

29 de septiembre de 2004

El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa

De forma conjunta con el recientemente publicado “Enfoque Integrado de Gestión de Riesgo Empresarial” del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), el Instituto de Auditores Internos (IIA), en coordinación con su organización afiliada IAI-Reino Unido e Irlanda, ha emitido una declaración de posición acerca de “*El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa*”. El propósito de la declaración es ayudar a los directores ejecutivos de auditoría (DEA) a resolver los problemas relacionados con la gestión de riesgo empresarial (ERM, en inglés) en sus organizaciones. Dicha declaración sugiere maneras para que los auditores internos mantengan la objetividad e independencia exigidas por las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna del IIA (las Normas)* al prestar servicios de aseguramiento y consultoría

El rol principal de la auditoría interna con respecto a ERM es proporcionar aseguramiento objetivo al consejo de administración respecto de la eficacia de las actividades de ERM de una empresa, para ayudar a garantizar que los riesgos clave del negocio se están gestionando correctamente y que el sistema de control interno está funcionando eficazmente.

Roles recomendados

Los factores principales que los DEA deben tener en cuenta al establecer el rol de la auditoría interna consisten en determinar si la actividad amenaza de alguna manera la independencia y objetividad del auditor interno, y si existe la posibilidad de mejorar los procesos de gestión de riesgos, control y gobierno de la organización. La declaración de posición del IIA indica cuáles son los roles que debe, y que no debe, desempeñar la auditoría interna durante todo el proceso de ERM.

Principales roles de la auditoría interna en relación con ERM.

- Otorgar aseguramiento respecto de los procesos de gestión de riesgos.
- Otorgar aseguramiento respecto de la evaluación correcta de los riesgos.
- Evaluar los procesos de gestión de riesgos.
- Evaluar la elaboración de informes sobre los riesgos clave.
- Revisar la gestión de riesgos clave.

Roles legítimos de la auditoría interna con resguardos.

- Facilitar la identificación y evaluación de riesgos.
- Asesorar a la dirección para responder a los riesgos.

Coordinar actividades de ERM.
Consolidar la elaboración de informes sobre riesgos.
Mantener y desarrollar el enfoque de ERM.
Defender el establecimiento de ERM.
Desarrollar la estrategia de gestión de riesgos para la aprobación por parte del consejo.

Roles que la auditoría interna NO debe desempeñar.

- Definir el grado de aceptación de riesgo.
- Imponer procesos de gestión de riesgos.
- Tener a su cargo la reponsabilidad sobre la gestión de riesgos.
- Tomar decisiones sobre las respuestas a riesgos.
- Implementar respuestas para los riesgos en nombre de la dirección.
- Responsabilidad por la gestión de riesgos.

El Instituto hace hincapié en que las organizaciones deben comprender plenamente que la dirección sigue siendo responsable de la gestión de riesgos. Los auditores internos deben asesorar, cuestionar o respaldar las decisiones de la dirección respecto a riesgos; pero no tomar ellos mismos tales decisiones. La naturaleza de las responsabilidades de la función de auditoría interna se debe documentar en el estatuto de auditoría y debe ser aprobada por el comité de auditoría.

Por último, adjuntamos el documento *“El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa”*.

El IIA, fundado en 1941, presta sus servicios a aproximadamente 95.000 socios en materia de auditoría interna, gobierno, control interno, auditoría de TI, formación y seguridad en todo el mundo. El Instituto es autoridad reconocida, principal formador y líder reputado en cuanto a certificaciones, investigaciones y orientaciones tecnológicas de la profesión en todo el mundo.

Introducción

A lo largo de los últimos años se ha tomado conciencia de la importancia que reviste la gestión de riesgos para un gobierno corporativo fuerte. Las organizaciones se sienten bajo presión y deben identificar todos los riesgos de negocio que enfrentan: sociales, éticos, ambientales, financieros y operativos; además de explicar cómo los gestionan para lograr un nivel aceptable. Mientras tanto, se ha extendido el uso de los enfoques de gestión de riesgos para toda la empresa a medida que las organizaciones reconocen sus ventajas sobre los enfoques de gestión de riesgos menos coordinados.

