

Convergencia urgente:
Fomentando la inteligencia frente al
riesgo en las industrias de tecnología,
medios de comunicación &
telecomunicaciones



Tabla de contenidos

Prefacio	ii
La administración equivocada del riesgo de la empresa	1
La urgencia de converger	1
Promesa y peligro en la convergencia de TMT	3
La estructura de la inteligencia frente al riesgo	5
La estructura en acción	6
El anillo exterior: gobierno, personas, procesos y tecnología	7
Hacer la selección inteligente frente al riesgo	9
Para más información	9
Preguntas a considerar en relación con la inteligencia frente al riesgo	10
Contactos	11
¿Es su compañía inteligente frente al riesgo?	12

Prefacio

Esta publicación representa la novena entrega de nuestra serie acerca de Risk Intelligence [Inteligencia frente al riesgo]. Los conceptos y los puntos de vista que se presentan se elaboran a partir de los contenidos en el primer documento de esta serie, *The Risk Intelligent EnterpriseTM; ERM Done Right* [La empresa inteligente frente al riesgo; ERM aplicada en forma correcta], así como también en los títulos subsiguientes. Usted puede tener acceso gratis a los documentos anteriores de la serie en www.deloitte.com/RiskIntelligence.

La comunicación abierta y sincera es una característica clave de la empresa inteligente frente al riesgo. Fomentamos que usted comparta este documento con los colegas en los niveles ejecutivo, de junta y de administración principal de su compañía. Los problemas que aquí se señalan servirán como punto de partida para el diálogo crucial acerca de elevar en su compañía la inteligencia frente al riesgo.

Convergencia urgente: Fomentando la inteligencia frente al riesgo en las industrias de tecnología, medios de comunicación & telecomunicaciones

Con las tendencias de la convergencia acelerándose en las industrias de tecnología, medios de comunicación y telecomunicaciones (TMT*), ¿cuál debe ser el principal problema en su mente – la de un ejecutivo de TMT?

Quizás no el que usted espera. No son las fusiones y adquisiciones. No es el desarrollo de producto. No es la competencia o la tercerización.

Por el contrario, consideramos que usted le debe prestar mucha atención a... la *física*.

Sí, la física. En particular, le recomendamos que vuelva a leer de manera cuidadosa la Tercera Ley de Newton, que señala, “Para cada *acción*, hay una *reacción* igual y opuesta.”

Al interior de las TMT, la *acción* es la convergencia, la cual ha desvanecido las fronteras de la industria y que ha hecho que sectores anteriormente distintos se unan. La *reacción* opuesta, que a menudo pasa desapercibida, pero que sin embargo está al acecho, es la intensificación del riesgo. En la medida en que las compañías de TMT incursionan crecientemente en nuevos territorios – mercados no probados, alianzas inciertas, productos no familiares – los riesgos que enfrentan se multiplican de manera exponencial.

O, para decirlo en términos más sencillos: en la medida en que los sectores contraen, el riesgo se expande. Acción. Reacción.

Las compañías de TMT que fallan en prestarle atención a la lección fundamental de la física pueden encontrar que entra en juego otro principio newtoniano – la gravedad – al ver que sus elevadas aspiraciones para el crecimiento y la rentabilidad de manera permanente son puestas en tierra.

La administración equivocada del riesgo de la empresa

Algunos ejecutivos de TMT piensan, “El riesgo no es mi problema.” Consideran que la administración del riesgo es dominio de algún otro – quizás auditoría interna o el director de riesgo jefe o el director de cumplimiento jefe.

Si ello describe su manera de pensar, aquí hay unas pocas preguntas para usted: si falla la integración con su compañía de

medios de comunicación recientemente adquirida, ¿es un problema para algún otro, o es un problema para usted? Si su compañía no es capaz de hacerle seguimiento exacto a los ingresos ordinarios que fluyen entre sus socios de negocio, ¿quién tiene la culpa? Si su producto electrónico principal no puede ser repuesto con suficiente rapidez debido a problemas de producción con el socio de tecnología clave, ¿quién será en última instancia el responsable? Cuando llega el momento de presentarse ante la junta de directores y explicarle tales dificultades, ¿quién se está poniendo colorado?

Si esto no es suficientemente convincente, otros factores deben colocar al riesgo en lo alto de su lista. Por un lado, su mundo se está volviendo más complejo, con la creciente globalización, expansión de las cadenas de suministro, tercerización y deslocalización crecientes, fusiones & adquisiciones transfronterizas, y otros factores, todos ellos entrando en juego. Por otro, las agencias de noticias frecuentemente reportan juicios multimillonarios en dólares contra compañías que fallaron en identificar los riesgos relacionados con el comportamiento no ético de los empleados. Tercero, en muchos países, los reguladores y los intercambios financieros (tales como la SEC, PCAOB y NYSE en los Estados Unidos) todos ellos requieren o fomentan fuertemente las actividades de administración del riesgo. Al mismo tiempo, las encuestas recientes muestran que los CEO califican la administración del riesgo como su preocupación número uno. Otra encuesta señala que hasta tres cuartas partes de las compañías desearían por completo todo su programa de administración del riesgo y comenzarían de nuevo, si pudieran hacerlo razonablemente.¹ Mientras tanto, las juntas y los comités de auditoría de manera creciente desean aseguramiento de que los riesgos de su compañía han sido identificados y están siendo administrados.

¿Cómo debe usted abordar esos problemas crecientemente complejos, que intensifican las presiones regulatorias, y que escalan las demandas del *stakeholder* acerca de la administración del riesgo? Podemos resumir nuestra respuesta en dos palabras: “*Risk Intelligence*” [Inteligencia frente al riesgo].

La urgencia de converger

Varios factores le están dando orientación a la convergencia de la industria de TMT, principalmente la digitalización, la conectividad y la innovación

* TMT = Technology, Media & Telecommunications = Tecnología, medios de comunicación y telecomunicaciones (N del t).

¹ Open Compliance and Ethics Group (OCEG), 2007 OCEG Governance Risk & Compliance Strategy Survey, Sept. 2007. www.oceg.org/view/GRCStrategyStudy

Características de la inteligencia frente al riesgo

Las empresas inteligentes frente al riesgo [Risk Intelligent Enterprises™] son compañías que han logrado un estado avanzado de administración del riesgo. Muchas características definen a tales compañías. La empresa inteligente frente al riesgo:

Desarrolla visión de espectro total: Valora y administra de manera efectiva los riesgos a través de las divisiones, departamentos, compañías, y geografías.

Tiende puentes entre las islas: Reconoce la necesidad de especialización en relación con el riesgo – conocimiento profundo de los riesgos y respuestas específicos – pero construye puentes entre las “islas” de riesgo.

