ALEXANDRA PSICA, CMC
DIRECTORA GENERAL
INTERIS CONSULTING INC.

Un enfoque a su medida

Auditoría de los enfoques de ERM

El enfoque ideal para la ERM se diseña de forma personalizada para que se adecue a los objetivos de la organización, al nivel de riesgo inherente y a la tolerancia a los riesgos; lo suficiente como para maximizar sus oportunidades pero no demasiado para que no quede en una posición comprometida. La ERM, basada en la cultura de gestión de riesgo de la organización, reproduce todas las prácticas de negocios que una organización implementa para evaluar, comunicar y gestionar los riesgos. Un enfoque de ERM adecuado permite a la organización prever las consecuencias potenciales de eventos futuros, implementar los cambios necesarios para minimizar los riesgos, gestionar las secuelas negativas si se materializa un evento, y capitalizar las oportunidades que ofrece para el crecimiento. Asegura que los encargados de tomar las decisiones tengan acceso de forma oportuna a la información crucial para la elección de las opciones adecuadas, dentro de los límites establecidos de tolerancia al riesgo, a fin de conducir a la organización hacia el logro de sus objetivos. Al hacerlo, el enfoque de ERM ayuda a guiar la asignación de recursos y a reforzar el gobierno. ■ Más aún, los enfoques de ERM permiten la divulgación de información y proporcionan a la dirección, el consejo y los accionistas la seguridad de detectar la evolución de los riesgos con la anticipación necesaria como para poder mitigarlos. No todos los riesgos pueden evitarse, pero su revelación temprana otorga un margen de tiempo adecuado para tomar

Las revisiones de la ERM aseguran que la organización posee una base sólida para evaluar y mitigar los riesgos.

medidas apropiadas, para poder identificar y maximizar cualquier ventaja potencial. Los enfoques de ERM también permiten que las organizaciones unan la información utilizada por las diferentes funciones, como auditoría, cumplimiento y gestión. ■ La auditoría desempeña un papel clave en asegurar que el enfoque de ERM de la organización sea lo suficientemente fuerte como para ejecutar la función deseada y lo suficientemente eficiente, como para asegurar un buen valor. Dado que los enfoques de ERM pueden variar en función del propósito, tamaño, complejidad y madurez de la organización, los auditores deben confiar en su buen criterio para poder concluir si el enfoque es adecuado para el contexto de la organización.

FUNCIÓN DE LA AUDITORÍA

Un enfoque de ERM consiste en un conjunto de prácticas de negocios respaldado por la cultura de gestión de riesgo, que a su vez evalúa, gestiona y comunica los riesgos a un nivel adecuado según los objetivos, las operaciones y el perfil de riesgo de la organización (consulte "Principios que rigen el enfoque de ERM", en la página 54). Normalmente, incluye políticas y guías de fácil seguimiento; procesos y técnicas prácticos, flexibles y autodirigidos; y herramientas que apoyan la gestión de la información relativa a los riesgos para su identificación, evaluación, gestión, comunicación y supervisión. Sin embargo, de una organización a otra o incluso en una misma organización, el enfoque de ERM puede ser muy diferente, en función del nivel de riesgo inherente asociado con los objetivos de negocio al igual que con la tolerancia al riesgo. Por ejemplo, el departamento de tecnología de la información puede exigir un marco con procedimientos claros para la identificación, evaluación y reajuste de los riesgos debido a la naturaleza de sus tareas, mientras que el departamento de recursos humanos puede requerir sólo de una política clara y una revisión de los procedimientos. También es frecuente encontrar que el área de la organización que se ocupa de las operaciones de transacción posee un marco maduro, orientado al cumplimiento, en el que se definen claramente los indicadores de riesgo y que puede estar incluso integrado a los procesos cotidianos, mientras que la parte de la organización que se dedica a los riesgos estratégicos cuenta con un marco menos formal que requiere más desarrollo. Debido a que los recursos de auditoría interna se orientan generalmente a las áreas de mayor riesgo, resulta fundamental que el enfoque de ERM se audite periódicamente para asegurar que permite identificar los riesgos adecuados para la producción de informes confiables, en función de los cuales asignar los recursos, planificar la auditoría y tomar otras decisiones. Es más, dado que la convergencia impulsa a la organización a buscar sinergia entre las funciones de auditoría, cumplimiento y gestión de riesgo, resulta importante brindar aseguramiento de que la función de gestión de riesgos es sólida, de modo tal que las diferentes partes de la organización puedan confiar en los resultados de la función. Los auditores deben considerar todos los objetivos que la organización espera que sean cumplidos por el enfoque de ERM al momento de diseñar la auditoría y de evaluar si es adecuado.