La auditoría interna, tanto en su rol de aseguramiento como de consultoría, contribuye de distinta manera a la gestión de riesgos. En 2002 el Instituto de Auditores Internos del Reino Unido e Irlanda emitió una declaración de posición sobre “El rol de la auditoría interna en relación con la gestión de riesgos” para guiar a sus socios en cuanto a los roles permitidos y los resguardos necesarios para proteger la independencia y objetividad de la auditoría interna. Esta nueva declaración de posición revisada reemplaza a la anterior y tiene en cuenta los avances recientes procedentes de todo el mundo en el campo de la gestión de riesgos y de la auditoría interna.

¿En qué consiste la gestión de riesgos para toda la empresa?

Las personas llevan a cabo actividades de gestión de riesgos para identificar, evaluar, gestionar y controlar todo tipo de eventos o situaciones. Estos pueden variar abarcando desde tipos de riesgo para proyectos únicos o estrictamente definidos, como por ejemplo, los riesgos de mercado, hasta amenazas y oportunidades que debe afrontar la organización como una sola unidad. Los principios presentados en esa declaración de posición se pueden utilizar para guiar la participación de la auditoría interna en todo tipo de gestión de riesgos, pero nos interesa especialmente la gestión de riesgos para toda la empresa porque es probable que esta última mejore los procesos de gobierno de la organización.

La **gestión de riesgos para toda la empresa** es un proceso estructurado, coherente y continuo que abarca a toda la organización para identificar, evaluar, afrontar e informar las oportunidades y amenazas que afectan el logro de sus objetivos.

Responsabilidad por ERM

El consejo de administración tiene la responsabilidad general de asegurar que se gestionen los riesgos. En la práctica, el consejo delega la operación del enfoque de gestión de riesgos al equipo de dirección, el cual será responsable de llevar a cabo las actividades incluidas a continuación. Puede existir una función separada que coordine y dirija estas actividades, a la vez que centra su atención en habilidades y conocimientos de especialista.

Todos los miembros de la organización desempeñan un rol para el aseguramiento de una gestión de riesgo empresarial exitosa pero la responsabilidad primordial de identificar los riesgos y gestionarlos recae en la dirección.

Ventajas de ERM

La ERM puede realizar una gran contribución para ayudar a la organización a gestionar los riesgos para el logro de sus objetivos. Las ventajas incluyen:

- Mayor probabilidad de lograr dichos objetivos
- Información consolidada de riesgos dispares en el ámbito del consejo de administración
- Mayor comprensión de los riesgos clave y sus implicancias más amplias
- Identificación e intercambio de conocimientos sobre riesgos de negocio cruzados
- Mayor atención de la dirección a los problemas realmente importantes
- Menos sorpresas o crisis
- Mayor atención internamente para hacer lo correcto de la manera correcta
- Mayor probabilidad de que se logren las iniciativas de cambio
- Capacidad para asumir mayores riesgos en pos de mayores recompensas
- Asunción de riesgos y toma de decisiones más informadas

Actividades incluidas en ERM

- Expresar y comunicar los objetivos de la organización
- Determinar el grado de aceptación de riesgos de la organización
- Establecer un entorno interno adecuado, que incluya un enfoque de gestión de riesgos
- Identificar las amenazas potenciales para el logro de los objetivos
- Evaluar el riesgo, es decir, el impacto de las amenazas y la probabilidad de que se produzcan
- Seleccionar e implementar respuestas ante los riesgos
- Tomar el control y llevar a cabo otras actividades de respuesta
- Comunicar la información sobre riesgos de manera coherente en todos los niveles de la organización
- Supervisar y coordinar de forma central los procesos de gestión de riesgos y sus resultados
- Brindar aseguramiento sobre la eficacia con que se gestionan los riesgos

Declaración de posición

El rol de la auditoría interna en la gestión de riesgos para toda la empresa

Brindar aseguramiento de ERM

Una de las exigencias claves del consejo de administración u organismo equivalente es obtener el aseguramiento de que los procesos de gestión de riesgos funcionan eficazmente y que los riesgos principales se gestionan para lograr un nivel aceptable.

