Traducción al Español Auspiciada por:

FLAI
Fundación Latinoamericana
de **Auditores Internos**

PERSPECTIVAS Y PERCEPCIONES GLOBALES

Gobernanza, riesgo y control

PARTE I: Repensar el apetito de riesgo desde una perspectiva de riesgo no financiero

PARTE II: Cuantificación del riesgo no financiero

PARTE III: Cómo la transformación digital está transformando la GRC

The Institute of
Internal Auditors

Contenido

Parte 1 Repensar el apetito de riesgo desde una perspectiva de riesgo no financiero

Sobre el Experto

W. Scott Page, CIA, CCSA, CRMA, CPA, CA

Scott es director de auditoría interna en MDA, Ltd. Con sede en Brampton, Ontario, Canadá, MDA proporciona sistemas de geointeligencia, robótica y operaciones espaciales y por satélite. Scott cuenta con más de 20 años de experiencia en defensa y fabricación espacial, servicios profesionales, asistencia sanitaria, servicios de distribución e industrias manufactureras.

Introducción

El concepto de apetito de riesgo — la cantidad de riesgo que una organización está dispuesta a aceptar para alcanzar sus objetivos- es fundamental para una gobernanza eficaz en todas las organizaciones. Históricamente, las decisiones sobre el apetito de riesgo de una empresa se regían principalmente por consideraciones de riesgo financiero. Sin embargo, esto está cambiando debido a la creciente atención que se presta a los riesgos no financieros, incluidos los riesgos medioambientales, sociales y de gobernanza (ASG) y las consideraciones reglamentarias y de información conexas. Cada vez se presta más atención a los riesgos asociados a la forma en que las organizaciones operan en relación con el mundo que las rodea.

La evaluación de estos riesgos como parte del apetito de riesgo es un área en la que los auditores internos pueden hacer contribuciones significativas. Este Informe Global de Conocimiento (Global Knowledge Brief), el primero de una serie de tres partes sobre gobierno, riesgo y control (GRC) del IIA, examina en detalle este tema, los retos de replantear el apetito de riesgo teniendo en cuenta el riesgo no financiero, y el importante papel de la auditoría interna en el proceso.

El Apetito de Riesgo

El equilibrio entre amenazas y oportunidades

Los perfiles de riesgo influyen en el apetito

Marco Internacional de Práctica Profesional del IIA The IIA's define el apetito de riesgo simplemente como "El nivel de riesgo que una organización está dispuesta a aceptar". En la práctica, el apetito de riesgo, también referido como tolerancia al riesgo, representa un equilibrio entre los beneficios potenciales de la innovación y las amenazas que el cambio inevitablemente conlleva. Como tal, el apetito de riesgo es único para cada organización y varía en función de una serie de factores, tales como:

Cultura — Basándose en directrices, actitudes u otros factores arraigados, la organización puede ser más o menos agresiva en su enfoque del riesgo.

Industria — El grado de regulación u otros problemas de cumplimiento, por ejemplo, pueden influir en su aversión al riesgo.

Mercado — El nivel de competencia al que se enfrenta una empresa o la estabilidad de su mercado son factores que pueden afectar a la toma de decisiones sobre el riesgo.

Fortaleza financiera— Una empresa que confía menos en su situación financiera puede ser más aversa al riesgo[1].

¿Qué es el riesgo no financiero?

La incorporación del riesgo no financiero a los debates sobre el apetito de riesgo empieza por comprender lo que puede abarcar. De hecho, el gran número de riesgos que se incluyen en esta categoría (véase la lista relacionada) aumenta las posibilidades de que algunos se pasen por alto o se malinterpreten, lo que subraya la importancia de incorporar los riesgos no financieros a cualquier debate sobre el apetito de riesgo. Más allá de la simple incorporación, sin embargo, las organizaciones también deben estar preparadas para actuar sobre estos elementos no financieros, identificando la información necesaria para abordar el riesgo dentro de los diferentes procesos de negocio a nivel corporativo,

RIESGOS NO FINANCIEROS (lista parcial)

- Operacional
- Conformidad
- Estratégico
- Terceros
- Ciberseguridad
- Responsabilidad social
- Reputación
- Protección de datos
- Integridad de los datos
- Protección de la propiedad intelectual
- Compensación
- Conducta de los empleados
- Cultura ética y empresarial
- Salud pública
- Diversidad, igualdad e inclusión
- Derechos humanos
- Recursos humanos
- Medioambiental:
  - Emisiones de gases de efecto invernadero
  - Gestión de residuos
  - Abastecimiento de materias primas
  - Acceso/gestión de los recursos naturales
  - Cambio climático

[1] Jean-Gregoire Manoukian, "Risk Appetite and Risk Tolerance: What's the Difference?", Wolters Kluwer, September 29, 2016, https://www.wolterskluwer.com/en/expert-insights/risk-appetite-and-risk-tolerance-whats-the-difference#:~:text=Risk%20Appetite%20Is%20the%20General%20Level%20of%20Risk%20You%20Accept&text=Because%20determining%20risk%20appetite%20will,risk%20you%20need%20to%20manage.

Retos relacionados con la información sobre riesgos no financieros

Preparación de Reportes

Más del 60% de los CAE de organizaciones que cotizan en bolsa consideraron que los niveles de riesgo de los informes de sostenibilidad/no financieros eran moderados, altos o muy altos, según el Pulso Norteamericano de Auditoría Interna 2023 del IIA. [2] De hecho, muchas empresas están trabajando para medir e informar sobre cuestiones de sostenibilidad/no financieras. Por ejemplo, el 96% de las empresas que cotizan en el índice S&P 500 y el 81% de las que cotizan en el Russell 1000 publican informes de sostenibilidad. [3]

Un reto para las organizaciones en este ámbito es que muchos riesgos no financieros son difíciles de medir. Algunos ejemplos son la inclusión, el comportamiento ético, la cultura corporativa y el impacto medioambiental de las acciones emprendidas por la empresa y sus proveedores y socios comerciales. [4] Una preocupación conexa se refiere a las posibles consecuencias si las organizaciones se basan en indicadores o marcos incorrectos o engañosos para agregar o comunicar información no financiera.

En la actualidad no existen normas definitivas y aceptadas en todo el mundo sobre información y divulgación no financiera, lo que puede dar lugar a una falta de coherencia y comparabilidad de la información. En su lugar, las organizaciones suelen tener la oportunidad de elegir un conjunto de directrices, reunir diferentes directrices u optar por no informar completamente en función de sus necesidades. De hecho, el Center for Sustainable Organizations (Centro de Organizaciones Sostenibles) ha elaborado una lista de 23 normas y marcos de medición y elaboración de informes no financieros que abordan una gran variedad de grupos de interés, conceptos de rendimiento y formatos de medición primarios. [5]

Sin embargo, se vislumbra en el horizonte un conjunto de normas de información de aceptación más general. Un avance importante ha sido la creación del Consejo de Normas Internacionales de Sostenibilidad (ISSB) por parte de la Fundación de Normas Internacionales de Información Financiera (IFRS). El ISSB consolida la Fundación para la Información sobre Valores y el Consejo de Normas de Divulgación sobre el Clima, y ha asumido la responsabilidad del Marco Integrado de Información, todo ello como parte de un esfuerzo por crear una base global de divulgación de la sostenibilidad para los mercados de capitales. Su objetivo es satisfacer la demanda de informes de alta calidad, transparentes, fiables y comparables de las empresas sobre el clima y otras cuestiones ASG. La ISSB anunció que sus normas iniciales sobre información climática y de sostenibilidad se publicarán hacia finales del segundo trimestre de 2023.

Regulatorio

Según el Consejo Empresarial Mundial para el Desarrollo Sostenible (WBCSD), en la actualidad existen más de 2.000 requisitos y recursos obligatorios y voluntarios de información ASG en más de 70 países. Esto por sí solo supone un enorme reto para las organizaciones que intentan comprender la información no financiera obligatoria y voluntaria y los riesgos relacionados.

La Unión Europea (UE) ha tomado la iniciativa en materia de divulgación obligatoria de riesgos no financieros. Desde 2014, la Directiva sobre información no financiera (NFRD) exige a las grandes empresas de interés público con sede en la UE y más de 500 empleados (aproximadamente 11.700) que publiquen información relacionada con cuestiones medioambientales, sociales, de trato a los empleados, de respeto de los derechos humanos, de lucha contra la corrupción y el soborno, y de diversidad en los consejos de administración de las empresas (en términos de edad, sexo, educación y formación profesional), entre otras cuestiones.