La clave para una auditoría exitosa del enfoque de ERM reside en la capacidad del auditor para evaluar adecuadamente el equilibrio óptimo entre el nivel de madurez de las prácticas de ERM y el nivel de riesgo que enfrenta la organización. Dado que se trata de una práctica de negocio incipiente, es poco realista esperar que las organizaciones hayan desarrollado completamente su capacidad

de ERM. Es responsabilidad del auditor dar su opinión sobre el objetivo de la auditoría, como por ejemplo, sobre la eficiencia y la eficacia del enfoque. No obstante, los auditores también deben tener en cuenta el contexto de la organización, incluyendo las fallas del enfoque que se producen como resultado del plazo del que ha dispuesto la organización para establecer el enfoque y el presupuesto que puede dedicar de forma realista a la ERM. Además, las auditorías deben considerar la gestión de riesgo operacional (riesgos en la prestación diaria) y la gestión de riesgo corporativo (riesgos para el logro de los objetivos de negocio). En resumen, lo esencial de auditar el enfoque de ERM es que resulte útil en mejorar la gestión de la organización.

Al auditar un enfoque de ERM es importante distinguir entre evaluar la eficacia del enfoque dentro de la organización, y evaluar la responsabilidad de la dirección para tomar decisiones y para supervisar la eficacia de estas en mitigar riesgos individuales. La auditoría del enfoque de ERM se centrará en la eficacia del marco para ayudar a la organización a gestionar el riesgo; y no, en evaluar si la dirección tomó las decisiones correctas. Es más, en numerosas organizaciones, los auditores internos deben caminar en la cuerda floja para mantener la independencia necesaria para auditar el enfoque. Como son expertos en riesgos, frecuentemente se recurre a ellos para obtener asesoramiento, no obstante es fundamental que la dirección se apropie del enfoque y los procesos de ERM para que la auditoría interna pueda ofrecer una opinión objetiva acerca de su eficiencia y eficacia.

COMPONENTES DEL ENFOQUE

Un enfoque para la ERM no consiste en una sola política sino en una selección de componentes que pertenecen a una organización y que trabajan conjuntamente para gestionar el riesgo de forma eficaz y eficiente a través del tiempo. Es tarea del auditor evaluar si la suma de estos componentes conforma un enfoque adecuado para la organización. Interis Consulting ha desarrollado un modelo conceptual de ERM que se basa en las prácticas de gestión de riesgo del sector público, del sector financiero y de otras industrias, y al mismo tiempo, en criterios de la gestión de riesgo y de las normas de control. El modelo conceptual se ocupa de los componentes principales de un enfoque de ERM eficaz y sustentable: establecimiento del enfoque, implementación de prácticas y procesos para evaluar y abordar los riesgos, y supervisión del enfoque.