Es probable que el aseguramiento se obtenga a partir de fuentes diferentes. Entre ellas, el aseguramiento proveniente de la dirección es fundamental. Debe complementarse mediante la provisión de aseguramiento objetivo, para el cual la auditoría interna es una fuente clave. Otras fuentes incluyen la auditoría externa y las revisiones realizadas por especialistas independientes. La auditoría interna normalmente brinda aseguramiento en tres áreas:

- Procesos de gestión de riesgo, en cuanto a su diseño como a su correcto funcionamiento
- Gestión de aquellos riesgos clasificados como “clave”, incluidos la eficacia de los controles y otras respuestas a esos riesgos
- Evaluación confiable y adecuada de los riesgos e información del estado de los riesgos y del control

El rol de la auditoría interna en ERM

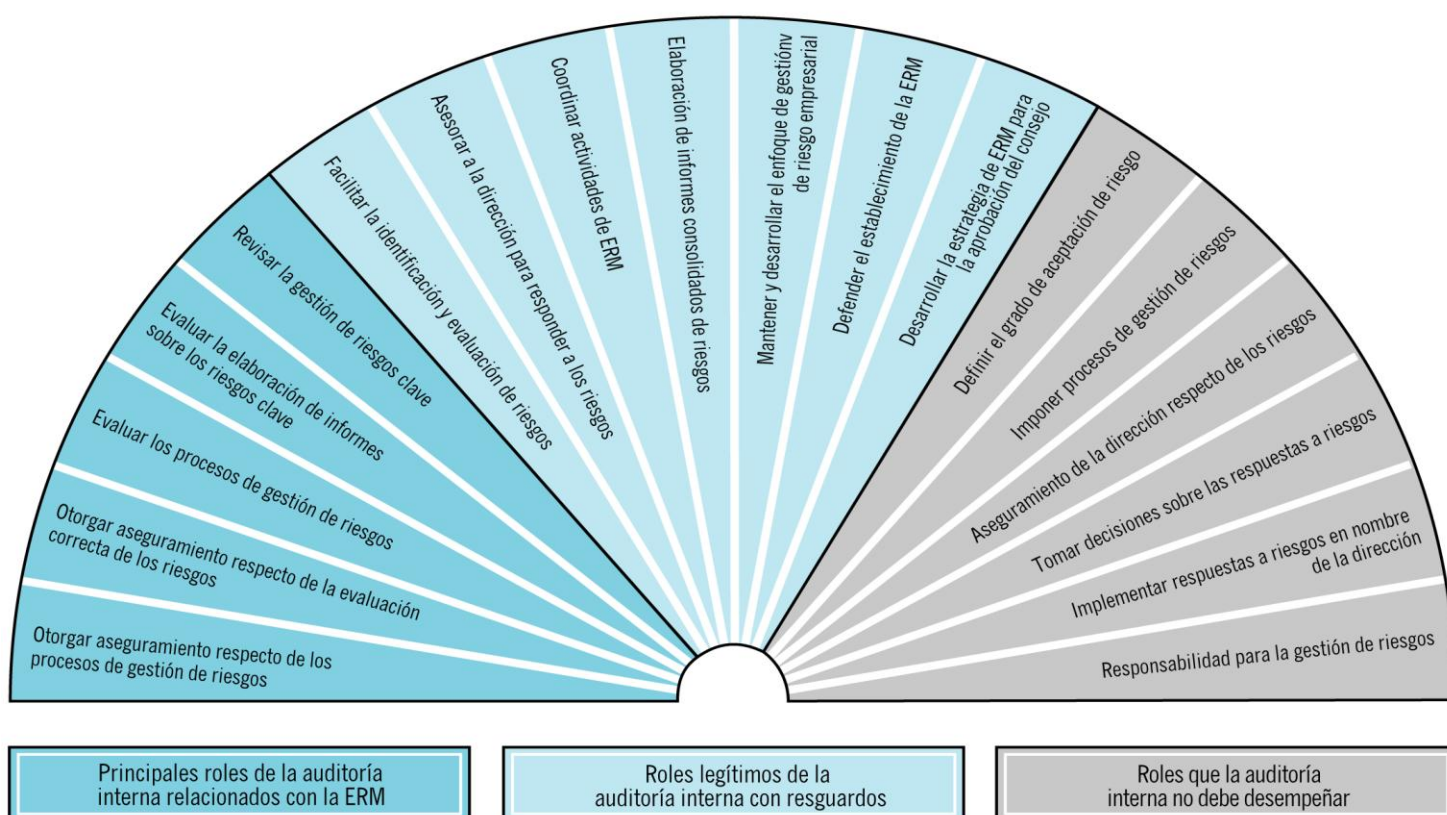
La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta. Su rol fundamental respecto de ERM es brindar un aseguramiento objetivo al consejo de administración en cuanto a la eficacia de la gestión de riesgo. En efecto, la investigación ha demostrado que los directores que forman el consejo de administración y los auditores internos coinciden en que las dos maneras más importantes a través de las cuales la auditoría interna agrega valor a la organización son brindando aseguramiento objetivo de que los principales riesgos de negocio se gestionan apropiadamente y de que el enfoque de gestión de riesgo y control interno funciona eficazmente.(1)