---

2. *2023 North American Pulse of Internal Audit*, The IIA, 2023, https://www.theiia.org/globalassets/site/content/research/pulse/2023/2023-Pulse-of-Internal-Audit.pdf.
3. *2022 S&P 500 and Russell 1000 Sustainability Reporting in Focus*, Governance & Accountability Institute Inc., 2022, https://www.ga-institute.com/research/ga-research-directory/sustainability-reporting-trends/2022-sustainability-reporting-in-focus.html#:~:text=All%2DTime%20High%20of%20Sustainability,and%2081%25%20of%20Russell%201000.
4. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA,, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.
5. "Non-Financial Measurement & Reporting Standards & Frameworks," Center for Sustainable Organizations, 2023, https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf.

En enero de 2023 entró en vigor la Directiva de la UE sobre Informes de Sostenibilidad Corporativa (CSRD). Actualiza las normas de información social y medioambiental de la NFRD y amplía el número de empresas obligadas a informar (aproximadamente 50.000). Las empresas tendrán que aplicar las nuevas normas por primera vez en el ejercicio 2024 para los informes que se publiquen en 2025. Hasta entonces, se aplicarán las normas de información de la NFRD.[6]

En Estados Unidos, la Comisión del Mercado de Valores (SEC) ha propuesto exigir a los solicitantes de registro que incluyan información específica sobre el clima y la ciberseguridad en sus declaraciones de registro e informes periódicos. Se espera que la SEC anuncie normas definitivas en estas dos áreas en 2023. Aunque están exentas de cualquier requisito de la SEC, las empresas privadas también pueden sentirse presionadas por las partes interesadas para que divulguen información similar.

Lavado Verde (Greenwashing)

Además de la falta de comparabilidad y transparencia en la información, la fiabilidad puede convertirse en un problema cuando las empresas utilizan supuestos demasiado optimistas para establecer objetivos o cuando tergiversan los datos para presentar una imagen más positiva. En Europa, las autoridades nacionales de protección del consumidor encontraron motivos para creer que el 42% de las afirmaciones ecológicas de las empresas eran exageradas, falsas o engañosas. Estas prácticas, conocidas como "lavado verde", pueden dañar la reputación de las organizaciones. El impacto resultante en la satisfacción de los clientes con una empresa y sus productos o servicios puede influir en los beneficios por acción y el rendimiento de la inversión.[7]

42

PORCENTAJE DE DECLARACIONES ECOLÓGICAS DE LAS EMPRESAS QUE SE CONSIDERAN EXAGERADAS, FALSAS O ENGAÑOSAS.

Fuente: Harvard Business Review, *"How Greenwashing Affects the Bottom Line"*

Además, según el IIA, "sin una estrategia razonada de gestión de riesgos ASG basada en una comprensión clara de los problemas, los informes de sostenibilidad mal elaborados pueden incumplir rápidamente la normativa y desviarse de las expectativas de los inversores."[8]

Las empresas que se enfrentan por primera vez a los datos no financieros tendrán que desarrollar nuevos indicadores clave de rendimiento y otras métricas, junto con políticas, procesos y medidas de control interno adecuados para generar información fiable para la toma de decisiones y garantizar la calidad de los datos que se producen y comunican.

6. "Corporate Sustainability Reporting," European Commission, accessed March 2023, https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en.
7. Ioannis Ioannou, George Kassinis, and Giorgos Papagiannakis, "How Greenwashing Affects the Bottom Line," July 21, 2022, Harvard Business Review, https://hbr.org/2022/07/how-greenwashing-affects-the-bottom-line.
8. *Internal Audit's Role in ESG Reporting: Independent Assurance Is Critical to Effective Sustainability Reporting*, The IIA, May 2021, https://www.theiia.org/globalassets/documents/communications/2021/june/white-paper-internal-audits-role-in-esg-reporting.pdf.

Función de la Auditoría Interna

Servicios de garantía y asesoramiento

Consideración de los riesgos no financieros en la planificación de la auditoría

Los auditores internos planifican sus auditorías basándose en los apetitos de riesgo de la organización en su conjunto y de las áreas auditadas. A menudo se asigna a la auditoría interna la responsabilidad de proporcionar una garantía independiente sobre la eficacia del marco de apetito de riesgo de una organización. El creciente enfoque regulatorio y de las partes interesadas en la sostenibilidad y otras cuestiones no financieras exige que los líderes de auditoría interna consideren los riesgos relacionados que pueden representar una amenaza para la organización, incluyendo la comprensión de cómo encajan en las actividades y estrategias de la empresa y saber qué departamentos tienen la supervisión de las prácticas relacionadas. Los responsables de auditoría interna también deben sensibilizar a los consejos de administración y a la dirección ejecutiva sobre los riesgos no financieros.

Una función clave de la auditoría interna será determinar un entorno de control adecuado para los riesgos no financieros que pueda supervisar las medidas pertinentes y evitar que una organización presente información no válida y engañosa debido a controles y sistemas mal diseñados. Las funciones de auditoría interna competentes cuentan con las competencias y la experiencia necesarias para respaldar entornos de control no financiero eficaces, incluidos servicios de formación y asesoramiento. La auditoría interna puede asesorar sobre los marcos o normas que la organización puede utilizar para gestionar, mitigar y, posiblemente, informar sobre los riesgos no financieros. La auditoría interna también puede ofrecer asesoramiento sobre las métricas de información más útiles, incluidos los nuevos indicadores diseñados para capturar datos cuantitativos y cualitativos que representen con precisión los riesgos no financieros.

Los datos sugieren que la sostenibilidad y las consideraciones no financieras se están abriendo paso lentamente en la rutina de la auditoría interna. Según el informe Pulse, el 22% de los encuestados afirma incorporar consideraciones de sostenibilidad en sus auditorías en general. Sin embargo, las auditorías específicas de sostenibilidad/información no financiera representaron un escaso 2% de la asignación de planes de auditoría.[9]

El valor de un enfoque centralizado: la experiencia de una empresa

Establecer las bases adecuadas es un factor importante para incorporar los riesgos no financieros a la propensión al riesgo.

Cuando Scott Page se incorporó a MDA, Ltd. como director de auditoría interna, cada área de negocio tenía su propio proceso de gestión de riesgos, pero la empresa estaba interesada en centralizar su enfoque. Para lograr esa centralización, era clave un enfoque holístico e integrado. Para aglutinar la información, la empresa pública con sede en Canadá, que presta servicios de robótica, sistemas por satélite y geointeligencia, adoptó una herramienta informática versátil para el proceso de evaluación. La misma herramienta puede ser utilizada por otros equipos, incluidos los de auditoría interna en las pruebas de control y los de TI en la evaluación de los riesgos cibernéticos y de terceros.

De este modo, la información sobre riesgos y los controles se comparten en toda la empresa. La herramienta reúne información detallada sobre todos los riesgos que pueden repercutir en la estrategia o los objetivos para ver cómo pueden afectar a la capacidad de la empresa para cumplir sus objetivos a corto plazo, así como su plan estratégico a largo plazo. "Queríamos reunir todas las

9. *2023 North American Pulse of Internal Audit*, The IIA.

consideraciones de riesgo en una única fuente de información", afirma Page. "Nos ayuda a entender cómo lo que hacemos se interrelaciona con todo el mundo".

Los riesgos relacionados con los controles internos, los estados financieros, las operaciones, las TI y los terceros ya estaban bien captados con los enfoques actuales. Sin embargo, la organización también ha empezado a considerar los riesgos ESG y otros riesgos no financieros. Utilizar la misma herramienta para consolidar estos riesgos adicionales significa que "siempre se está informado de lo que ocurre en otras áreas", dijo Page.

Aunque identificar, contabilizar y auditar los riesgos no financieros puede ser complicado, el enfoque centralizado de MDA le ha proporcionado un sólido punto de partida. Entre otras cosas, la empresa no quiere separar los ASG en un silo, porque los riesgos no financieros conexos afectan a muchas áreas.