ESTABLECIMIENTO DEL ENFOQUE Cuando se audita un enfoque de ERM, los auditores deben prestar atención a las actitudes y los valores expresados en relación con la gestión de riesgos en las políticas de la organización, el marco de gobierno y el conjunto de procesos y herramientas de gestión de riesgos. A pesar de que los auditores no participan en el establecimiento del enfoque (el cual debe ser diseñado por la empresa misma), cuando llevan a cabo una auditoría, están evaluando los elementos del enfoque de la organización. En determinadas organizaciones, los auditores encuentran elementos del enfoque que incluyen valores explícitos de gestión de riesgo, pautas exigentes y claras para la gestión de riesgo destinadas al personal, y sólidos programas de capacitación en gestión de riesgo. En otras organizaciones, puede resultar más difícil para el personal identificar las prácticas de gestión de riesgo, especialmente si la ERM es nueva para la organización. Es posible que los auditores necesiten adaptar su vocabulario para asegurarse de que el personal comprenda lo que representa la gestión de riesgo en el propio trabajo. Es especialmente importante en esos casos tener en cuenta diversas fuentes de evidencia para asegurar que la ERM arraigada en la organización (las prácticas de gestión de riesgo que no se identifican como tales dentro de la organización), no sea desestimada por la dirección. Una vez establecido el enfoque, la organización implementa los elementos que lo componen y lleva a cabo actividades continuas de gestión de riesgo (evalúa y aborda los riesgos de forma regular). Los auditores deben buscar evidencias de que las prácticas de gestión de riesgo definidas en el enfoque se están utilizando y funcionan de acuerdo con lo previsto.

EVALUACIÓN DE RIESGOS Durante la auditoría de los procesos continuos de gestión de riesgos, los auditores deben observar si se documentan claramente los objetivos de negocio ya que el personal debe saber en qué consisten los objetivos para gestionar los riesgos que los afectan. Los auditores, en función de una comprensión del entorno de negocio de la organización, deben verificar si la organización cuenta con un proceso coherente de identificación de riesgos que aborde todas las categorías de riesgo a los cuales la empresa está inherentemente expuesta. De la misma manera, deben determinar si existe un proceso formal de evaluación de riesgos, si se examina la exposición al riesgo residual comparándola con las tolerancias al riesgo establecidas por la dirección, y si se documentan y comunican las respuestas formales a los riesgos.

TRATAMIENTO DE LOS RIESGOS Para evaluar si la organización está abordando los riesgos de forma adecuada, los auditores deben buscar planes de acción para la gestión de los riesgos inaceptables, que incluyan medidas específicas de mitigación, cronologías y responsables a cargo. Regularmente, se deben revisar y supervisar dichos planes de acción para controlar su eficacia en la reducción de los riesgos. Los miembros de la organización responsables por la gestión de riesgo deben identificar y supervisar de forma regular los indicadores de riesgo clave para proporcionar una advertencia temprana de la materialización de los riesgos. Por último, los auditores deben controlar si existe un enfoque estandarizado para la gestión de la información sobre los riesgos, con terminología y datos comunes.

SUPERVISIÓN DEL ENFOQUE La organización debe disponer de procesos y prácticas que le permitan supervisar la eficacia del enfoque de ERM. Normalmente, el auditor debe buscar los objetivos e indicadores preestablecidos en función de los cuales se miden los procesos y el enfoque de ERM. Si el objetivo consiste en la cobertura total de los riesgos de toda la organización, entonces la cantidad de divisiones que hayan completado un perfil de riesgo puede constituir un indicador. Los auditores deben evaluar si la dirección supervisa el enfoque para asegurar que los

A pesar de que los auditores no participan en el establecimiento del enfoque (el cual debe ser diseñado por la empresa misma), cuando llevan a cabo una auditoría, están evaluando los elementos del enfoque de la organización.

procesos funcionen de la forma prevista, y si existe una supervisión independiente que controle la calidad de la gestión de riesgo y la diligencia debida para la toma de decisiones relativas a los riesgos.

EL PROCESO DE AUDITORÍA

Si bien las auditorías del enfoque de ERM se parecen a otros tipos de auditorías en cuanto a su proceso básico, se diferencian de ellas por su contenido debido a la naturaleza única de cada enfoque. Los auditores deben evaluar si el enfoque de la organización satisface las necesidades de forma adecuada.