En la *Figura 1* se presenta una variedad de actividades de gestión de riesgo empresarial y se indica cuáles son los roles que debe desempeñar una función de auditoría interna profesional y, lo que es igualmente importante, cuáles son los roles que no debe llevar a cabo. Los factores principales a tener en cuenta para determinar el rol de la auditoría interna se basan en evaluar si la actividad amenaza de alguna manera la independencia y objetividad de la función de auditoría interna, y si es probable mejorar los procesos de gestión de riesgos, control y gobierno de la organización.

Figura 1: Rol de la auditoría interna en ERM

Las actividades de la izquierda de la *Figura 1* son todas de aseguramiento. Forman parte del objetivo más amplio de otorgar aseguramiento sobre la gestión de riesgos. La función de auditoría interna que responde a las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna* puede y debe realizar como mínimo algunas de esas actividades.

La auditoría interna puede prestar servicios de consultoría que mejoren los procesos de gobierno, gestión de riesgos y control de la organización. El alcance de las actividades de consultoría de la auditoría interna en relación con ERM depende de los otros recursos, internos y externos, que estén disponibles para el consejo de administración, y de la madurez de riesgos de la organización(2), y es probable que varíe con el paso del tiempo. La competencia experta de la función de auditoría interna para considerar los riesgos, comprender las conexiones entre riesgos y gobierno, y en cuanto a facilitación significa que está bien calificada para actuar como líder e incluso como director de proyecto de ERM, especialmente en las primeras etapas de su introducción. A medida que se incrementa la madurez de riesgo de la organización y que la gestión de riesgos se integra más con las operaciones del negocio, es probable que el rol de la auditoría interna en cuanto a defensa de ERM se reduzca. De manera similar, si una organización contrata los servicios de un especialista en gestión de riesgo, es más probable que la auditoría interna agregue valor concentrándose en su rol de aseguramiento que llevando a cabo actividades más relacionadas con la consultoría. No obstante, si la auditoría interna aún no ha adoptado el enfoque basado en el riesgo representado por las actividades de aseguramiento que se incluyen a la izquierda de la *Figura 1*, es poco probable que esté equipada como para asumir las actividades de



consultoría del centro del diagrama.

Roles de consultoría

En el centro de la *Figura 1*, se presentan los roles de consultoría que la auditoría interna puede desempeñar en relación con ERM. En general cuanto más se acerca la auditoría interna hacia la derecha del dial, mayores son los resguardos que se exigen para asegurar que se mantenga su independencia y objetividad. Algunos de los roles de consultoría que puede desempeñar la auditoría interna son:

- Poner a disposición de la dirección las herramientas y técnicas utilizadas por la auditoría interna para analizar riesgos y controles
- Ser un defensor de ERM al introducirla en la organización, aprovechando su competencia experta en relación con la gestión y control de riesgos, y su conocimiento general de la organización
- Brindar asesoramiento, facilitar talleres, capacitar a la organización en materia de riesgos y control, y promover el desarrollo de un lenguaje, enfoque y entendimiento comunes
- Actuar como el punto central para coordinar, supervisar e informar riesgos
- Apoyar a los gerentes en su trabajo de identificar la mejor manera de mitigar un riesgo