La centralización permite utilizar un lenguaje común comprensible para toda la empresa y las partes interesadas, afirma Page. Él, junto con los responsables del grupo de gestión de riesgos empresariales (ERM), define los riesgos y cómo deben evaluarse en una escala del 1 al 5. La información sobre riesgos puede recopilarse una sola vez y aprovecharse en toda la organización, lo que aumenta la eficacia de la auditoría interna y de otros ámbitos, además de garantizar el control de las versiones. Utilizando ese lenguaje común, la dirección ejecutiva y el consejo de administración pueden entender fácilmente cuándo la auditoría interna u otros equipos designan un riesgo como prioridad máxima - Categoría 5 - frente a una prioridad menos urgente - Categoría 1.

Una consideración permanente es la auditabilidad de la información no financiera, ya que, como se ha comentado anteriormente, no existen normas de información generalmente adoptadas. Hasta que esto cambie, la auditoría interna puede asesorar sobre los controles, procesos e información para los que una organización tendrá que estar preparada.

Cuantificar las cifras es otro reto, porque los datos pueden no estar disponibles y puede ser difícil obtener datos comparables. MDA, por ejemplo, no tiene muchas emisiones de gases de efecto invernadero, una de las preocupaciones más comunes en materia de ASG. Sin embargo, trabaja con muchos proveedores y consultores externos, y esos terceros podrían estar generando emisiones o adoptando otras medidas que MDA deberá tener en cuenta. Al desarrollar los pilares de su programa de riesgos no financieros, MDA está identificando a esos terceros, considerando cómo medir cualquier riesgo relacionado, decidiendo cuál es la mejor manera de auditarlos y, a continuación, desarrollando una comprensión más amplia de lo que los riesgos de terceros y otros riesgos no financieros significan para la empresa.

Según la encuesta Pulse del IIA, las relaciones con terceros son la tercera área de mayor riesgo (después de la ciberseguridad y las TI), y la frecuencia de auditoría de las relaciones con terceros es relativamente baja en comparación con el nivel de riesgo.

Aunque la MDA se encuentra en las primeras fases de identificación de áreas de posibles riesgos no financieros, el proceso ha puesto de relieve hasta ahora el impacto que podrían tener en la capacidad de la empresa para alcanzar sus estrategias, así como en la percepción pública de la empresa. El proceso también proporcionará más información para la toma de decisiones a la dirección ejecutiva y al público, dijo Page. "Tenemos un conocimiento más completo de los riesgos financieros y no financieros y de cómo debemos controlarlos", declaró.

Participar desde el principio

Los auditores internos deben alertar a la dirección y a los consejos sobre el valor de incluir la auditoría interna desde el principio, especialmente cuando se aborda un concepto nuevo como el riesgo no financiero. "Si la auditoría interna participa desde el principio, hay más posibilidades de éxito en el futuro", afirma Page. "¿Por qué debería una empresa desplegar sus planes o procesos ESG o no financieros, y luego tener a la auditoría interna viniendo más tarde y señalando todos los problemas con él una vez que está en su lugar?".

Para mantener la independencia, la auditoría interna no puede estar en posición de tomar decisiones por una empresa, pero puede ofrecer ideas sobre la mejor manera de empezar a considerar los riesgos no financieros y qué planteamientos pueden funcionar o no. "Podemos ser un socio empresarial de valor añadido", afirma.

Page ha descubierto que establecer contactos en toda la organización es una buena forma de comprender mejor las áreas que auditará su equipo. Page se pone regularmente en contacto con personas implicadas en funciones empresariales importantes y les pide una reunión de 15 minutos tomando un café, y anima a su personal a hacer lo mismo. "Nadie ha dicho nunca que no", afirma. "Todos son apasionados y aman lo que hacen".

"Lo que me preocupa como jefe de auditoría es: ¿Qué es lo que no sé?" añadió Page. "La única forma de saberlo es hablando con la gente". Las auditorías de su equipo incluyen conversaciones con el personal del área auditada. También se mantiene al día del trabajo del equipo corporativo de ERM, aunque la auditoría interna tiene su propio proceso independiente de evaluación de riesgos.

Establecer contactos con sus homólogos en comités sectoriales o profesionales también ayuda a determinar si su enfoque de gestión de riesgos está actualizado y es todo lo riguroso que puede ser. Este conocimiento previo será especialmente importante para la información no financiera o ASG, ya que estos riesgos siguen evolucionando.

Page y su equipo han salido de sus conversaciones con una mayor comprensión y, por tanto, están mejor posicionados cuando llega el momento de auditar un área, algo que será especialmente útil para comprender la nueva frontera de los datos no financieros. El MDA abarca tres áreas de negocio distintas, por lo que la auditoría interna también puede compartir prácticas de éxito utilizadas por otros equipos y detectar la duplicación innecesaria de esfuerzos. "La perspicacia empresarial conduce a un éxito mucho mayor", afirma Page. Los auditores internos también pueden aportar valor desafiando el statu quo, cuestionando las prácticas existentes y desarrollando directrices que permitan una mejor comprensión e identificación de la información no financiera.

Orientación práctica de "*Risk in Focus 2023*"

Risk in Focus 2023, el último informe anual sobre riesgos elaborado por los miembros de la Confederación Europea de Institutos de Auditoría Interna (ECIIA), abordó diversas áreas de riesgo no financiero, incluidos los riesgos macroeconómicos y geopolíticos. Los participantes en una mesa redonda de líderes de auditoría interna abordaron la reevaluación del riesgo global, en particular porque el conflicto en Ucrania ha afectado a los riesgos en diversas áreas, incluida la estabilidad de los sistemas energéticos mundiales. Uno de los participantes en la mesa redonda, Ken Marnoch, vicepresidente Ejecutivo de Auditoría Interna e Investigaciones de Shell International, afirmó que él y su equipo están entablando "conversaciones más intensas sobre el apetito de riesgo".

De *Risk in Focus 2023*:

> "[Marnoch] afirma que tener una idea clara de cuánto riesgo puede asumir cada empresa en áreas específicas es muy útil cuando se plantea un dilema, en el que todas las opciones pueden tener ventajas e inconvenientes. Entonces, la claridad sobre el apetito por los riesgos asociados a las distintas opciones puede servir de guía para resolver el problema.
>
> Históricamente, la auditoría interna de Shell se había centrado en los riesgos operativos, culturales y de conducta. Ahora, el grupo de auditoría interna ha creado un equipo específico para centrarse en los riesgos y el marco de control asociados a la consecución de los objetivos estratégicos.
>
> 'Si se desglosan los objetivos estratégicos en metas cuantificables, los riesgos asociados, los controles explícitos y la forma en que los directivos saben que los controles funcionan, se dispone de margen para una auditoría interna", afirma. Parte de la función del nuevo equipo es ayudar a la gente a dejar de pensar de forma rígida sobre la corrección de las suposiciones que hicieron al principio de un proyecto o estrategia, cuando hay tantas cosas en el mundo que cambian drásticamente. Para navegar por un futuro incierto se necesita ser activamente inquisitivo, encontrar información que ponga a prueba las creencias y una rápida retroalimentación sobre la realidad actual.
>
> 'Si dejas de lado la necesidad de tener razón y reconoces que fue una decisión tomada con la mejor información del momento, estarás más abierto a buscar información que cuestione tu forma de pensar. De este modo, podrá tener mucho más poder a la hora de gestionar un riesgo clave para la realización de sus objetivos estratégicos.'"[10]

Risk in Focus 2023 incluye una lista de preguntas que la auditoría interna puede utilizar para evaluar el riesgo organizativo:

1. En términos del tiempo y el esfuerzo dedicados a las tareas de auditoría interna, ¿cómo se alinea la auditoría interna con los objetivos estratégicos de la organización, incluidos los relacionados con el riesgo geopolítico y el cambio climático?
2. ¿En qué medida se apoyan las actividades de auditoría interna en ámbitos como la estrategia y la gestión de crisis y qué puede hacerse para mejorar ese apoyo allí donde falta?
3. ¿En qué medida es capaz la auditoría interna de aprovechar los recursos de otras líneas para proporcionar una cobertura adecuada y minimizar la duplicación de esfuerzos?
4. ¿Cómo sabe si las suposiciones que la organización (y la función de auditoría interna) han hecho sobre la naturaleza de las áreas de riesgo clave siguen siendo válidas hoy en día y se ajustan a las circunstancias que probablemente se den en 2023?
5. ¿Dispone la organización de evaluaciones actualizadas del riesgo de sanciones y de controles sólidos para investigar la titularidad de terceros y los accionistas de la empresa?
6. ¿En qué medida aprovecha la organización las herramientas digitales para modelar los riesgos clave y ejecutar escenarios hipotéticos?
7. ¿Ha reevaluado la relación entre los equipos de continuidad de negocio, gestión de crisis y gestión de riesgos de la organización para asegurarse de que son adecuados para su propósito?
8. ¿Considera seriamente la organización las voces críticas y las de expertos externos en su evaluación de riesgos?

