesgos de fraude

¿Cuáles han sido y serán los motivadores y móviles de fraude más frecuentes en su organización?



Tendencias en la gestión de riesgos de fraude

Figure 8. Does IA perform a regular fraud risk assessment exercise to consider, identify and prioritise risks of fraud?

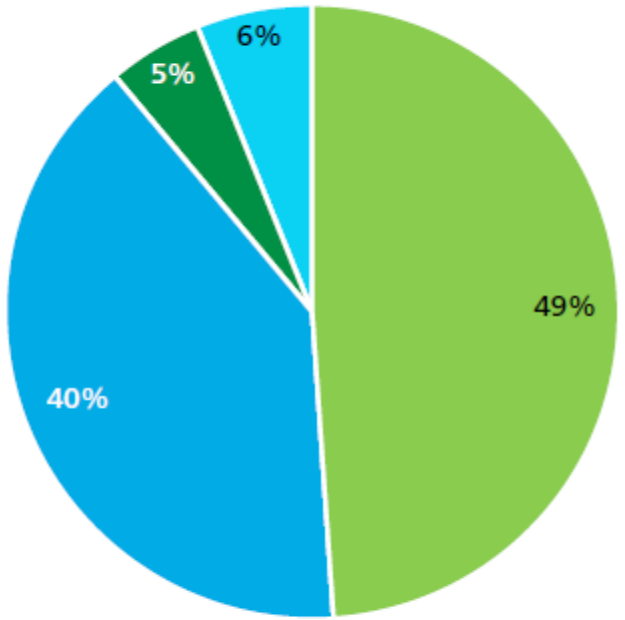
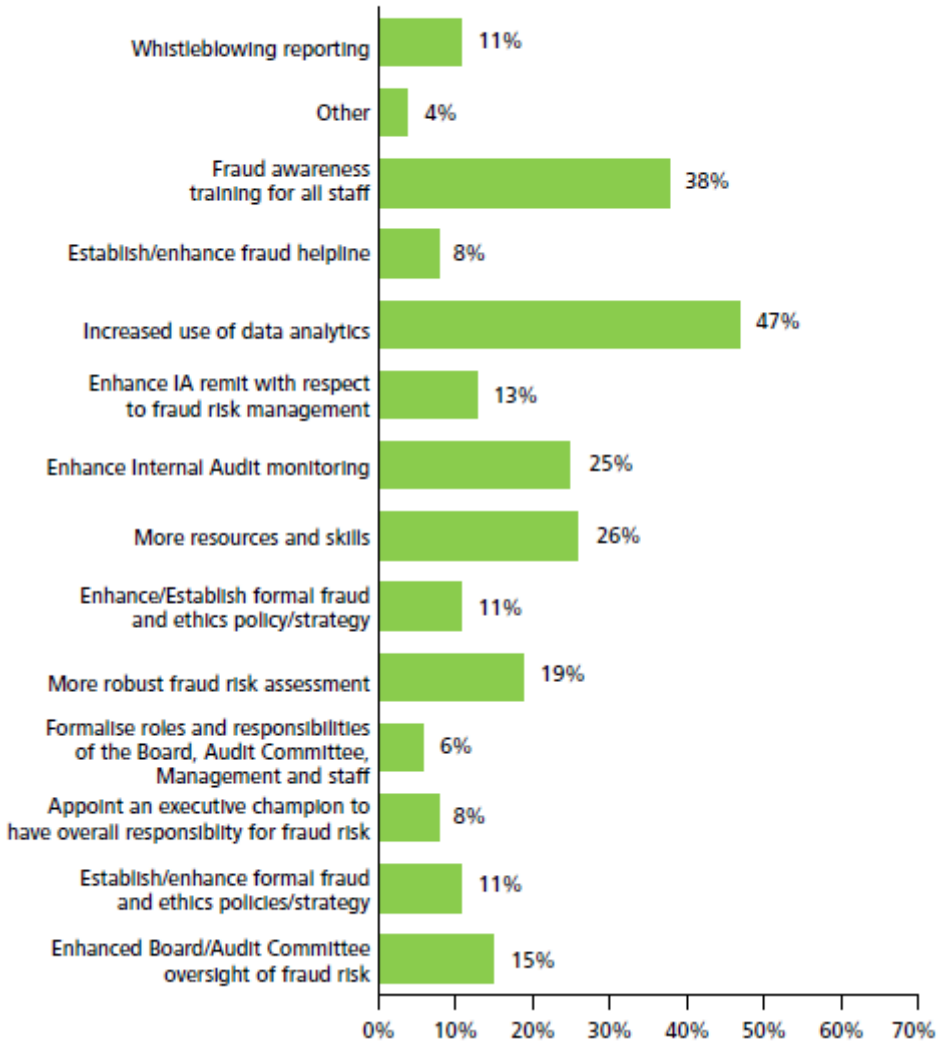