Habla un lenguaje común: Desarrolla una tecnología común sobre el riesgo, de manera que todos hablen el mismo lenguaje; y adopta métricas comunes, de manera que todos midan el riesgo de una manera comparable.

Valora el impacto: Reconoce que, con un número casi infinito de riesgos, la planeación para todos ellos no es práctica, si no imposible. Se centra en los impactos finitos que podrían resultar de las múltiples amenazas.

Sopesa la vulnerabilidad: Aumenta el énfasis que la administración convencional del riesgo da a la probabilidad y lo hace mediante darle peso importante a la vulnerabilidad, dado que el riesgo en el extremo a menudo es el más mortífero.

Considera la interacción del riesgo: Adopta un enfoque que no solo considera los eventos de riesgo aislados, sino que también tiene en cuenta los escenarios de riesgo y la interacción de los múltiples riesgos.

Asigna los riesgos de manera apropiada: Realiza una valoración comprensiva del riesgo y luego prioriza y centra los esfuerzos en las áreas de mayor riesgo.

Cultiva la conciencia respecto del riesgo: Considera que la administración del riesgo es responsabilidad de toda la organización, hace parte de las operaciones diarias de la compañía y de las obligaciones rutinarias de su personal.

Y, muy importante, **Persigue asumir el riesgo en búsqueda de recompensa:** Busca no solo la mitigación del riesgo, sino que también persigue asumir el riesgo como un medio para la creación de valor

Tres niveles de convergencia

The Trillion Dollar Challenge: Principles for Profitable Companies (Deloitte Touche Tohmatsu, 2005), observa que la convergencia de TMT está ocurriendo en los siguientes tres niveles:

- 1) Los productos y servicios representan el nivel de convergencia más alto, proporcionando bienes y servicios que satisfacen las necesidades reales de los clientes – por encima y más allá de los actualmente disponibles. Sin embargo, el resultado se puede lograr solamente cuando está respaldado por la convergencia de la plataforma y la convergencia organizacional de los otros tres niveles.
- 2) La convergencia de la plataforma implica consolidación alrededor de un pequeño número de estándares – tales como protocolos de red, formatos de datos, y tipos de medios estándares – permitiéndoles a las compañías centrar sus esfuerzos, y creando masa crítica en el mercado. Por ejemplo, la adopción del Protocolo de Internet (IP = Internet Protocol) como el estándar universal para las comunicaciones digitales está apoyando múltiples dispositivos y aplicaciones de comunicación convergentes.
- 3) La convergencia organizacional implica diferentes personas de las compañías y diferentes sistemas de TI trabajando juntos para entregar un producto o servicio convergente. Dado que la mayoría de las ofertas de convergencia se extienden más allá de las capacidades de una sola organización – sin importar qué tan grande o diversificada sea – la convergencia en el nivel organizacional es generalmente un requisito previo para entregar un producto o servicio convergente.

Digitalización: El movimiento desde datos análogos a digitales está en la raíz de la convergencia, proporcionando un medio uniforme para la representación de todos los tipos de información. En la era pre-digital, cuando las palabras principalmente residían en papel, las imágenes en lienzos, la música en vinilo, e incluso los datos de computador en tarjetas perforadas, ningún dispositivo individual podría ajustarse a todo. Pero toda la información se convirtió a la forma digital – unos y ceros – y de repente un dispositivo convergente que pueda manejarla no es sólo una posibilidad, es algo inevitable. Con la destilación de la información en datos digitales, ésta puede verse y ser manipulada usando los mismos dispositivos, tecnologías, técnicas de procesamiento, redes, y medios de comunicación.

Conectividad: Las redes de conexión con cable y las redes inalámbricas se están volviendo más rápidas y más generalizadas: el 60 por ciento de los hogares en los países desarrollados está conectado a Internet; las redes móviles de voz y datos ahora cubren la mayoría de las principales ciudades; y las suscripciones a los celulares móviles ahora suman dos billones en todo el mundo.

Esta conectividad ubicua está cambiando de manera fundamental la naturaleza de los productos y servicios. En los viejos días, cuando el producto era enviado desde la fábrica, era literalmente un producto terminado, sin manera para incrementar sus capacidades o valor. Hoy, los productos están siendo diseñados con la conectividad incorporada, permitiéndoles que sean actualizados remotamente con nuevo contenido, interactividad, y capacidades. (Un ejemplo excelente de esto es el iPhone, para el cual Apple ha prometido actualizaciones periódicas para mejorar las características y funciones del teléfono). La conectividad puede comprimir el ciclo de vida del producto, permitiéndoles a las compañías entregar pronto nuevas características, haciendo por lo tanto que la oferta convergente sea más convincente.

Innovación: La tecnología continúa su avance incontenible. Observaciones tales como la Ley de Moore, sobre el incremento continuo en la velocidad de procesamiento del computador, permanecen hoy más válidas que cuando fueron promulgadas por primera vez hace cuatro décadas. Otras áreas clave de la tecnología, incluyendo el almacenamiento en discos duros y la memoria de estado sólido, también han progresado rápidamente. Los mejoramientos en la tecnología hacen que los productos sean más rápidos, más baratos, más pequeños, y más eficientes en términos de energía – permitiéndoles a los diseñadores empacar más capacidad y características en un solo dispositivo sin que sea difícil de manejar. Los teléfonos inteligentes más poderosos del presente, por ejemplo, reemplazan toda una sala llena de dispositivos y elementos independientes – teléfono, estéreo, buscador en la red, reproductor de video, calculadora, álbum de fotos, libro de citas, brújula, reloj de alarma, y más – con un solo producto que cabe cómodamente en su bolsillo. Los avances en la tecnología han ayudado a darle dirección a la tendencia de la convergencia, y continuarán haciéndolo, redefiniendo constantemente los límites de lo que es posible.

Promesa y peligro en la convergencia de TMT

Es probable que a usted se le tenga que vender las oportunidades que surgen de la convergencia. La tendencia es inexorable y la urgencia de converger es prácticamente irresistible. La convergencia en cualquier nivel – plataforma, organización, producto, o servicio – puede crear nuevas oportunidades de mercado y nuevas fuentes de ingresos ordinarios.

Pero seamos lúcidos. Toda iniciativa de negocios tiene sus peligros, y la convergencia de TMT puede tener más de los que son justos. La convergencia puede transformar las industrias, inspirar fundamentalmente nuevos modelos de negocio,

reestructurar las cadenas de valor, y cambiar el balance de poder. Todos ellos resultados maravillosos – si usted está del lado del ganador.

Para posicionarse a fin de tomar ventaja de la oportunidad que ofrece la convergencia, usted se tiene que preparar para abordar los riesgos asociados. La tabla que se presenta en la página 4 y la discusión que sigue ilustra unos pocos riesgos potenciales que las compañías de TMT encuentran comúnmente. Este no tiene la intención de ser un inventario comprensivo de todos los riesgos concebibles (lo cual, por supuesto, sería imposible producir). Más aún, es una muestra representativa de los posibles riesgos que pueden surgir.