[10] *Risk in Focus 2023: More Risky, Uncertain, and Volatile Times Ahead,* European Confederation of Institutes of Internal Auditing, 2022, https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead/.

Conclusión

Una comprensión integral

Es importante comprender que los riesgos no financieros pueden tener un impacto financiero significativo en una organización, incluidos sus esfuerzos de ERM. Para ayudar a la dirección a comprender y abordar los riesgos no financieros, los responsables de la auditoría interna pueden utilizar su conocimiento exhaustivo de las múltiples facetas -y amenazas- de la entidad para aportar información valiosa sobre estos riesgos, así como para contabilizarlos y abordarlos adecuadamente cuando ayuden a determinar el apetito de riesgo de la organización.

Parte 2. Cuantificación del riesgo no financiero

Sobre el experto

Anishka Collie, CIA, CPA

Anishka Collie, CIA, CPA, es consejera delegada y consultora principal de ATC Financial Advisors & Consultants, en Nassau (Bahamas). Cuenta con más de 20 años de experiencia en auditoría externa, auditoría interna y gobierno corporativo, gestión de riesgos empresariales y controles internos, así como en planificación financiera, consultoría, corrección de procesos financieros y revisión de procesos empresariales. Se centra en clientes del sector de los servicios financieros y ha participado como ponente en numerosos seminarios de formación sobre contabilidad y auditoría.

Hassan NK Khayal, CIA, MBA, CRMA, CFE

Hassan NK Khayal, CIA, MBA, CRMA, CFE, es director de auditoría interna de Scope Investment en Dubai. En Internal Auditor, una publicación mundial del Instituto de Auditores Internos, figura entre los 15 líderes emergentes mundiales menores de 30 años como estrella emergente de la profesión de auditoría interna. Está terminando su doctorado en Administración de Empresas en la Universidad Católica de Murcia, España. Además de sus títulos y certificaciones profesionales, también posee certificaciones profesionales en automatización robótica de procesos, gestión de calidad, salud y seguridad, gestión medioambiental y gestión de riesgos.

Jason Minard, CIA, CISA, CPA (inactive)

Jason Minard, CIA, CISA, CPA (inactivo), es vicepresidente sénior y director sénior de Controles y Análisis de Supervisión en Wells Fargo Advisors, en San Luis (Misuri, EE. UU.). Con más de 25 años de experiencia en el sector de los valores y la auditoría, ha realizado y gestionado auditorías en áreas como la venta de inversiones, el cumplimiento normativo, las operaciones con valores, la banca de inversión, la gestión de activos, la administración fiduciaria y las finanzas. Es licenciado en administración de empresas por la Universidad de St. Louis y posee las licencias de representante general de valores y supervisor general de ventas.

INTRODUCCIÓN

A la persona Peter Drucker, gurú de la gestión, se le suele escuchar decir, "[sólo] lo que se mide, se gestiona". De hecho, las empresas llevan mucho tiempo comprendiendo la importancia de cuantificar y medir los riesgos financieros. La novedad de los últimos años ha sido el creciente interés por los riesgos no financieros, incluidos los medioambientales, sociales y de gobernanza (ASG), y las consideraciones reglamentarias y de información conexas. El reto ha sido cómo medir algo que a menudo no tiene un valor monetario fácilmente identificable. Es un reto que las organizaciones deben superar, porque los riesgos no financieros pueden tener sin duda un impacto financiero.

Este Informe Global de Conocimiento (Global Knowledge Brief), el segundo de una serie de tres partes sobre gobernanza, riesgo y control (GRC), examina los retos de cuantificar los riesgos no financieros y cómo las empresas los están abordando, así como el importante papel que la auditoría interna puede desempeñar en el avance de la comprensión en esta área.

COMPRENDER LOS RIESGOS NO FINANCIEROS

Innumerables amenazas potenciales

Aprender a reconocer y medir

Por regla general, los riesgos no financieros son los que se derivan del impacto de una organización en el mundo y, a la inversa, del impacto del mundo en la organización. Una lista parcial (véase el recuadro) refleja muchos, pero no todos, los riesgos no financieros a los que pueden enfrentarse las organizaciones. Las definiciones de estos riesgos son a menudo incoherentes o poco claras, lo que dificulta su reconocimiento y medición.

Sin embargo, los riesgos no financieros también existen en las transacciones financieras sencillas. Por ejemplo, al considerar el riesgo de crédito de un préstamo de 50.000 dólares, el valor del préstamo y la posible pérdida inicial están claros. Por otra parte, el riesgo no financiero de esta operación incluye consideraciones como el tiempo y el esfuerzo dedicados a hacer frente a un posible impago del préstamo, señala Anishka Collie, CIA, CPA, CEO y consultora principal de ATC Financial Advisors & Consultants, Nassau, Bahamas, que presta servicios de asesoramiento externalizado sobre riesgos y auditoría interna. Si el préstamo es importante o forma parte de un patrón de préstamos fallidos, es posible que la organización también tenga que profundizar para saber si la cultura corporativa, la documentación y los controles internos disponibles, o el nivel de formación actual son adecuados para mitigar el riesgo de crédito y garantizar unas buenas decisiones de préstamo.

Dado que los riesgos no financieros pueden ser difíciles de cuantificar, un riesgo relacionado es la posibilidad de que los informes y la divulgación de riesgos no financieros de una organización no sean fiables. Por ejemplo, el logro de determinados objetivos de sostenibilidad puede considerarse inflado intencionadamente o que se subestiman los problemas para alcanzar esos objetivos, una práctica conocida como "lavado verde" cuando está relacionada con cuestiones ASG. El "greenwashing" puede ser intencionado, o puede ocurrir simplemente debido a los niveles relativamente bajos de madurez disponibles actualmente en las normas de información no financiera, señaló un director ejecutivo de auditoría en una mesa redonda celebrada por la Confederación Europea de Institutos de Auditoría Interna (ECIIA).[11] Por el momento, la información puede ser inconsistente o difícil de comparar porque no existen estándares adoptados globalmente sobre información y divulgación no financiera. También hay varios marcos o normas disponibles, lo que hace potencialmente difícil para las empresas determinar qué directrices seguir y cómo aplicarlas, sobre todo porque a menudo pueden utilizarse en parte o en combinación con normas de otra norma o marco. El Center for Sustainable Organizations elaboró una

Riesgos no financieros
(lista parcial)

- Operacional
- Cumplimiento
- Estratégico
- Terceros
- Ciberseguridad
- Responsabilidad social
- Reputacional
- Privacidad de datos
- Integridad de los datos
- Protección de la propiedad intelectual
- Compensación
- Conducta de los empleados
- Gestión laboral
- Cultura ética y empresarial
- Salud pública
- Diversidad, equidad e inclusión
- Derechos humanos
- Recursos humanos
- Medio ambiente:
  - Emisiones de gases de efecto invernadero
  - Gestión de residuos
  - Abastecimiento de materias primas
  - Acceso/gestión de los recursos naturales
  - Cambio climático

[11] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

lista de 23 normas y marcos de medición e información no financiera que se basan en numerosas medidas de rendimiento diferentes y están dirigidas a distintos tipos de organizaciones.[12]

Preparando el escenario

Las organizaciones deberían considerar proactivamente cómo cuantificar el riesgo no financiero, pero muchas no lo hacen. Abordar el riesgo financiero se correlaciona con el objetivo principal de una organización: maximizar la riqueza de los accionistas y aumentar los ingresos. Al abordar los riesgos no financieros, se pide a las organizaciones que gasten dinero en esfuerzos cuyo valor puede ser difícil de entender y que no añaden ingresos inmediatamente. Según PwC, "hasta que no se pueda cuantificar y asignar una cifra financiera al impacto del riesgo, es improbable que se consiga la implicación necesaria de la dirección para abordarlo".[13]

Otro obstáculo es que las funciones de control de los riesgos no financieros pueden estar aisladas en una organización. Como estos riesgos son tan diversos, a menudo están bajo la supervisión de una amplia gama de equipos. Cada equipo puede tener su propio proceso de identificación de riesgos, estructura de informes e incluso diferentes sistemas informáticos relacionados con los riesgos no financieros. "Se pide a las mismas personas, ya sean de auditoría interna, de cumplimiento o de otra área, que realicen el mismo procedimiento una y otra vez", afirma Hassan NK Khayal, CIA, MBA, CRMA, CFE, director de auditoría interna de Scope Investment en Dubai. El gasto añadido de esta duplicación de esfuerzos hace que sea más probable que la dirección rechace las inversiones en recopilación de información y cuantificación.