ALCANCE Si bien la determinación de su alcance representa un paso importante para todas las auditorías, resulta especialmente crítico para los enfoques de ERM porque las actividades de gestión de riesgo constituyen una función dominante que frecuentemente no se identifica como gestión de riesgo. Por ejemplo, la organización puede contar con un manual de procedimiento operativo que sirve para la gestión de riesgo pero no se lo denomina manual de gestión de riesgo. Cada organización confía en combinaciones diferentes de sistemas, personas y tecnología para identificar y gestionar el riesgo, y los auditores deben revisarlos a todos. Para una auditoría de la ERM puede resultar necesario incluir la revisión del programa de capacitación operacional si la gestión de riesgos forma parte del mismo. Los auditores internos pueden conocer los objetivos, los procesos, la madurez, las condiciones comerciales y el perfil de riesgo de una organización a través del examen de los aspectos clave que definen al negocio, como por ejemplo:

- El propósito de la organización, su misión, programas y servicios, objetivos y resultados clave.
- Las partes interesadas que integran la organización o se relacionan con la misma, entre ellas, los recursos, clientes y proveedores.
- Los procesos de trabajo y los sistemas de control clave para la consecución de la misión y los objetivos de la organización.
- Los ciclos de negocio de los programas, los servicios y las actividades principales y su interacción con otros ciclos de negocio.
- Los sitios en donde se prestan los servicios y programas.
- Las condiciones en las cuales se proporcionan los programas y servicios (por ejemplo, económicas, normativas, políticas o legales)
- Las tendencias o la estabilidad de los factores precedentes.

Es fundamental que el auditor conozca la exposición de la organización a riesgos y amenazas, así como los antecedentes en el tratamiento de ellos. Por ejemplo, para la auditoría de un departamento de gobierno de gran envergadura, los auditores de Interis destinaron el primer tercio del trabajo a planificar la tarea, determinar el alcance de la auditoría, conocer el entorno, captar el sentido del enfoque filosófico del tratamiento de los riesgos, y entender los riesgos de alto nivel que afectan el trabajo. Después de obtener un conocimiento sobre la organización que les sirviera de base, la dividieron en áreas clave, como funciones operacionales y recursos humanos, y restringieron la auditoría a las tres áreas para las cuales la gestión de riesgo resultaba más importante. Se asignaron los miembros del equipo a cada una de dichas áreas para que se informaran al máximo nivel posible sobre las políticas, los procesos y las herramientas que se utilizaban en el área específica para la ERM, lo cual les brindó el contexto para el diseño y la implementación del programa de auditoría.

Los auditores apuntan a brindar un aseguramiento razonable de que las prácticas de negocio de la organización no tienen fallas y son sustentables, y que reciben la información de riesgo que ayuda a la organización a responder eficazmente ante los mismos.

OBJETIVOS Y CRITERIOS Al revisar el enfoque de ERM de la organización, el objetivo del auditor es brindar un aseguramiento razonable respecto de que sus prácticas de negocio no tienen fallas y son sustentables, y de que reciben la información de riesgo que le ayuda a la organización a responder eficaz y eficientemente. Para desarrollar los objetivos y criterios de la auditoría, los auditores deben realizar lo siguiente:

- Diseñar a medida el enfoque conceptual de gestión de riesgo para que se adecue al entorno de la organización. Por ejemplo, si la organización acaba de implementar un programa de gestión de riesgo no es probable que disponga de resultados provenientes del programa de supervisión.
- Alinear los criterios de la auditoría con los cuatro componentes del modelo del enfoque de ERM. Es muy probable que la auditoría de un programa de gestión

Principios que rigen el enfoque de ERM

A pesar de que pueden adoptar formas diferentes, en función de los objetivos de la organización, los enfoques sólidos de ERM incorporan tres principios de guía:

- *Las prácticas de ERM han evolucionado de la misma manera que los objetivos de negocio y del entorno de la organización, incluido su perfil de riesgo. De este modo, el enfoque se adapta bien a las condiciones de negocio, los objetivos y los riesgos que caracterizan a la organización.*
- *Las prácticas de ERM se entrelazan para todas las áreas relevantes de la organización, incluidas las políticas y guías, y cuentan con el apoyo de herramientas eficaces para la evaluación, comunicación y supervisión de los riesgos.*
- *Las prácticas de ERM de toda la organización se diseñan para multiplicarse entre sí, asegurando que los grupos que participan en las actividades relacionadas con los riesgos trabajen en pos de objetivos comunes. Para alcanzar este nivel de integración, los grupos deben conocer claramente los procesos de gestión de riesgo de cada uno, sus metas y métodos, al igual que las responsabilidades de gestionar el riesgo. La ERM recurre a los sistemas y controles actuales de la organización para apoyar la gestión de riesgo.*

Las organizaciones están cada vez más conscientes del valor que puede generarse a través de la gestión de los riesgos. Resulta imprescindible contar con un enfoque sólido de gestión de riesgo para generar dicho valor.

de riesgo nuevo especifique los criterios de supervisión tomando como base la existencia de una estrategia de supervisión, en lugar de los resultados del programa de supervisión.