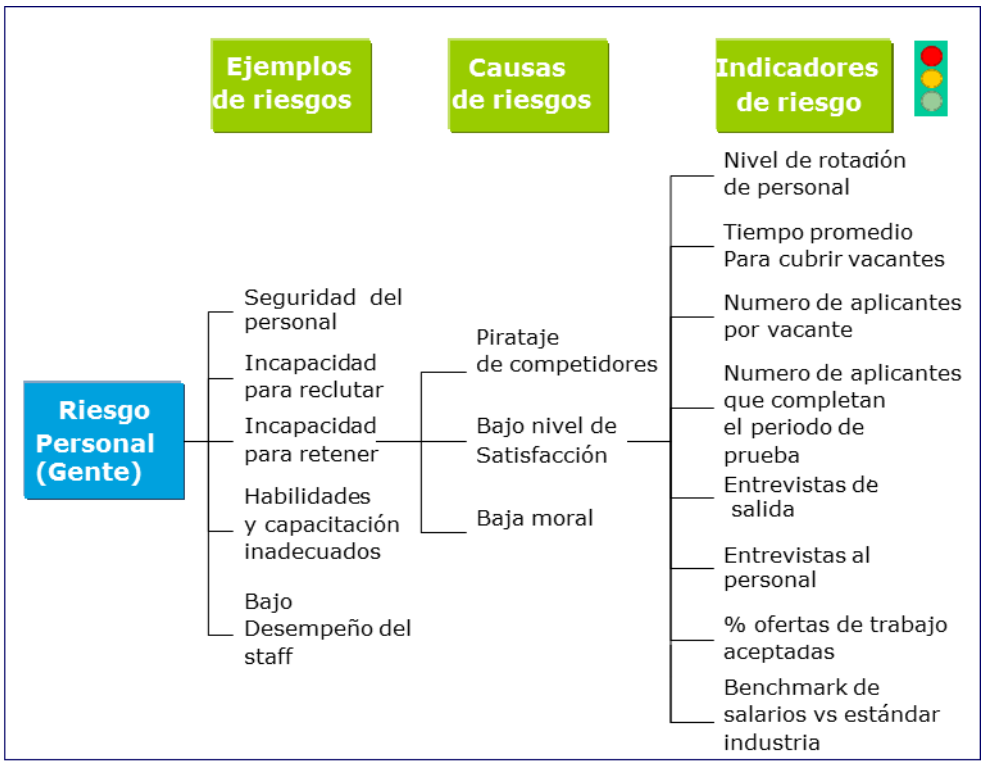
Figure 16. Which of the following would most help IA be more effective in providing assurance over fraud risk in the organisation?



4. Identifica y evalúa cambios que pueden impactar significativamente la gestión de riesgos

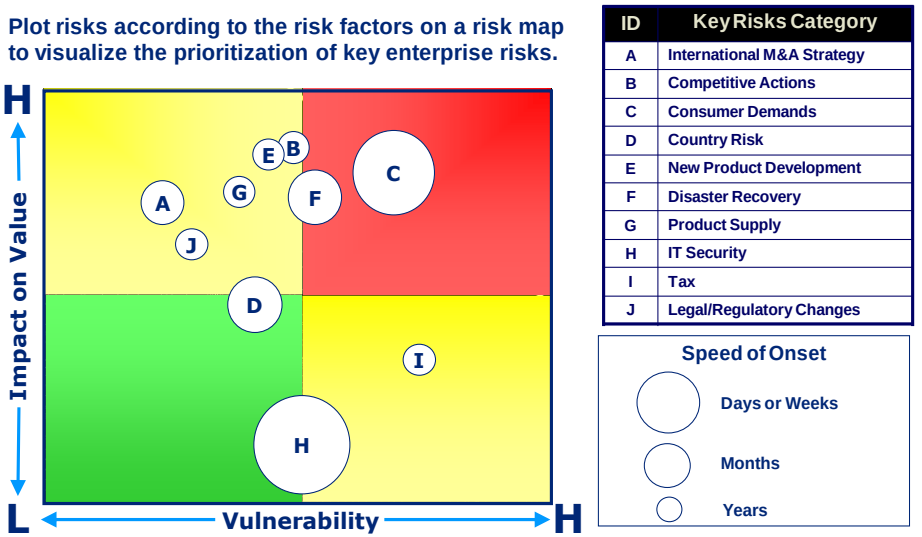
Monitoreo de alertas tempranas— atención en las métricas correctas

- Los indicadores clave de riesgos representan medidas que indican la presencia potencial, estado o tendencia de una condición de riesgo
- Cuando son diseñadas y utilizadas correctamente, las métricas de riesgos tienen un valor predictivo y pueden actuar como alertas tempranas para permitir acciones anticipadas



Evaluar el riesgo con un nuevo giro— ubicar el “Cisne Negro” antes de que él te encuentre

- En el libro *The Black Swan*, Nassim Taleb describe el impacto de eventos altamente improbables
- Evaluar riesgos con base en probabilidad asumida ha llevado a fallas catastróficas y grandes oportunidades perdidas
- La mayor parte de las herramientas y métodos de identificación de riesgos son retrospectivas. En un mundo cambiante, las premisas tradicionales no permanecen verdaderas
- Una nueva visión del riesgo implica considerar impacto vs vulnerabilidad vs velocidad de aparición, dejando en un segundo plano a la probabilidad.
- Proporciona un enfoque mejorado para priorizar la respuesta a los riesgos



Deloitte.