Sin embargo, la adopción de medidas preventivas reduce los costes de reparación y protege la marca de la empresa y sus relaciones comerciales. En la mayoría de las organizaciones, los métodos de información sobre riesgos aún no son lo bastante sofisticados o precisos para convencer a la dirección, afirma Khayal. Pero si se seleccionan adecuadamente, los indicadores correctos pueden captar y cuantificar con precisión los riesgos no financieros y proporcionar el contexto adecuado para que la dirección comprenda sus posibles repercusiones.

Identificar proactivamente las posibles amenazas no financieras antes de que se produzcan facilita su comprensión y cuantificación. Por ejemplo, en el sector de la alimentación y bebidas, es fácil cuantificar el riesgo financiero cuando se estropea una determinada cantidad de comida. Sin embargo, calcular los costes y riesgos relacionados con la salud y la seguridad es más difícil, señala Khayal. Al tener en cuenta estos riesgos, una organización puede tomar medidas proactivas y preparatorias, como mejorar la limpieza para que un restaurante sea más atractivo y menos propenso a causar enfermedades a los clientes. Del mismo modo, en el sector de la construcción, cuando los ingenieros de seguridad son más estrictos en el control y la aplicación de las normas de salud y seguridad, el número de accidentes suele disminuir.

"Cada incidente tiene su propio coste asociado", afirma Khayal, ya sea el coste directo de hacer frente al suceso y a los posibles heridos, o el coste de los retrasos asociados. "En el momento en que se ha producido el riesgo, ya es demasiado tarde", señaló, y el daño a la reputación y las relaciones de la organización ya está hecho, quizá con repercusiones duraderas o importantes. Pero cuando las organizaciones evalúan los costes de los riesgos potenciales, es más probable que vean el valor de tomar medidas preventivas.

Khayal cree que los riesgos no financieros pueden tener mayores efectos que los financieros. Su impacto puede hacer que partes interesadas como accionistas, empleados y clientes cuestionen el modelo de negocio o las prácticas de una empresa cuando se produce un daño reputacional. "Todo ello ejerce una presión considerable sobre las organizaciones para que gestionen los riesgos no financieros", afirma.

Trabajando hacia la cuantificación

Aunque los riesgos no financieros no conllevan valores monetarios directos, es posible asignarles valores numéricos. La clave está en definir los riesgos y lo que abarcan, y luego encontrar consideraciones tangibles que medir. Al abordar el riesgo de cliente, por ejemplo,

[12] https://www.sustainableorganizations.org/Non-Financial-Frameworks.pdf
[13] "Taking Control: How to Get on top of Non-Financial Risks," Christopher Eaton and David O'Brien, PwC Channel Islands, March 9, 2021.

es posible determinar factores como el número de reclamaciones de clientes, los lugares o situaciones relacionados, las pérdidas de clientes asociadas, la disminución de nuevos clientes, y qué tendencias revelan estos datos a lo largo del tiempo.

Cuando no hay criterios tangibles para medir, una opción es categorizar los riesgos de una manera que sea lo más descriptiva y significativa posible, como si están en niveles altos, medios o bajos. Por ejemplo, cuando existe un riesgo de cumplimiento y reglamentario, las organizaciones podrían intentar cuantificar el riesgo determinando la gama de posibles hallazgos de un regulador en cada categoría de riesgo. Categorizar los hallazgos de esta manera proporciona a las empresas un marco para evaluar más a fondo cada riesgo y establecer prioridades.

Un marco organizado de calificaciones es otra opción que permite captar las conclusiones sobre una serie de riesgos no financieros. Los equipos de auditoría interna podrían utilizar un marco de calificaciones que califique las observaciones realizadas por la auditoría interna y cualquier otro equipo, como el de cumplimiento, riesgos, seguridad de la información o jurídico, que identifique riesgos no mitigados y los rastree, notifique o remedie. El marco puede utilizarse para evaluar el impacto de los riesgos no financieros y apoyar su cuantificación. Un ejemplo del tipo de marco que las empresas pueden utilizar para comprender y comunicar mejor el impacto financiero de sus medidas de sostenibilidad es el modelo Global Compacto de las Naciones Unidas de Impulsores de Valor para Principios de Inversión Responsable.

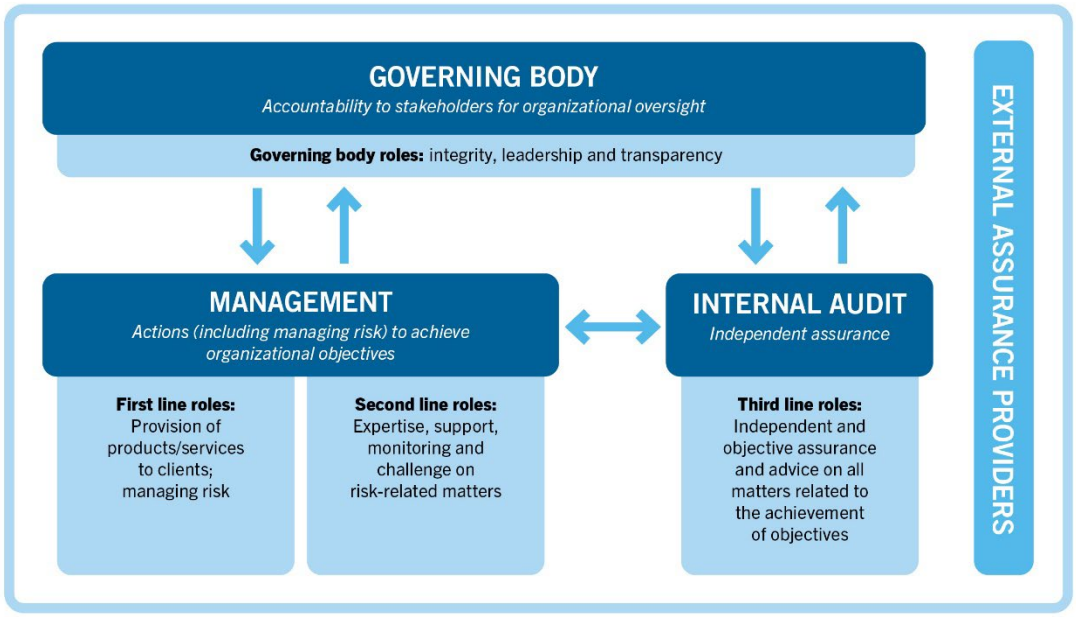
EL PAPEL DE LA AUDITORÍA INTERNA

"Pioneros" del riesgo no financiero

Controles futuros y de seguimiento pendientes

Las empresas se esfuerzan por cuantificar, El papel de la auditoría interna es ser estratégica y centrarse en las mejores formas de añadir valor, como se describe en el Modelo de las Tres Líneas del IIA (véase la Figura 1). Para lograr este objetivo, los auditores internos no deben limitarse a analizar los estados financieros y los riesgos financieros, sino que deben ser pioneros en abordar los riesgos no financieros siguiendo un enfoque basado en el riesgo y teniendo siempre en cuenta el futuro, afirma Khayal. "Lo ideal sería que fuéramos uno de los departamentos más orientados al futuro de la organización", dijo. "Deberíamos centrarnos en los riesgos futuros antes de que la dirección, con la vista puesta en los impactos del día a día, sea siquiera consciente de ellos". Para mantener la independencia, la auditoría interna no define las categorías o definiciones de riesgo que utiliza la organización, pero sí cuestiona las políticas de riesgo no financiero y cómo se aplican en consonancia con el proceso general de evaluación de riesgos.