- Mantener un punto de vista amplio al prescribir las prácticas de negocio que esperan encontrar para asegurar que la organización tenga la flexibilidad de adaptarse a las condiciones de negocio, y que se tengan en cuenta todas las prácticas diseñadas para gestionar el riesgo.

Además, al inicio de la auditoría, los auditores deben obtener el consentimiento de la dirección sobre los criterios de auditoría. Si la dirección no está de acuerdo con los criterios de comparación seleccionados para realizar las evaluaciones, habrá resistencia a las conclusiones y recomendaciones propuestas por la auditoría.

EJECUCIÓN la realización de las entrevistas relativas a la auditoría de un enfoque de ERM requiere de experiencia y conocimientos acerca de las prácticas generales de gestión debido a que la ERM abarca prácticas comerciales que se relacionan con otras áreas como finanzas, cumplimiento, operaciones y seguridad. Aunque se puede usar una amplia gama de procedimientos, la mayoría de las auditorías recurre a las entrevistas y a la revisión de documentos. La tarea de determinar a quiénes entrevistar, se debe hacer en función de los objetivos de riesgo de la organización. Por ejemplo, si el programa de ERM está diseñado para que sea exhaustivo, los auditores deberán entrevistar a una amplia lista de representantes de toda la organización. Los auditores deben adaptar las preguntas para acceder al cuerpo de conocimientos del entrevistado y reformular la terminología desconocida. Al evaluar la calidad de la información de riesgo de una organización, deben buscar evidencias de que se reduce la inseguridad para la toma de decisiones porque la dirección tiene acceso a datos relevantes y exactos sobre las posibles consecuencias indeseadas, producidas por los eventos que pueden afectar a los objetivos de la organización.

Para realizar una auditoría del enfoque de ERM, los auditores deben:

- *Escuchar a los clientes*. Los auditores deben tomarse el tiempo para conocer los objetivos de negocio de los clientes, su entorno competitivo, exposición al riesgo y tolerancia al riesgo. La auditoría de un enfoque de ERM no consiste en compararlo con una serie de características de control sino en asegurar que este le permitirá a la organización lograr sus objetivos. Por ejemplo, los auditores de Interis ayudaron a la directora financiera de una empresa de software a usar la ERM para asegurar que se le notifique de inmediato cualquier atraso en el cronograma de entrega de proyectos de la empresa. Al recibir esta información de riesgo de forma oportuna, pudo tomar decisiones para compensar la postergación de los ingresos del cliente renunciando a gastos o investigando la posibilidad de acelerar otros proyectos, lo cual permitió que la empresa cumpliera con las expectativas de ingresos trimestrales.
- *Reconocer que los enfoques de erm son tareas siempre en evolución*. Los enfoques cambian según el contexto comercial y la madurez de la organización. Para determinar recomendaciones relevantes, es importante conocer en qué condiciones se encontraba la organización cuando se realizó la última auditoría, cómo está actualmente y hacia dónde se dirige. Por ejemplo, un nuevo departamento de gobierno contaba con un elevado nivel de madurez en la ERM en las áreas operacionales que resultaban cruciales para la empresa, pero tenía un nivel muy bajo de madurez en las áreas de gestión corporativa. Para sus recomendaciones, los auditores de Interis tuvieron presente que el departamento comenzó dos años atrás sin ningún enfoque de ERM; el punto importante que debía tenerse en cuenta era cuánto había avanzado el departamento hacia el logro de un enfoque sólido de ERM y cuáles serían las recomendaciones que le resultarían más útiles para acelerar el progreso en las áreas débiles.
- *Reconocer que puede haber diferentes tipos de ERM*. Algunas organizaciones tienen la ERM integrada a sus sistemas. Por ejemplo, las instituciones financieras normalmente poseen pautas claras para el personal en materia de los puntos de referencia que deben alcanzarse antes de que un cliente califique para obtener un producto o servicio en particular. Otras organizaciones son muy flexibles al momento de permitir que los gerentes tomen decisiones basadas en su propio criterio.
- *Estar alerta para detectar prácticas ocultas de ERM*. La gestión de riesgo no constituye un concepto nuevo, pero las personas que integran la organización no pueden describir sus prácticas de gestión de riesgo en esos términos, especialmente en las organizaciones en las que el enfoque de ERM está en una etapa inicial o es específico para el caso. Auditores experimentados examinan las políticas, las unidades funcionales como recursos humanos y los parámetros operacionales para detectar una ERM integrada. Si los gerentes pueden responder la pregunta: "¿Cómo sabe cuándo debe...?", entonces existe una política o práctica que respalda la ERM. De hecho, las prácticas de gestión de riesgo, que están integradas en todos los aspectos de una organización pueden constituir, incluso, un indicio de la existencia de un enfoque y capacidad avanzados de ERM, en donde la ERM es parte integral del entorno de trabajo a tal punto que los empleados no la diferencian conscientemente en base a términos de riesgo.