¿Dónde está el riesgo?

¿Cuáles son los mayores riesgos que enfrenta su compañía? Si usted le hace seguimiento al dinero o monitorea los medios de comunicación o rastrea las tendencias regulatorias, usted puede asumir que el riesgo de información financiera es la mayor causa de insomnio de los ejecutivos. Pero una encuesta reciente sugiere que tal supuesto es incorrecto.

De acuerdo con una encuesta a más de 1,100 ejecutivos de TMT realizada durante un webcast Dbrief en Agosto 2007,^{*} los riesgos a la estrategia y operaciones de TI de lejos sobrepasaron a la información financiera como la preocupación principal. Aproximadamente la mitad de quienes respondieron citaron uno de esos dos riesgos; poco menos del 10 por ciento mencionó la información financiera.

^{*} Dbriefs for Financial Executives, "Risk Intelligence in the Technology, Media, and Telecommunications Industries," August 22, 2007. Para más información visite www.deloitte.com/us/dbriefs.

Estrategia

Modelos de negocio complejos. Han pasado décadas desde que cualquier compañía lo hacía todo – esto es, realizaba cada faceta de su negocio en casa y con su propio personal. Pero las tendencias hacia la tercerización, la deslocalización, la asociación y las alianzas se han acelerado en los últimos años. Tome como ejemplo el personal típico de computación: una compañía elabora los chips de memoria, otra los discos duros, un tercero la tarjeta de la red. Un fabricante taiwanés puede producir el monitor, mientras que una compañía mexicana crea el teclado. Hoy, la cadena de valor es una red de valor, con interrelaciones complejas entre las partes creando un conjunto completamente nuevo de riesgos.² Basta con decir, en la medida en que se incrementa su dependencia de organizaciones externas, *los riesgos de ellas* progresivamente se convierten en *los riesgos de usted*.

Administración de la propiedad intelectual. Las compañías de TMT gastan tiempo importante y grandes sumas en investigación y desarrollo del producto. Esta inversión tiene que ser protegida ante la infracción de patentes, robo, piratería, y otros peligros, a menudo con un enorme gasto. Sin embargo, la falta de protección puede ser aún más costosa, dado que los infractores erosionan la participación en el mercado y la rentabilidad.

² Vea "The Risk Intelligent Approach to Outsourcing and Offshoring" en www.deloitte.com/RiskIntelligence.

Principales riesgos de una compañía de TMT hipotética

Categoría de riesgo	Riesgos específicos
Estrategia	Modelos de negocio complejos Integración de fusión Administración de propiedad intelectual Asociaciones/ alianzas
Operaciones	Operación fuera de las competencias centrales Interrupción del negocio Riesgo de falla en cascada
Factores externos	Competencia incrementada Cambios en la demanda y preferencias de los clientes No control sobre los dispositivos del consumidor Tecnologías emergentes y de maduración rápida Hacer borrosas las barreras competitivas Vulnerabilidad de los productos y servicios digitales

Categoría de riesgo	Riesgos específicos
Legal	Reputación Anti-fraude/ FCPA
Cumplimiento	Riesgo regulatorio Comodín legislativo Inversiones en sociedades / negocios conjuntos
Finanzas	Requerimientos tributarios Modelos de ingresos ordinarios
Recursos humanos	Retención de talento Código de ética / conducta Planeación de la sucesión Administración compleja de recursos distribuidos
TI	Administración de derechos digitales Robustez de la infraestructura Seguridad y privacidad

Copyright © 2008 Deloitte Development LLC. All rights reserved

Operaciones

Operaciones por fuera de las competencias centrales. Que usted pueda construir un negocio rentable en, digamos, fabricación de unidades de disco para compañías de computación, ello no significa que usted será exitoso en desarrollar una línea de reproductores de MP3 para los consumidores. Una vez que usted se aventura más allá de sus competencias centrales, lo espera un mundo nuevo de riesgos potenciales.

Factores externos

Tecnologías emergentes y de maduración rápida. Incluso si usted consigue que su reproductor de música digital esté en las vitrinas virtuales, ¿está listo usted para hacerle frente al ritmo implacable de innovación y obsolescencia en su nuevo campo? En algunos sectores, los productos se desactualizan antes que lleguen al mercado.

Hacer borrosas las fronteras competitivas. En la era de la convergencia, se vuelve difícil incluso *identificar* la competencia, sin importar cuál sea la suerte de ella. Por ejemplo, muchas compañías de TV por cable se han ampliado más allá de sus orígenes de "tubería tonta" para incluir en su menú de ofertas el desarrollo de programas de TV, servicio de Internet de banda ancha, y servicio telefónico. Cuando el enemigo de ayer es el socio del mañana, cuando las compañías rutinariamente desechan un modelo de negocios y rápidamente acogen otro, la inteligencia competitiva simultáneamente se vuelve más ardua y más esencial.

Vulnerabilidad de los productos y servicios digitales. La apertura de Internet, la interoperabilidad de los dispositivos digitales, y la ubicuidad de los datos digitales son simultáneamente las fortalezas y las debilidades de la era digital. Los mismos sistemas que permiten la entrega sin restricciones de productos y servicios, también proporcionan los medios para que actores inescrupulosos se comprometan en actos viles. Esto no es únicamente un riesgo de seguridad – es un problema de administración del activo digital: cómo proteger la propiedad intelectual ante la copia y transmisión en todo el mundo y cómo prevenir la venta y el uso no autorizados de ese contenido.

Riesgo regulatorio: centro de atención puesto en la privacidad

Un área de riesgo clave para las compañías en la industria de TMT es administrar la red compleja de requerimientos en relación con el uso de información personalmente identificable. Las firmas de TMT tienen que considerar los riesgos y las implicaciones que surgen de su acceso a una variedad de datos privados que incluyen los registros de facturación y llamadas de los clientes, búsquedas en la red y hábitos de ver, registros de empleados / recursos humanos, e información compartida con compañías de tarjetas de crédito y otras. Esos problemas se vuelven aún más complejos debido a la maraña de leyes de privacidad que existen internacionalmente y en los Estados Unidos a nivel federal y estatal.

Cumplimiento

Riesgo regulatorio. En la medida en que las compañías de TMT se fusionan y convergen, sobre las entidades recientemente constituidas se generan requerimientos regulatorios desconocidos. Las compañías que operan en múltiples jurisdicciones pueden enfrentar aún desafíos más complejos. Y las organizaciones a través de la mayor parte del mundo necesitan prestar constante atención a un entorno en evolución, dado que las regulaciones son adoptadas, abandonadas y alteradas.