El factor clave para decidir si los servicios de consultoría son compatibles con el rol de aseguramiento consiste en determinar si el auditor interno asume algún tipo de responsabilidad de dirección. En el caso de ERM, la auditoría interna puede prestar servicios de consultoría siempre que no desempeñe ningún rol en la gestión efectiva de riesgos —esa es responsabilidad de la dirección— y que la alta dirección respalde y apoye activamente la ERM. Recomendamos que, cuando la auditoría interna actúe para ayudar al equipo de dirección a implementar o mejorar los procesos de gestión de riesgos, su plan de trabajo incluya una estrategia y una línea cronológica claras para transferir la responsabilidad por estas actividades a los miembros del equipo de dirección.

Resguardos

La auditoría interna puede ampliar su participación en ERM como se indica en la *Figura 1*, siempre que se den determinadas condiciones. Dichas condiciones son:

- Debe quedar claro que la dirección sigue siendo responsable de la gestión de riesgos.
- La naturaleza de las responsabilidades de la función de auditoría interna se debe documentar en el estatuto de auditoría y esto debe ser aprobado por el comité de auditoría.(3)
- La auditoría interna no debe gestionar ningún riesgo en nombre de la dirección.

- La función de auditoría interna debe asesorar, cuestionar y respaldar la toma de decisiones de la dirección, pero no debe tomar ella misma decisiones de gestión de riesgos.
- La auditoría interna tampoco puede brindar aseguramiento objetivo respecto de ninguna parte del enfoque de ERM del cual sea responsable. Dicho aseguramiento debe ser prestado por otros terceros interesados que estén debidamente calificados.(4)
- Todo trabajo que exceda las actividades de aseguramiento se debe reconocer como un trabajo de consultoría y se deben respetar las normas de implementación relacionadas con esos trabajos.(5)

Habilidades y cuerpo de conocimiento

Los auditores internos y los gerentes de riesgos comparten ciertos conocimientos, habilidades y valores. Ambos, por ejemplo, comprenden las exigencias del gobierno corporativo, poseen habilidades de dirección de proyecto, análisis y facilitación, y valoran un grado equilibrado saludable de aceptación de riesgos, en lugar de asumir o evitar riesgos de modo extremo. Sin embargo, los gerentes de riesgos como tales prestan servicios sólo a la dirección de la organización y no tienen que brindar un aseguramiento independiente y objetivo al comité de auditoría. Y los auditores internos que desean ampliar su rol en relación con ERM tampoco deben subestimar las áreas de conocimiento especializado de los gerentes de riesgos (como la transferencia de riesgos y las técnicas de cuantificación y generación de modelos de riesgo) que no están incluidas en el cuerpo de conocimiento de la mayoría de los auditores internos. Los auditores internos que no pueden demostrar las habilidades y los conocimientos adecuados no deben llevar a cabo trabajos en el área de la gestión de riesgos. Es más, el director de auditoría interna no debe prestar servicios de consultoría en dicha área si no se cuentan con habilidades y conocimientos adecuados dentro de la función de auditoría interna y estos no se pueden obtener de ninguna otra fuente.⁶

Conclusión

La gestión de riesgos es un componente fundamental del gobierno corporativo. La dirección es responsable de establecer y operar el enfoque de gestión de riesgos en nombre del consejo de administración. La gestión de riesgos para toda la empresa aporta muchos beneficios como resultado de su enfoque estructurado, coherente y coordinado. El rol principal de la auditoría interna en relación con ERM debe ser brindar aseguramiento a la dirección y al consejo de administración en cuanto a la eficacia de la gestión de riesgos. Cuando la auditoría interna amplía sus actividades más allá de ese rol fundamental, debe aplicar determinados resguardos, incluso tratar los trabajos como servicios de consultoría, y aplicar así todas las *Normas* relevantes. De esta manera, la auditoría interna protege su independencia y la objetividad de sus servicios de aseguramiento. Con estas restricciones, ERM puede ayudar a elevar el perfil y a incrementar la eficacia de la auditoría interna.