Figura 1: Modelo de tres líneas



Como consultora, el papel de Collie se parece mucho al de un auditor interno y es el que pueden seguir los auditores cuando se trata de riesgos no financieros. Al principio, habla con los líderes de la organización, incluidos no sólo el CEO y el CFO, sino también los jefes de cumplimiento, riesgo y auditoría interna. El objetivo es conocer sus definiciones de riesgo para su organización, cómo identifican los riesgos, con qué nivel de detalle y qué controles existen. Durante estos debates, los participantes suelen llegar a una nueva comprensión del riesgo y su impacto, afirma Collie.

Estas conversaciones iniciales son de alto nivel para comprender qué se necesita para que la organización funcione con eficacia. El siguiente paso es hablar con los directivos o jefes de departamento para conocer mejor las operaciones cotidianas y dónde pueden producirse los riesgos. Una vez comprendido esto, el auditor puede intercambiar ideas con los empleados de este nivel para saber qué medidas de gestión de riesgos han tenido éxito o han fracasado y dónde existen puntos débiles en la gestión de riesgos. Al igual que los consultores pueden ofrecer experiencia en diversas organizaciones, los auditores internos tienen un conocimiento holístico de muchas áreas de la organización. "Pueden sacar a la superficie cosas en las que estos equipos quizá no hayan pensado", afirma Collie.

Los auditores necesitarán nuevas competencias para facilitar el proceso. Los enfoques tradicionales de auditoría interna consisten en identificar el riesgo en relación con los controles, los datos y los documentos. Trabajar con los clientes para identificar y comprender los riesgos no financieros requiere habilidades adicionales y formación continua en relación con las entrevistas o la facilitación de una sesión de lluvia de ideas, dijo Collie. "Ayudar realmente a los clientes a recorrer el proceso de identificación de riesgos es un ejercicio completamente distinto", afirma. La dirección tendrá que invertir en esta formación para garantizar que la organización funciona de forma eficaz y eficiente.

La auditoría interna también puede evaluar el valor y la fiabilidad de los indicadores clave de rendimiento y métricas existentes cuando se aplican a riesgos no financieros, así como nuevas medidas desarrolladas específicamente para riesgos no financieros y controles y procesos de gestión de riesgos relacionados. Para evitar acusaciones de lavado verde, pueden garantizar que los datos compartidos con las partes interesadas ofrezcan una imagen justa y exacta de los esfuerzos de la empresa, según la ECIIA.[14]

Khayal elabora su plan de auditoría y evaluación de riesgos en torno a los numerosos elementos de riesgo que pueden afectar a la capacidad de una organización para alcanzar su estrategia, tanto financiera como no financiera. Por ejemplo, si la estrategia de la organización y la creación de valor dependen de unas prácticas rigurosas en la cadena de suministro, las compras serán siempre una preocupación clave, afirma. La cartografía de los riesgos, y en particular de los riesgos no financieros, puede revelar amenazas como problemas de solvencia de los clientes, problemas en la cadena de suministro y retos de ciberseguridad.

A medida que las organizaciones desarrollan sus marcos y perfeccionan las definiciones que utilizan, crean un lenguaje común sobre los riesgos no financieros. Esto mejora la comunicación sobre el riesgo entre la primera, segunda y tercera línea; aclara las responsabilidades de cada línea; y permite a cada una añadir sus propias mejoras a las definiciones compartidas.

Responsabilidades para el futuro

En la organización de Khayal, cualquiera que participe en los controles y la autoevaluación de riesgos debe seguir un curso detallado de formación sobre riesgos que incluye los riesgos no financieros. También anima a su personal a centrarse en tres tareas clave:

- **Manténgase informado**. Los auditores internos deben mantenerse al corriente de los últimos acontecimientos mundiales y locales para comprender mejor los incidentes que podrían repercutir en el riesgo ahora o a corto o largo plazo.
- **Manténgase al día sobre las tecnologías emergentes.** Khayal cree que los auditores del futuro y las organizaciones para las que trabajan deben ser expertos en TI. Los auditores ya no pueden confiar únicamente en los métodos tradicionales, sino que deben incorporar herramientas tecnológicas. "El mundo cambia a un ritmo cada vez más rápido", afirma. Sin una tecnología sólida, "las organizaciones no podrán seguir el ritmo, sobre todo porque cada vez hay más factores macroeconómicos no financieros a los que nos enfrentamos."
- **Mantenerse en sintonía con la estrategia, la misión y la visión de la organización.** Los planes de auditoría deben considerar qué riesgos son los más importantes y cuál es la mejor manera de cuantificarlos. Dado que, por lo general, las organizaciones no pueden abordar todos los tipos de riesgo a los que pueden enfrentarse, los auditores deben tener en cuenta diversos factores para identificar e intentar cuantificar aquellos riesgos que probablemente tengan mayor importancia e impacto.

[14] *Risk in Focus 2023: Hot Topics for Internal Auditors*, European Confederation of Institutes of Internal Auditing, 2023.

CONCLUSIÓN

Como asesores de confianza de la organización, Los auditores internos se encuentran en una posición única para impulsar una mayor comprensión y reconocimiento de los riesgos no financieros. Pueden hacerlo aprovechando su actual conocimiento exhaustivo de la empresa, añadiendo nuevas competencias y abogando por un cambio en la perspectiva organizativa que determine la mejor manera de cuantificar el riesgo no financiero.

Parte 3: Cómo la transformación digital está transformando la GRC

Sobre los expertos

Sarah Kuhn, CIA, CCSA, CRMA

Sarah Kuhn es una profesional con gran experiencia en el campo de la auditoría interna. Con más de 20 años de pertenencia al Instituto de Auditores Internos (IIA) y una pasada presidencia del capítulo de Tulsa, ha demostrado su compromiso con el sector con experiencia en formación de departamentos, elaboración de informes y cumplimiento de normas, así como dirigiendo un equipo de auditoría centrado en la analítica y la automatización. Sarah también trabaja actualmente como oficial en el capítulo de Houston del IIA.

Audra Nariunaite, CIA, CISA, CFE, CHC, CHPC

Audra Nariunaite es una profesional del cumplimiento y la auditoría con experiencia en múltiples sectores y una capacidad demostrada para impulsar el crecimiento y la excelencia a través de iniciativas estratégicas y la reingeniería de procesos. Actualmente forma parte de la junta directiva de The IIA Northeast Florida Chapter y es miembro de IIA-Lithuania. Audra es actualmente directora de cumplimiento en la plataforma global de empleo Oyster HR..

Introducción

Podría decirse que no hay tendencia está afectando al panorama de la gobernanza, el riesgo y el cumplimiento (GRC) de forma más significativa que el aumento de las tecnologías en las operaciones empresariales diarias, y es fácil ver por qué. No se pueden subestimar los beneficios de la transformación digital, ya que las herramientas derivadas de esta tendencia se utilizan actualmente en casi todos los sectores importantes para automatizar y acelerar los procesos, lo que permite a las operaciones de GRC y seguridad identificar y responder rápidamente a los posibles riesgos y problemas.

Por ejemplo, gracias a su capacidad para analizar fuentes de datos no estructuradas, desde correos electrónicos hasta fuentes de redes sociales, el procesamiento del lenguaje natural asistido por IA puede combinarse con las habilidades y la experiencia de los equipos humanos de GRC para proporcionar recursos de gestión de riesgos y cumplimiento a un nivel de sofisticación y complejidad que no podría haberse imaginado hace tan solo una generación.

Aunque la necesidad de someterse a una transformación digital tan radical podría haberse considerado un lujo en el pasado, el panorama de riesgos actual ofrece a las organizaciones poco margen para retrasar la adopción. Las ciberamenazas se intensifican día a día en volumen y sofisticación; el volumen bruto de datos que se producen, recopila y procesan sigue creciendo a un ritmo asombroso, creando riesgos cada vez mayores para la privacidad de los datos; y el panorama normativo sigue evolucionando rápidamente para adaptarse a la velocidad de los riesgos actuales. De hecho, sin las ventajas que ofrece la transformación digital, las funciones de GRC en el mundo actual bien podrían perderse.

Como Parte 3 de la serie Informe Global de Conocimiento (Global Knowledge Brief) del IIA sobre GRC, esta última entrega aborda cómo los sistemas de GRC están evolucionando a partir de la incorporación de nuevas tecnologías, así como los riesgos inherentes que implica la adopción de la transformación digital. Este resumen también aborda dónde encaja la auditoría interna en esta conversación y cómo podría ayudar mejor a las organizaciones a medida que continúan este viaje crítico.