Cuando sus ojos (de riesgo) son más grandes que su estómago (de riesgo)

El apetito y la dieta no siempre coexisten de manera armoniosa. Algunas veces queda sensación de hambre. Algunas veces cuando se llega al postre ya se está saciado.

El mismo fenómeno puede darse en la administración del riesgo. Las compañías pueden definir cuidadosamente su apetito por el riesgo – qué tanto riesgo están dispuestas a aceptar en la búsqueda de lograr sus metas estratégicas – y aún así encontrarse sorprendidas por un riesgo del cual nunca estuvieron conscientes. En otras palabras, no se ajustaban su apetito por el riesgo y su dieta ante el riesgo.

Y así como ocurre con ciertos alimentos, que si se comen en combinación pueden causar indigestión, diferentes riesgos pueden combinarse o interactuar para crear nuevos y mayores riesgos. Por ejemplo, considere el caso hipotético de una compañía de servicios financieros que está administrando sus riesgos de moneda, de tasa de interés y de flujos de efectivo. La compañía encuentra un riesgo de privacidad – una base de datos de los clientes es robada – para el cual no estaba preparada. Rápidamente entran en juego otros problemas relacionados con el riesgo: riesgo reputacional, riesgo de litigación, y riesgo financiero. Los reguladores se involucran; las agencias calificadoras se preocupan; el costo del capital aumenta; cae la confianza del inversionista.

Esta es la razón por la cual es importante trabajar metódicamente mediante la estructura de la inteligencia frente al riesgo. Si bien en la administración del riesgo no se puede alcanzar la perfección, la estructura puede mejorar la probabilidad de que los eventos de riesgo pueden ser prevenidos o detectados antes que se llegue a la etapa de crisis.

Recursos humanos

Código de ética/conducta. La ética, los valores, y la relación riesgo/recompensa han llegado a las primeras páginas de las noticias para las compañías de TMT que “presionaron el sobre” demasiado rápido. (Para referencia, vea artículos de noticias recientes sobre retroactividad de las opciones en acciones y otros delitos.) Pero incluso quienes juegan limpio están sujetos a la aceleración del ritmo del cambio. Dada la creciente demanda por y el suministro limitado de talento, es crecientemente difícil identificar, atraer, y retener al personal con tecnología crítica en tecnología digital y entrega de contenido.

Retención de talento. En la “guerra” por el talento entran en juego muchos factores, incluyendo la intensa competencia por trabajadores en los Estados Unidos; las restricciones a la contabilidad de las opciones en acciones, que pueden obstaculizar los esfuerzos de reclutamiento de las compañías en crecimiento; y el “factor Google,” que tiene a Google vinculando a un porcentaje importante del mejor talento de TI en el Silicon Valley.

Administración compleja de recursos distribuidos. El conocimiento especializado requerido por las compañías de TMT presenta desafíos y riesgos complejos para conseguir la gente correcta con el conocimiento y las habilidades correctos en el lugar correcto y en el momento correcto. Ante la presión para hacer todo esto de una manera costo-efectiva, muchas compañías de TMT con sede en los Estados Unidos han buscado en el exterior, y en el proceso a menudo sin saberlo aumentaron los riesgos de su “gente” al entrar en mercados de trabajo desconocidos y menos seguros. Otra tendencia reciente ha sido el uso incrementado del uso de mano de obra contratada y la tercerización – lo cual cambia el control del conjunto de talento pero puede no reducir el riesgo inherente del talento. De hecho, cuando esas iniciativas son administradas pobremente, la compañía se expone a sí misma a más riesgo, no a menos riesgo.

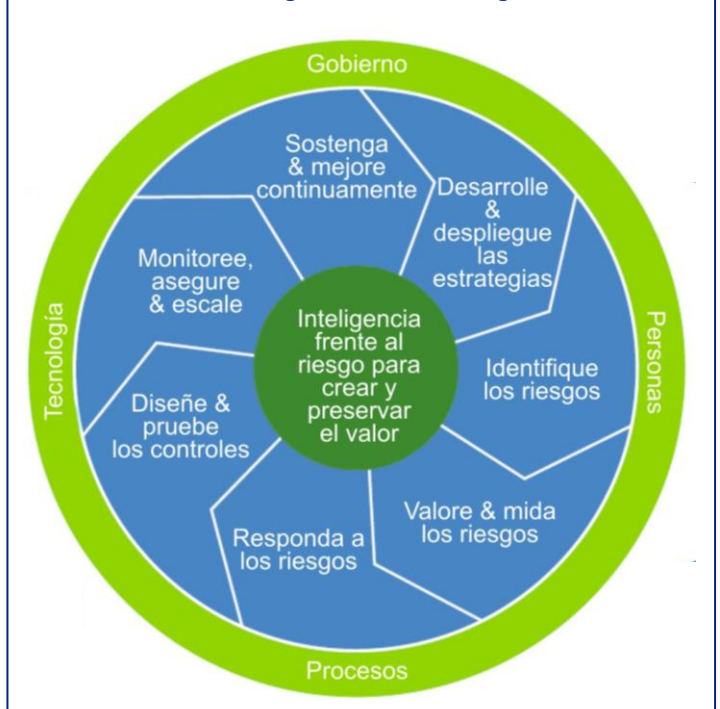
Tecnología de la información

Seguridad y privacidad. Las pérdidas de datos a menudo conllevan importantes consecuencias reputacionales, legales y financieras. ¿Es usted capaz de mantener seguros los datos de los clientes? ¿Tiene usted medios para identificar, compartir, proteger, monitorear y hacerle seguimiento a todas las formas de uso de los datos de los clientes?

La estructura de la inteligencia frente al riesgo

El objetivo de la estructura de la inteligencia frente al riesgo es asegurar que la meta primaria de la organización – la creación y preservación de valor – es buscada de una manera informada en relación con el riesgo, y que el riesgo es administrado de manera efectiva de una manera tanto centralizada como descentralizada. La meta inicial de la aplicación de la estructura es permitirle a la compañía identificar sus 10 o 20 riesgos más críticos y responder de manera apropiada frente a ellos. Sin embargo, los mismos principios pueden ser aplicados a todas las dimensiones (y a todos los niveles) de la organización – estratégico, operacional, financiero, legal y cumplimiento regulatorio, recursos humanos, TI, y similares.

La estructura de la inteligencia frente al riesgo



Implícitas en cada uno de los pasos del anillo interior están consideraciones que son críticas, si bien no siempre observadas de manera amplia. Usted puede descubrir que desempeña bien algunos de esos pasos, pero, de acuerdo con nuestra experiencia, es rara la compañía que administra todos los pasos de manera competente. La identificación de cuáles pasos necesitan desarrollo adicional representará uno de sus avances hacia la inteligencia frente al riesgo.