Glosario de términos

Servicios de aseguramiento: Inspección objetiva de la evidencia con el fin de proporcionar una evaluación independiente de los procesos de gestión de riesgos, control o gobierno de la organización. Como ejemplo se pueden incluir los trabajos financieros, de desempeño, cumplimiento, seguridad de sistemas y diligencia debida.

Consejo de administración (consejo): Es el órgano de gobierno de una organización, como el consejo de administración, el consejo de supervisión, director de un organismo o cuerpo legislativo, consejo de gobierno o miembros de la dirección de instituciones no lucrativas.

Defensor: Es alguien que apoya y defiende a una persona o causa. Por lo tanto, un defensor de la gestión de riesgos promocionará sus beneficios, educará a la dirección y al personal de la organización en las acciones que deben tomar para implementarla, los alentará y apoyará cuando tomen dichas medidas.

Servicios de consultoría: Incluyen las actividades de asesoramiento y los servicios relacionados para clientes, cuya naturaleza y alcance se acuerdan con el cliente, se diseñan para agregar valor y mejorar los procesos de gobierno, gestión de riesgos y control de la organización sin que el auditor interno asuma responsabilidades por la gestión. Como ejemplos se pueden mencionar consultoría, asesoramiento, facilitación y capacitación.

Control : Todas las acciones tomadas por la dirección, el consejo de administración y demás partes para gestionar el riesgo y favorecer el logro de los objetivos y metas establecidos. La dirección planifica, organiza y dirige la realización de acciones suficientes para brindar una seguridad razonable de que se lograrán los objetivos y las metas.

Empresa: Toda organización establecida para lograr un conjunto de objetivos.

Gestión de Riesgo Empresarial (ERM): La Gestión de riesgos para toda la empresa es un proceso estructurado, coherente y continuo que abarca a toda la organización para identificar, evaluar, afrontar e informar las oportunidades y amenazas que afectan el logro de sus objetivos.

Facilitación: Trabajar con un grupo (o individuo) para facilitarle a ese grupo (o individuo) el logro de los objetivos acordados por el grupo para la reunión o la actividad. Para esto se requiere escuchar, desafiar, observar, cuestionar y apoyar al grupo y a sus miembros. No incluye hacer el trabajo ni tomar decisiones.

Riesgo: La posibilidad de que se produzca un evento que tendrá un impacto en el logro de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

Grado de aceptación del riesgo: Es el nivel de riesgo aceptable para el consejo de administración o la dirección. Puede fijarse en relación con la organización como un todo, para los diferentes grupos de riesgos o en un nivel de riesgo individual.

Enfoque de gestión de riesgos: La totalidad de las estructuras, metodología, procedimientos y definiciones elegidos por una organización para la implementación de sus procesos de gestión de riesgos.

Procesos de gestión de riesgos: Procesos para identificar, evaluar, gestionar y controlar eventos o situaciones potenciales, con el fin de brindar un nivel de seguridad razonable respecto del logro de los objetivos de la organización.

Madurez del riesgo: Indica hasta qué grado la dirección ha adoptado y aplicado un enfoque de gestión de riesgos sólido en toda la organización, según lo planificado, para identificar, evaluar, decidir sobre las respuesta e informar las oportunidades y amenazas que afectan el logro de los objetivos de la organización.

Respuestas a los riesgos: Medios mediante los cuales una organización elige gestionar los riesgos individuales. Las categorías principales son tolerar el riesgo, tratarlo mediante la reducción de su impacto o probabilidad, transferirlo a otra organización o terminar con la actividad que lo genera. Los controles internos constituyen una manera de tratar los riesgos.