La conversación sobre la Transformación Digital en 2023

Comprender un riesgo cargado

El alcance de la transformación digital

La explosión de la transformación digital visto durante la pandemia de COVID-19 sigue haciendo estragos y, en cierto modo, su evolución está ganando velocidad. Esto ha ocurrido no sólo por el deseo básico de aumentar los beneficios y la eficiencia para obtener una ventaja competitiva en el mercado, sino también por el afán de mantener el ritmo (o, en el mejor de los casos, adelantarse) a la extensa lista de riesgos emergentes que se han materializado en los últimos años. La inflación, las tensiones geopolíticas como el conflicto de Ucrania, la disputa entre China y Taiwán, la incertidumbre económica generalizada resultante de acontecimientos como el cierre repentino de numerosas instituciones bancarias a gran escala, los debates en curso relativos a los riesgos ESG y los cambios relacionados con el panorama normativo, las interrupciones de la cadena de suministro y la escasez, son sólo algunas de las formas que ha adoptado el riesgo en 2023. Desde la perspectiva de las organizaciones encargadas de mantener una cierta seguridad frente a ellos, la adopción a gran escala de la transformación digital se considera un bálsamo eficaz. De hecho, según un informe reciente de Gartner, el 89 % de los directores de consejos de administración afirman que el negocio digital está ahora integrado en todas las estrategias de crecimiento empresarial, aunque solo el 35 % afirma haber alcanzado o estar en vías de alcanzar los objetivos de transformación digital.

"Los consejos de administración han llegado a un punto en el que la estrategia empresarial digital y la estrategia empresarial general son una misma cosa", afirma Jorge López, vicepresidente y analista distinguido de Gartner, en el informe. "Aunque los CIO han hecho progresos significativos aprovechando la tecnología para la excelencia operativa, esto no es suficiente para obtener los beneficios empresariales estratégicos que [los consejos de administración] buscan de las inversiones digitales."[15]

El aspecto de la transformación digital varía de un lugar a otro, de un sector a otro y de una organización a otra. Lo que es eficaz, o incluso factible, para una organización puede no ser ideal para otra. A pesar de ello, existen algunas similitudes fundamentales entre las organizaciones que adoptan alguna forma de transformación digital. "La transformación digital es algo más que tecnología", afirma Chintan Shah, CEO y fundador de Brainvire, en un artículo para Forbes. Se trata del cambio de mentalidad que permite a las organizaciones reimaginar sus modelos y procesos empresariales para aprovechar las oportunidades creadas por las tecnologías emergentes."[16]

López expresó un sentimiento similar. "Como las empresas operan cada vez más en un mundo de constantes trastornos, los consejos más preparados para el futuro están considerando cómo los trastornos y los riesgos pueden servir de fuente de oportunidades. Los consejeros delegados y los directores de sistemas de información tendrán que adoptar esta mentalidad, ya que la tecnología desempeña un papel cada vez más importante en el éxito de las empresas."

Esta reimaginación puede adoptar muchas formas, entre otras:

15. "Gartner Says 89% of Board Directors Say Digital Is Embedded in All Business Growth Strategies," press release, Gartner, Oct. 29, 2022, https://www.gartner.com/en/newsroom/press-releases/2022-10-19-gartner-says-89-percent-of-board-directors-say-digital-is-embedded-in-all-business-growth-strategies.

16. Chintan Shah, "Businesses Need to Watch these Digital Transformation Trends in 2023," Forbes, Jan. 27, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/01/27/businesses-need-to-watch-these-digital-transformation-trends-in-2023/?sh=7147b04a185d.

- Adopción de la inteligencia artificial (IA), el aprendizaje automático y el procesamiento del lenguaje natural.
- Automatización robótica de procesos (RPA).
- Ciberseguridad y privacidad de datos.
- Migración a la nube.
- Análisis de datos.
- Adopción de 5G y optimización digital.
- Blockchain.
- Colaboración empresarial virtual.
- Plataformas de datos de clientes.

Efecto de la transformación digital en la GRC

Es evidente que, con tantas connotaciones y aplicaciones, la transformación digital ha tenido un profundo efecto en las funciones de GRC y, en muchos casos, las organizaciones han luchado por mantener niveles adecuados de cobertura de GRC a medida que los cambios en el panorama tecnológico continúan a buen ritmo. Una encuesta reciente de Risk.net en colaboración con IBM a profesionales de GRC del sector de servicios financieros reveló algunas tendencias alarmantes, entre ellas:

- El 62% cree que su transformación digital ha dejado al descubierto lagunas en los procesos GRC existentes, y casi la mitad de los encuestados (45%) piensa que sus organizaciones están ahora "jugando a ponerse al día." Solo el 37 % afirma haber invertido tiempo y recursos en su transformación digital antes del cambio.
- El 77% cree que los riesgos de sus empresas han aumentado al depender más de los canales digitales.[17]

Además, en el mismo estudio, cuando se les preguntó qué riesgos asumían una mayor prominencia en su organización como resultado de las tendencias de transformación digital, el 56% identificó la seguridad de la información/datos, el 48% dijo que las brechas de ciberseguridad, el 32% dijo que el riesgo de terceros/cadena de suministro y el 31% dijo que el riesgo de cumplimiento.

Para seguir siendo eficaces, las funciones de GRC han tenido que modernizarse tomando medidas definitivas para adoptar la transformación digital o arriesgarse a someter a sus organizaciones a un riesgo significativo. Estos pasos incluyen:

- Asignación o contratación de nuevos recursos.
- Adoptar algún tipo de modelo de almacenamiento de datos en la nube híbrida para usos mejorados de análisis de datos.
- Actualización de las herramientas y capacidades actuales de GRC.
- Implantación de tecnología avanzada, incluidas herramientas relacionadas con la IA y sistemas de automatización.

Aunque algunas de estas acciones pueden parecer algo obvias, la velocidad a la que evoluciona el panorama actual de los riesgos las convierte en cualquier cosa menos obvias. Por ejemplo, históricamente, las organizaciones se basaban en la conformidad con determinadas directrices o un marco de normas, certificaciones y/o reglamentos para establecer una base de controles y procesos probados que permitieran el éxito de la función de GRC.

Hoy en día, sin embargo, este planteamiento puede volverse complejo rápidamente. Esto puede deberse a:

- El rápido desarrollo de marcos nuevos o actualizados que requieren una rápida conformidad. Algunos ejemplos son la rápida creación de una serie de iniciativas normativas propuestas en la UE relacionadas con la estrategia digital, como la Ley de

[17] "Digital Transformation and the Future of GRC," Risk.net, IBM, Feb. 2022, https://www.ibm.com/downloads/cas/WWQXRPLG.

Conformidad de Datos, la Ley de Mercados Digitales, la Ley de Servicios Digitales, la Ley de Datos y la Ley de IA, todas las cuales prevén su aprobación para finales de 2023; o

- La falta de claridad u orientación de los marcos actuales, que deja a las organizaciones -al menos durante un tiempo- a su suerte.

"Con sistemas como ChatGPT y Bing Chat a punto de salir al mercado y CoPilot preparándose actualmente para su lanzamiento, muchas organizaciones están necesitando actuar rápidamente porque los empleados ya están utilizando algunas de estas tecnologías para completar tareas", dijo Sarah Kuhn, una destacada líder de auditoría interna con más de dos décadas de experiencia y servicio en la profesión. "Hay algunas organizaciones que las bloquearán por completo, mientras que otras con equipos más equipados para entender las tecnologías crearán directrices internas más detalladas sobre cómo y cuándo deben utilizarse."

Los equipos encargados de desarrollar estrategias para crear dichas directrices variarán en su composición en función de la organización, pero podrían incluir partes como el director digital y de información, equipos de TI y de gestión de riesgos, grupos jurídicos y financieros. Una vez creadas, sin embargo, las estrategias para comunicar y hacer cumplir las directrices son igualmente críticas. "Las empresas pueden funcionar hasta cierto punto según un sistema de honor", afirma Kuhn, "pero también se necesitan medidas más formales para comunicar la evolución de las directrices. Por ejemplo, cuando un empleado teclea una dirección determinada, se puede implantar un programa que haga que aparezca un banner en su navegador recordándole las directrices de la empresa."