La estructura en acción

Para entender cómo la rueda de la estructura de la inteligencia frente al riesgo se relaciona con el mundo real, la aplicaremos a uno de los factores de riesgo de TMT citados antes: las tecnologías emergentes y rápidamente en maduración.

La innovación en TMT es implacable, proporcionando tanto riesgos (e.g., ser desbordados por la competencia) como oportunidades (e.g., lograr el dominio del mercado con un nuevo producto creativo). La presión para innovar es inexorable, y ninguna compañía de TMT que espere prosperar en el largo plazo puede ignorarla. La adopción de los principios de la inteligencia frente al riesgo puede ser un factor determinante entre el éxito y el fracaso.

1. *Desarrolle y despliegue estrategias:* En esta etapa temprana de planeación, usted primero debe identificar las metas estratégicas de su compañía a través del espectro de áreas de negocio. Luego, se mapean los planes de ejecución para lograr las metas. Para los propósitos de nuestro ejemplo, esas metas se relacionarán con las tecnologías rápidamente en evolución. Una compañía de electrónica de consumo, por ejemplo, puede establecer la meta de proporcionar actualizaciones principales de los productos clave cada 18 meses; se elaborarían planes de ejecución para identificar los recursos (financieros, humanos, externos, etc.) y los pasos necesarios para lograrlos.
2. *Identifique los riesgos:* En seguida, usted debe identificar de manera sistemática los riesgos que puedan frustrar el logro de sus metas. Esto se puede lograr mediante diversos medios, siendo el más común de ellos la planeación por escenarios. En este proceso, los ejecutivos, los administradores del riesgo y otro personal clave hacen lluvias de ideas alrededor de preguntas, tales como: ¿Cuáles riesgos podrían interrumpir nuestros planes? ¿Qué tan vulnerables somos frente a esos riesgos? En el caso de las tecnologías emergentes y en maduración, las posibles interrupciones podrían incluir: (1) grandes avances de tecnología por parte de los competidores; (2) recursos insuficientes dedicados a investigación y desarrollo; y (3) obsolescencia rápida de productos nuevos.
3. *Valore y mida los riesgos:* En esta fase, los riesgos identificados se valoran, miden y priorizan. Tome, por ejemplo, los tres riesgos que alrededor de las tecnologías en evolución se citaron arriba. Las actividades de valoración del riesgo pueden incluir recopilación de inteligencia para determinar los programas y progresos de la competencia; una valoración de I&D para determinar lo adecuado de la financiación en relación con los pares de la industria y las demandas del mercado; y un análisis del mercado para determinar la necesidad de reducir los ciclos entre los lanzamientos de los productos principales y las actualizaciones.

Observe que esas valoraciones pueden ser realizadas por los diferentes administradores del riesgo que trabajan en las diversas unidades de negocio. En tales casos, es crítico que las bases para la valoración sean comparables. Por ejemplo, sabemos de una compañía de TMT que de manera rutinaria

realizó cientos de valoraciones del riesgo en todas sus operaciones globales. Junto a las preocupaciones por la sobrecarga de información, las valoraciones fueron realizadas usando diferentes metodologías y criterios de calificación, haciendo imposible que la administración y la junta determinen dónde se deben realizar las inversiones relacionadas con la administración del riesgo. Se pueden evitar tales problemas mediante la coordinación y consolidación de las valoraciones del riesgo.

4. *Responda a los riesgos:* Son posibles varias respuestas a los riesgos identificados, dependiendo de las prioridades, recursos, apetito por el riesgo, y otros factores. Las opciones incluyen buscar, evitar, aceptar, transferir, y administrar (vea el recuadro, “Respuestas frente al riesgo,” en la página 8).

Inteligencia frente al riesgo ≠ ERM

Si bien la empresa inteligente frente al riesgo aborda los riesgos a través de toda la organización, ello no implica que la inteligencia frente al riesgo sea lo mismo que ERM. Ni la inteligencia frente al riesgo es “sólo otro nivel de administración del riesgo.” Más aún, la inteligencia frente al riesgo representa un cambio en la manera como las funciones existentes de administración del riesgo trabajan, colaboran, y piensan acerca del riesgo. Un enfoque inteligente frente al riesgo nunca abandona las capacidades existentes ni comienza desde cero. Más, aún, construye a partir de las competencias y experiencias que ya existen en la organización. La inteligencia frente al riesgo le proporciona a la administración principal y a la junta mejores luces – mejor inteligencia – sobre la exposición de la compañía frente a los riesgos y cómo están siendo administrados.

Las recompensas de la inteligencia frente al riesgo incluyen:

- carga reducida en las operaciones de negocio
- costo más bajo de la administración del riesgo
- capacidad mejorada para prevenir, detectar, corregir, y escalar los problemas de riesgo críticos
- medios para mejorar la flexibilidad estratégica en los escenarios de riesgo tanto de “arriba” como de “abajo”
- capacidad para proporcionar a la junta y a los otros *stakeholders* un “nivel de comodidad” de que todo el rango de riesgos es entendido y administrado.

En nuestro ejemplo, si la valoración del riesgo determina que I&D está sub-financiada, la compañía puede seleccionar incrementar el presupuesto para la investigación en casa; desviar recursos internos hacia I&D (con un impacto neutral en el presupuesto); asociarse con una firma externa para aumentar la I&D; o invertir en tecnologías prometedoras que estén siendo desarrolladas por otras compañías.

5. *Diseño, implemente y prueba los controles:* En seguida, se ponen en funcionamiento controles para permitir que usted prevenga, detecte, y responda ante los eventos de riesgo. Si bien en muchos casos la selección más efectiva es la prevención, un evento puede estar más allá de nuestro control o capacidad para prevenir. Entonces entran en juego la detección, la respuesta y la recuperación. La detección requiere sistemas de alarmas tempranas para proporcionar suficiente plazo de ejecución para la respuesta: a más temprana sea la detección, mayor es su capacidad para intervenir exitosamente. La detección temprana también beneficia el asumir el riesgo en búsqueda de recompensa, dado que le da a las compañías la capacidad para reconocer y tomar ventaja de los eventos de “arriba”. En esta etapa muchas compañías incrementan el rol de la tecnología mediante desplegar controles automatizados, los cuales ofrecen los beneficios duales de reducir el costo en el largo plazo y mejorar la efectividad.
6. *Monitoree, asegure y escale:* Si bien son posibles muchas jerarquías organizacionales, nosotros recomendamos los siguientes roles: la administración asegura que los controles del riesgo están funcionando tal y como se intenta, y proporciona aseguramiento a la junta de que el riesgo está siendo administrado dentro del apetito de riesgo definido (vea el recuadro, “Cuando sus ojos [de riesgo] son más grandes que su estómago [de riesgo]”, página 5). Mientras tanto, auditoría interna proporciona reaseguramiento a la junta respecto de que se puede confiar en las aseveraciones de la administración. La “propiedad” del riesgo se mantiene en el nivel apropiado, el cual puede ser dentro de una unidad de negocios o geografía; los problemas relacionados con el riesgo se escalan hasta que la administración lo requiera.