Material adicional de lectura

Si desea más información sobre el tema de gestión de riesgos, las siguientes publicaciones pueden resultar de interés:

Publicación y autor

Risk Management: Changing the Internal Auditor's Paradigm
por Georges Selim y David McNamee

IIA Professional Briefing Note 13: Managing Risk

The Complete Guide to Business Risk Management por Kit Sadgrove
Operational Risk and Resilience: Understanding and minimising operational risk to secure shareholder value por PriceWaterhouseCoopers

Risk Management Guide 2001

It's a Risky Business

The Risk Management Standard

AN Z Risk Management Standard

Nueva

Enterprise Risk Management Framework

Risk Management in the Public Services

Independence and Objectivity – Professional Issues Bulletin 2003

Editorial

Fundación de Investigaciones del IIA

IAI-Reino Unido e Irlanda

Gower
Butterworth Heinemann

White Page

CIPFA

IRM, AIRMIC and ALARM

Normas de Australia y Normas de
Zelanda

COSO

CIPFA & ALARM

IAI-Reino Unido e Irlanda

Embedding Risk Management into the Culture of your organisation – Professional Briefing Note 2003	IAI-Reino Unido e Irlanda
Managing business risk – Adam Jolly	IOD, Ernst & Young y Kogan Page
The universe of risk – Pamela Shimell	Pearson Education and FT
Management of risk – OGC	TSO
Enterprise wide risk management – James Deloach	Pearson Education and FT
Risk – John Adams	Routledge
Risk management for company executives – John Smullen	Pearson Education y Financial Times Prentice Hall
Enterprise Risk Management: Trends & Emerging Practices – Miccolis, Hively y Merkley	Fundación de Investigaciones del IIA
Enterprise Risk Management: Pulling it All Together – Walker, Shenkir y Barton	Fundación de Investigaciones del IIA

El departamento de publicaciones del Instituto lo ayudará a obtener estos libros. Contáctese con publications@iia.org.uk ó llame al teléfono +44 020 78 19 1924

También pueden ser de interés los siguientes sitios Web:

Dirección del sitio Web – Título u organización

- www.iia.org.uk – Instituto de Auditores Internos – Reino Unido e Irlanda
- www.theiia.org - IIA Global
- www.gee.co.uk - Gee Publishing
- www.corpgov.net – Sitio de gobierno corporativo
- www.coso.org – Comité de Organizaciones Patrocinadoras (COSO, en inglés)
- www.theirm.org - The Institute of Risk Management (IRM)
- www.airmic.com - The Association of Insurance and Risk Managers (AIRMIC)
- www.alarm-uk.com - The National Forum for Risk Management in the Public Sector (ALARM)
- www.whitepage.co.uk – Sitio Web de White Page
- www.standards.org.au – Normas de Australia
- www.standards.co.nz – Normas de Nueva Zelanda

Declaración de posición:

El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa

Acerca del Instituto.

Derechos de autor

Los derechos de autor de esta declaración de posición son de posesión conjunta. Para obtener autorización para su reproducción en el Reino Unido o Irlanda, comuníquese con el IAI-Reino Unido e Irlanda. Si desea autorización para su reproducción en otros lugares, contáctese con el Instituto de Auditores Internos en issues@theiia.org.

Acerca de las declaraciones de posición

Las declaraciones de posición son parte de una variedad de guías técnicas y profesionales preparadas por el Instituto para sus socios. Su propósito es dejar en claro la posición política oficial del IAI-Reino Unido e Irlanda en cuanto a los temas importantes y potencialmente complejos que deben afrontar los auditores internos.

Si desea más información sobre otro material de guía del Instituto, visite nuestro sitio Web, www.iaa.org.uk, o envíe un correo electrónico a technical@iaa.org.uk

Descargo de responsabilidades

Este material de guía técnica no tiene el propósito de brindar respuestas definitivas a circunstancias individuales específicas y como tal, sólo tiene el objeto de ser utilizado como guía. El Instituto de Auditores Internos del Reino Unido e Irlanda recomienda que siempre se solicite asesoramiento experto e independiente en relación con cualquier situación específica. El Instituto no acepta responsabilidad alguna por ninguna persona y confía únicamente en esta guía técnica.

www.iaa.org.uk

Institute of Internal Auditors – UK and Ireland Ltd

13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX

Teléfono: +44 020 7498 0101; Fax: +44 020 7978 2492; Dirección de correo electrónico: technical@iaa.org.uk

Inscrito en Inglaterra y Gales, N.º 1 474735

© September 2004

Declaración de posición:

El rol de la auditoría interna en relación con la gestión de riesgos para toda la empresa