Si el enfoque de ERM es sólido y ha sido auditado asegurará que la organización está gestionando el riesgo y puede realizar los ajustes necesarios y oportunos en el proceso de alcanzar sus objetivos.

Para la evaluación de los enfoques de ERM, es importante que los auditores tengan en cuenta que la ERM no debe hacerse porque sí, como un simple ejercicio de cumplimiento. Deben concentrarse en asegurar que se logre su verdadero valor —la capacidad de contribuir a mejorar la toma de decisiones en toda la organización.

PREPARACIÓN DE INFORMES La tarea más difícil durante la auditoría de un enfoque de ERM consiste en arribar a conclusiones y hacer recomendaciones. Después de reunir la información descubierta y de agruparla según cada criterio, el auditor considera hasta qué punto el enfoque de ERM de la organización correspondiente a esa área cumple con sus objetivos. Las recomendaciones de la auditoría deben ser razonables y alcanzables, teniendo en cuenta el perfil de riesgo y los objetivos de la organización.

Al momento de confeccionar el informe de auditoría, los auditores deben describir explícita y exhaustivamente lo que encontraron

como contexto de la organización, de manera que quienes lo lean tengan los fundamentos para poder interpretar los resultados. Deben incluir una descripción breve de la información relevante acerca del entorno junto con cada una de las recomendaciones para que estén siempre relacionadas con el perfil de riesgo y los objetivos de la organización. De esta manera, el informe servirá de punto de referencia del estado actual del enfoque de ERM de la organización, y brindará una herramienta útil para la implementación de las recomendaciones.

LA BÚSQUEDA DEL EQUILIBRIO

Si el enfoque de ERM es sólido y ha sido auditado asegurará que la organización está gestionando el riesgo y puede realizar los ajustes necesarios y oportunos en el proceso de alcanzar sus objetivos. También puede proporcionar una base sólida para la toma de las decisiones de negocio. Debido a que las auditorías de la ERM deben adaptarse a enfoques de naturaleza diferente, puede resultar útil disponer de un conjunto de las mejores prácticas para evaluar la ERM en funcionamiento. En última instancia, el futuro de la ERM es integrar los enfoques de ERM a las funciones cotidianas. Durante el proceso, los auditores desempeñan un papel valioso para ayudar a su organización a desarrollar un enfoque que se adecue a sus necesidades.

Para comentar acerca de este artículo, envíe un mensaje de correo electrónico al autor a alexandra.psica@theiia.org.

El presente artículo de Internal Auditor, edición de abril de 2008, publicado por el Instituto de Auditores Internos, se public con el permiso del editor. El artículo se tradujo del inglés a español.