En nuestro ejemplo de los riesgos asociados con las tecnologías emergentes, una firma externa de abogados descubre la aplicación de la patente de un competidor para una nueva tecnología que podría hacer obsoleto al producto de la compañía. El hallazgo se escala a la administración, quien inicia un plan de respuesta de múltiples facetas que incluye finanzas (investigar la posible adquisición del competidor); I&D (valora la viabilidad de la nueva tecnología); y mercadeo (determina el apetito del consumidor por este producto nuevo). Estas actividades se presentan a la junta según sea necesario para permitirles a los miembros que conozcan acerca del riesgo emergente y las acciones tomadas.

7. *Sostenga y mejore continuamente:* Una vez que estén en funcionamiento todos los componentes de la estructura de la inteligencia frente al riesgo, usted debe dar pasos para mejorar la eficiencia y la efectividad de la administración del riesgo. Esto implica un proceso continuo de armonizar (asegurar que los administradores del riesgo hablan todos el mismo lenguaje), sincronizar (coordinar a través de las fronteras institucionales) y racionalizar (eliminar la duplicación de esfuerzo).

Aplicado a nuestro ejemplo, los riesgos asociados con las tecnologías rápidamente en evolución serían regularmente revisados y actualizados por los administradores del riesgo en las diversas funciones y unidades de negocio. Sus esfuerzos serían coordinados a través de toda la organización, para

asegurar que se cubren todas las contingencias y que no se está dando duplicación de esfuerzo innecesaria o no intencional.

El anillo exterior: gobierno, personas, procesos y tecnología

El gobierno, las personas, los procesos, y la tecnología constituyen los fundamentos y la infraestructura para lograr la inteligencia frente al riesgo.

Gobierno – En la base fundamental está una estructura de gobierno que reconoce el valor de administrar los riesgos para crear y preservar el valor. La definición y la articulación de la tolerancia que por el riesgo tiene la organización, así como su enfoque frente a ellos, necesitan ser realizadas por la junta, implementadas a través de los diversos niveles de la administración, y verificadas por la auditoría interna. Es el fundamento a partir del cual se construyen todas las otras infraestructuras y procesos y guía a la junta en la dirección de la vigilancia de la administración.

Definida GRC

En el mercado existe mucha confusión acerca del término “GRC” – gobierno, riesgo y cumplimiento. Algunos lo consideran igual a las aplicaciones de software de computador; otros lo consideran sinónimo de las prácticas de gobierno corporativo. Nosotros consideramos que es todas esas cosas – y más.

Más que considerar por aislado los componentes de GRC, nosotros recomendamos un punto de vista más amplio, que abarca más, *inteligente frente al riesgo*, que reconoce y entiende las interdependencias de las tres áreas. El hecho es que usted no puede lograr buen gobierno sin prestarle atención al cumplimiento regulatorio; ni puede lograr el cumplimiento sin abordar los riesgos que le acompañan. Dado que las tres áreas no existen de manera independiente, nosotros consideramos que tiene eminente sentido tener un enfoque integrado, inteligente frente al riesgo, para abordarlos.

El enfoque inteligente frente al riesgo para GRC puede proporcionar un punto de vista de la empresa, integrado, sobre muchos de los desafíos de gobierno, administración del riesgo, y cumplimiento regulatorio que enfrenta su organización.

Este enfoque puede mejorar la capacidad de su compañía para anticipar y responder de manera proactiva a los riesgos emergentes; y puede ayudar a reducir la actividad basada-en-islas, las redundancias, los costos excesivos, y las inefectividades.

Respuestas frente al riesgo

Una vez que identifica y valora los riesgos, usted tiene que decidir cómo manejarlos. Aquí hay algunas opciones:

Buscar – Asumir de manera inteligente que el riesgo es fundamental para el éxito del negocio. Aún así persiste la aversión ante el riesgo. Por ejemplo, algunas compañías grandes de medios de comunicación están tan preocupadas por la administración de los derechos digitales que no han puesto disponible en línea su contenido. Esta postura tiene el efecto irónico de proporcionarle incentivo a los consumidores que desean que su contenido esté electrónicamente disponible para recurrir a métodos ilegales, lo cual a la compañía le cuesta perder ingresos ordinarios. Inversamente, las compañías que han visto las oportunidades y abordado los riesgos en la entrega digital han desarrollado modelos de negocio viables y sustanciales bases de clientes.

Evitar – Evitar el riesgo es una respuesta común. Por ejemplo, algunas compañías de telecomunicaciones están escogiendo no entrar en ciertos mercados a causa de preocupaciones percibidas en relación con el riesgo geopolítico. Factores tales como disturbios sociales, inestabilidad política, regímenes hostiles, guerra, insurgencia, y terrorismo pueden todos ellos entrar en juego. Además, infraestructura pobremente desarrollada o mantenida, educación inadecuada, corrupción, mercados inmaduros, y otras preocupaciones pueden disuadir a las compañías de ampliarse a mercados particulares a pesar del tremendo potencial al alza.

Aceptar – Por supuesto, siempre existirán factores de riesgo exógenos que uno tiene que aceptar. Por ejemplo, después de gastar billones en líneas de fibra óptica, las compañías de telecomunicaciones pueden enfrentar el riesgo de que los consumidores elijan no comprarle a las compañías de telecomunicaciones características y aplicaciones avanzadas y solamente comprar el servicio de banda ancha. El valor importante reside en las aplicaciones, y otras firmas pueden vender las aplicaciones sin invertir en la infraestructura.

Transferir – Cuando la exposición frente al riesgo cae fuera del apetito de riesgo de la compañía, o cuando la organización desea eliminar sorpresas o suavizar costos, entran en juego las actividades de transferencia del riesgo. Los seguros y los contratos de futuros son dos de los enfoques más comunes para la transferencia del riesgo. Las compañías deben tener seguridad de que la transferencia del riesgo se ajusta a sus expectativas. Por ejemplo, los consultores de computación y los desarrolladores de software que toman los errores y las omisiones de los seguros deben escrutar de manera cuidadosa cualesquiera excepciones a la cobertura.

Administrar – La administración inteligente del riesgo es, por supuesto, la estrategia más importante de todas. Por ejemplo, las compañías de telecomunicaciones han estado enfrentando una serie de demandas por una variedad de problemas de protección del consumidor, que varían desde alegatos de que han cargado excesivamente honorarios e impuestos a los clientes hasta demandas por la falla en revelar las limitaciones de la cobertura inalámbrica. Un enfoque inteligente frente al riesgo tiene que reconocer la vulnerabilidad de las compañías frente al escrutinio incrementado de parte de los reguladores en la onda de tales demandas altamente publicitadas y realizar acción para satisfacer tales amenazas. Por ejemplo, legisladores y reguladores han estado preocupados acerca de los honorarios por terminación temprana impuestos por los proveedores de servicios inalámbricos. Una serie de proveedores de servicios inalámbricos escogió administrar ese riesgo mediante el anuncio reciente de que haría pro rata de tales honorarios cuando los clientes realicen transferencia a otro proveedor.

Personas – La inteligencia frente al riesgo no es acerca de tener un CRO (chief risk officer = director de riesgo jefe) o una función de riesgo centralizada, sino sobre desafiar la manera como la organización percibe y administra el riesgo. Las compañías deben proporcionar entrenamiento basado-en-el-rol que entregue las capacidades y la conciencia de la administración del riesgo a las personas correctas en el tiempo correcto; dado que las personas se mueven alrededor de la organización, es imperativo que reciban entrenamiento en relación con los roles que se espera desempeñen de una manera oportuna. Generalmente, este es un proceso continuo, no un evento de “una vez y hecho.” La filosofía corporativa alrededor de las necesidades de asumir el riesgo necesita ser articulada e insertada en la manera como las personas hacen sus trabajos, y esto requiere entrenamiento y monitoreo de los resultados.

Procesos – Un enfoque inteligente frente al riesgo establece los elementos comunes y los vínculos entre los procesos de administración del riesgo – estableciendo el apetito por el riesgo a nivel corporativo, trasladando y llevando en cascada los umbrales a través de la organización, y asegurando un enfoque consistente para administrar y reportar. La estructura de la inteligencia frente al riesgo también se refiere a la integración de la inteligencia frente al riesgo y las actividades consistentes de administración del riesgo en la corriente de los procesos de planeación, administración, y

toma de decisiones operacionales en todos los niveles. Reconozca que los pasos dados en el anillo interior aplican no solamente a los procesos corporativos de administración del riesgo, sino que también necesitan ser insertados en los procesos principales para asegurar que la planeación y administración inteligentes frente al riesgo de hecho se convierten en parte del trabajo de todos. El proceso corporativo de administración del riesgo es crítico para entender las interdependencias del riesgo y para administrar más holísticamente al riesgo.

Tecnología – En las compañías más sabias, la tecnología juega un rol clave en la administración del riesgo. Las herramientas de software que permiten el monitoreo de los controles y ofrecen vistas “tipo cuadro de mando” son dinámicas y evolucionan rápidamente, siendo continuamente desarrolladas capacidades nuevas y mejoradas. La tecnología puede ser aprovechada para proporcionar plataformas comunes para identificar, medir, reportar y monitorear los riesgos; actualmente hay una serie de soluciones y están surgiendo otras, incluyendo las suites “GRC” de los proveedores de ERP líderes. Tales suites proporcionan una oportunidad para racionalizar y automatizar los controles a través de las islas y dominios de la administración del riesgo, incrementando por consiguiente tanto la efectividad como la eficiencia de los controles.

Evolución al interior de una compañía de TMT inteligente frente al riesgo

Establezca un entorno de facilitación	<ul style="list-style-type: none">• Identifique los campeones en toda la empresa.• Comunique y haga de forzoso cumplimiento tanto la autoridad como la <i>accountability</i> por la toma de decisiones en relación con el riesgo.• Refuerce el “tono desde lo alto” mediante buen gobierno, códigos de conducta, y declaraciones de los valores compartidos
Logre cobertura para toda la empresa	<ul style="list-style-type: none">• Emplee actividades de administración del riesgo que cubran todos los tipos de riesgo y todas las unidades de negocio que sean materiales.• Implemente enfoques híbridos empleando las mejores técnicas basadas en probabilidad y vulnerabilidad.
Tome ventaja de los efectos del portafolio	<ul style="list-style-type: none">• Adopte un punto de vista de portafolio de los riesgos, que naturalmente compense las exposiciones frente al riesgo.• Mida las exposiciones frente al riesgo tanto desde arriba-hacia-abajo como desde abajo-hacia-arriba para volverse plenamente inteligente frente al riesgo.
Incorpore al riesgo en la estrategia	<ul style="list-style-type: none">• Evalúe los riesgos en los diversos niveles, desde el nivel general de la empresa hasta los niveles de unidad de negocios, proyecto, producto, o incluso transacción.• Use nuevas métricas para integrar al riesgo con la administración del desempeño.

Las empresas inteligentes frente al riesgo que son más efectivas y eficientes en la administración de los riesgos tanto para los activos existentes como para el crecimiento futuro, en el largo plazo, se desempeñarán mejor que las que lo hagan con menos efectividad y eficiencia.

Copyright © 2008 Deloitte Development LLC. Reservados todos los derechos

Hacer la selección inteligente frente al riesgo

Para sobresalir en los mercados que convergen, su compañía de TMT tiene que considerar al riesgo de maneras nuevas y tiene que abordar al riesgo de manera agresiva. En la medida en que usted se amplía más allá de sus dominios tradicionales y se mueve fuera de sus zonas de comodidad, usted puede mejorar sus prospectos mediante la adopción de los principios de la inteligencia frente al riesgo. Esto le permitirá a usted moverse más allá de valorar y reaccionar para anticiparse y responder de manera proactiva frente a los riesgos. Las compañías inteligentes frente al riesgo administran el asumir el riesgo en búsqueda de recompensa, haciéndolo tan agresivamente como administran los riesgos para los activos existentes.

El proceso puede parecer de enormes proporciones y, además, lograr la inteligencia frente al riesgo es un emprendimiento importante. Sin embargo, así como ocurre con cualquier iniciativa principal, los pasos pequeños pueden conducir a grandes resultados. No muerda demasiado en una sola vez; más aún, comience con las áreas de mayor vulnerabilidad (las que impactarán el precio de sus acciones si el riesgo se convierte en realidad) y dele forma a su trabajo descendiendo en la lista. Manejada de esta manera, su jornada hacia la inteligencia frente al riesgo se vuelve más manejable y navegable.

No se equivoque – el panorama está cambiando en el espacio de TMT. Las compañías que puedan capitalizar a partir de las tendencias y oportunidades clave, al tiempo que reconocen, asumen y administran el riesgo, estarán más efectivamente posicionadas para el éxito en el largo plazo.

Para más información

¿A dónde ir desde acá? La mayoría de las organizaciones se beneficiarán de toda nuestra serie de documentos sobre *Risk Intelligence* [Inteligencia frente al riesgo] que ofrece comparaciones y una hoja de ruta para abordar los cómo del gobierno, personas, procesos y tecnología de la administración efectiva del riesgo. La serie, ahora respaldada por el nuevo Risk Intelligence Map [mapa de la inteligencia frente al riesgo], ofrece perspectivas sobre la inteligencia frente al riesgo provenientes de puntos de vista de la industria y funcionales. Visite www.deloitte.com/RiskIntelligence para tener acceso a toda la serie de documentos.³

³ En español, buena parte de ellos puede descargarlos de: http://www.deloitte.com/view/es_CO/co/biblioteca-tecnica/recursos-auditora/erm/index.htm.

Preguntas a considerar en relación con la inteligencia frente al riesgo

- ¿Qué tanto podríamos perder si no administramos inteligentemente el riesgo?
- ¿Cuál es la probabilidad de que el riesgo ocurra?
- ¿Cuál es nuestra vulnerabilidad frente a este riesgo?
- ¿El riesgo está correlacionado con otras exposiciones frente al riesgo?
- ¿El riesgo representa una concentración de riesgo que pueda causar problemas en la administración o mitigación del riesgo?
- Si cubro o mitigo este riesgo, ¿cómo esto cambia la probabilidad y el impacto?
- ¿Nuestra estrategia de administración o mitigación del riesgo introduce cualesquiera riesgos adicionales?
- ¿Qué tanto podemos ganar si asumimos este riesgo – provisto que lo administramos de manera apropiada?
- ¿Cómo podemos tener aseguramiento de que nuestra confianza está justificada?
- ¿Qué tanto nos está costando (o nos costará) administrar este riesgo?
- ¿A partir de este riesgo hay un potencial impacto de riesgo reputacional?
- ¿Qué persona o equipo es responsable por administrar este riesgo desde el principio?

Contactos

Para más información sobre la inteligencia frente al riesgo y sobre la administración del riesgo en las industrias de TMT, por favor contacte a:

Mark Layton

Global Leader, Enterprise Risk Services
Deloitte & Touche LLP
+1 214 840 7979
mlayton@deloitte.com

Igal Brightman

Global Managing Partner
Technology, Media and Telecommunications
Deloitte Touche Tohmatsu
+972 3 608 55 00
ibrightman@deloitte.co.il

Eddie Leschiutta

Managing Partner
Enterprise Risk Services – Canada
Global TMT Enterprise Risk Services Leader
Deloitte & Touche LLP
+1 416 601 5841
eleschiutta@deloitte.ca

Phil Asmundson

Vice Chairman
U.S. Technology, Media and Telecommunications
Leader
Deloitte LLP
+1 203 708 4860
pasmundson@deloitte.com

Tom Connors

Partner, Enterprise Risk Services
Deloitte & Touche LLP
+1 212 436 2617
tconnors@deloitte.com

Carol Matthey

Managing Director
Technology, Media & Telecommunications
Regulatory & Capital Markets Consulting
Deloitte & Touche LLP
+1 703 251 3730
cmatthey@deloitte.com

James McDonnell

Principal
Deloitte Consulting LLP
+1 212 618 4130
jmcdonnell@deloitte.com

Peter Vogel

Senior Manager
Deloitte Consulting LLP
+1 212 618 4018
pevogel@deloitte.com

T. Brent Iredale

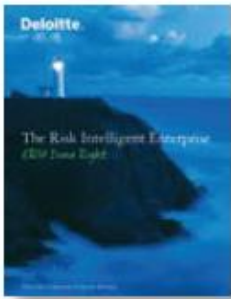
Senior Consultant
Deloitte Consulting LLP
+1 404 631 2192
tiredale@deloitte.com

Mark Baylis

Senior Manager
Deloitte & Touche LLP
+1 617 437 2353
mbaylis@deloitte.com

¿Es su compañía inteligente frente al riesgo?

Vea toda nuestra serie de documentos sobre la inteligencia frente al riesgo, que incluyen los siguientes:



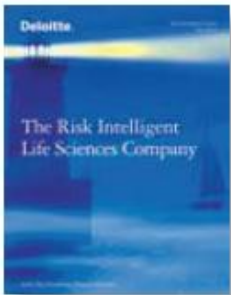
No. 1:
The Risk Intelligent Enterprise: ERM Done Right



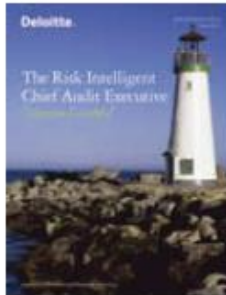
No. 2:
Risk Intelligence in the Age of Global Uncertainty



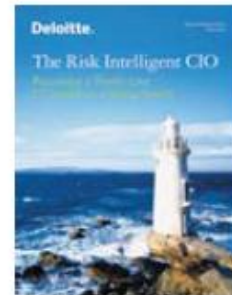
No. 3:
The Risk Intelligent Enterprise: ERM for the Energy Industry



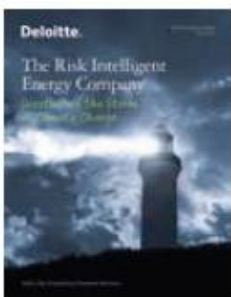
No. 4: *The Risk Intelligent Life Sciences Company*



No. 5: *The Risk Intelligent Chief Audit Executive: Mission Possible*



No. 6: *The Risk Intelligent CIO: Becoming a Front-Line IT Leader in a Risky World*



No. 7: *The Risk Intelligent Energy Company: Weathering the Storm of Climate Change*



No. 8: *The Risk Intelligent Approach to Outsourcing and Offshoring*



No. 9: *Urgent Convergence: Fostering Risk Intelligence in the Technology, Media & Telecommunications Industries*

Visite www.deloitte.com/RiskIntelligence para descargar copias electrónicas, o contacte a su profesional de Deloitte para copias impresas. No hay cargo por estas publicaciones.

Esta es una traducción al español de la versión oficial en inglés de **Urgent Convergence: Fostering Risk Intelligence in the Technology, Media & Telecommunications Industries**, publicado por Deloitte Development – 2008 – Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte & Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited, sociedad del Reino Unido no cotizada limitada mediante garantía y a su red de firmas miembro, cada una de las cuales es una entidad con personalidad jurídica propia e independiente. Consulte la página www.deloitte.com/about si desea obtener una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, tributación, consultoría y asesoramiento financiero a clientes públicos y privados en un amplio espectro de sectores. Con una red de firmas miembro interconectadas a escala global extendida por 150 países, Deloitte aporta las mejores capacidades y unos amplios conocimientos expertos a escala local que ayudan a sus clientes a tener éxito allí donde operan. Los 170.000 profesionales de Deloitte están comprometidos para convertirse en modelo de excelencia.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o entidades asociadas (conjuntamente, la "Red Deloitte"), pretenden, por medio de esta publicación, prestar servicios o asesoramiento profesionales. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar a un asesor profesional cualificado. Ninguna entidad de la Red Deloitte se hace responsable de las pérdidas sufridas por cualquier personal que actúe basándose en esta publicación.