Para lograr tal hazaña sin problemas, Kuhn señaló que una función GRC ágil y adaptable tendría que estar en marcha antes de que tecnologías emergentes como ChatGPT entraran en el panorama de riesgos de la organización. No todas las organizaciones van a tener la bendición de tal previsión, ya sea debido a recursos restringidos, datos disponibles limitados o de mala calidad, priorización de otras cuestiones o simple negligencia. Independientemente de las razones, la auditoría interna debe estar preparada para tomar la iniciativa y conseguir rápidamente que las funciones de GRC estén en una posición adecuada para tener éxito en esta nueva era.

Auditoría interna en la discusión sobre GRC

Mejorar la GRC en el contexto de la transformación digital

Mantener un puesto en la mesa

La auditoría interna puede contribuir a la eficacia de la GRC de varias formas clave, especialmente en organizaciones que se consideran atrasadas en sus objetivos de actualización de las funciones de GRC.

En primer lugar, pocos cambios que merezcan la pena pueden lograrse sin cierto grado de inversión. Estas inversiones, sin embargo, pueden ser difíciles si no cuentan con el apoyo de todos los niveles, desde la cúpula de la organización hasta cada una de las partes interesadas en la función de GRC. Si no hay aceptación de la transformación digital, es muy probable que sus beneficios no se comuniquen adecuadamente. En este sentido, la auditoría interna se encuentra en una posición única para transmitir dicha información simplemente manteniendo un asiento en la mesa.

"Desde nuestro puesto en la mesa, podemos garantizar, a través de cada tendencia emergente, que la dirección y el consejo toman decisiones con conocimiento de causa", afirma Kuhn.

De hecho, un asiento en la mesa siempre debería ser fundamental para que un auditor interno desempeñe sus funciones de acuerdo con su mandato. A través de una comunicación regular e informada con las partes interesadas, la auditoría interna desempeña un papel inestimable en la promoción de una cultura organizativa sólida en torno a la garantía del riesgo y el cumplimiento. Cuando los canales de comunicación de la auditoría interna se aprovechan al máximo, la GRC nunca debería estar lejos de ser una prioridad.

El riesgo de la proliferación de herramientas de GRC

No todos los controles disponibles para implantar favorecerán el éxito de una cultura centrada en la GRC. Por ejemplo, con la digitalización de los procesos organizativos, ahora hay muchas herramientas de análisis de datos disponibles que incluyen módulos de GRC como complementos. La auditoría interna podría verse considerablemente obstaculizada a la hora de comunicar una visión global de la GRC a las partes interesadas si todas las funciones individuales de GRC se comprometen a utilizar herramientas independientes para ayudarles.

"Me encantan las herramientas de análisis de datos y las capacidades de comprobación al 100% que ofrecen, pero ahora hay muchas otras herramientas que les añaden GRC como oferta de valor", afirma Audra Nariunaite, directora de cumplimiento normativo del proveedor de plataformas de empleo automatizadas Oyster. "Una herramienta que estuve examinando recientemente agrega otras herramientas SaaS para destacar qué contratos están próximos a renovarse y los ahorros potenciales en impuestos, pero también proporciona una versión de un cuadro de mandos de riesgos basado en la información que procesan las herramientas SaaS. Si la intención de comprar una herramienta de este tipo fuera para algo distinto de GRC, ni siquiera la conocería."

"De repente, podría encontrarme en una situación en la que tuviera una docena de herramientas SaaS aleatorias con componentes, todas ellas representando un riesgo de alto nivel porque los proveedores están procesando nuestra información privada", continuó Nariunaite. "Actualmente, hay más de 100 herramientas SaaS en nuestro ecosistema. Incluso si un pequeño porcentaje de esas herramientas ofrece una versión de GRC para procesos muy específicos, se hace difícil de gestionar. Se crean bolsas individuales en las que la gente cree que está haciendo evaluaciones de riesgos, pero no las está haciendo de una manera que esté integrada de una forma holística y reportable."

Para contrarrestar este riesgo, una estrategia consiste en que las partes interesadas en la GRC asignen propietarios de procesos individuales para racionalizar el enfoque de la GRC y crear una pista de comunicación clara para la auditoría interna. "Todo el mundo quiere hacer lo correcto", afirma Nariunaite. "Ahora hay un impulso para gestionar el riesgo global, y eso es estupendo. Sin embargo, hay que hablar de la división de funciones y de cómo hacerlo para alinear prioridades y ámbitos."

Kuhn expresó un sentimiento similar al subrayar el equilibrio que deben mantener las organizaciones entre la responsabilidad compartida y el control descendente. "La auditoría interna debe intentar que las partes interesadas dirijan los objetivos y procesos de GRC en la medida de lo posible, y luego abordarlo desde un contexto de fomento de la colaboración y la transparencia. La auditoría interna debe formar parte de esa conversación, de modo que podamos estar ahí para alertar cuando veamos algo. La mayoría de la gente entiende el riesgo y el control en relación con sus propias funciones. En realidad, no necesitan que interfiramos, pero tenemos que entender los objetivos más amplios y dónde residen las responsabilidades para realizar una supervisión adecuada."

Estrategias para dirigir y promover el debate

Siempre que sea posible, la auditoría interna debe predicar con el ejemplo proyectando y promoviendo los beneficios de la transformación digital a través de la eficacia de su función. Aunque algunos aspectos de la transformación digital dentro de la auditoría interna requieren obviamente un margen presupuestario significativo, otros aspectos, como la automatización básica, pueden llevarse a cabo a través de programas como Excel, Power BI y otras herramientas de productividad de Microsoft que probablemente ya sean internas o, al menos, puedan adquirirse a un coste mínimo.

Predicar con el ejemplo se aplica también a la puesta en común de conocimientos, lo que incluye destacar dónde faltan competencias críticas en las funciones de GRC. Tanto dentro de la función de auditoría interna como en otros departamentos, la auditoría interna puede desempeñar un papel constructivo a la hora de poner de relieve las carencias de conocimientos, formación o experiencia de los trabajadores en relación con el trabajo con tecnologías emergentes, promoviendo al mismo tiempo medidas correctivas adecuadas. Tales medidas podrían incluir la formación comunitaria en conferencias, la contratación de partes externas para la formación y la actualización de conocimientos, o simplemente la incorporación de la formación basada en habilidades en las funciones de trabajo a través de recursos en línea gratuitos o a un precio razonable.

En algunos casos, las organizaciones pueden trabajar para promover la mejora de las competencias dentro de la empresa mediante interacciones y colaboraciones con otros departamentos. "Una estrategia que he visto es crear un sitio web en el que todos los miembros de la organización puedan aportar sus propias ideas de innovación y luego votar o comentar lo que les gustaría ver en la empresa", explica Kuhn. "Sería una forma de compartir conocimientos e ideas de manera controlada, para que todo el mundo no se dedique a hacer mil cosas distintas para desarrollar competencias."

Ese debate no siempre tiene que ser formal; incluso algo tan sencillo como un chat comunitario puede producir un resultado similar. "En nuestra organización hay varios canales de Slack en los que cualquiera puede participar", explica Nariunaite. "Últimamente, por ejemplo, he estado pasando el rato en el canal de humor de ingeniería. Entienden que soy el jefe de cumplimiento, pero me tratan como a un compañero. Me encanta que todos podamos tener conexiones informales con equipos que realmente están a la vanguardia del movimiento de transformación digital."

Sin embargo, para contribuir al debate, la auditoría interna debería recibir un impulso adicional para adquirir conocimientos sobre estas tecnologías.

De hecho, la adquisición de estos conocimientos puede ser una valiosa oportunidad para que la auditoría interna añada valor a la organización. "No creo que podamos participar de manera significativa en el debate con las partes interesadas cuando pedimos reunirnos con ellos sobre, por ejemplo, IA o análisis de datos, si no tenemos un grado significativo de conocimiento por derecho propio", dijo Nariunaite. "Así que muchos aspectos de la transformación digital en GRC todavía están en el aire en cuanto a quién va a tomar posesión de ellos. ¿Por qué no la auditoría interna? Somos curiosos; tenemos una mente abierta; y siempre estamos aprendiendo junto a nuestros clientes para que podamos tener un lugar en las discusiones. ¿Y si fuéramos nosotros los que asesoráramos en algo como la implantación de la IA en el cumplimiento normativo?".

Conclusión

Forme parte activa de la comunidad de auditoría interna

No hay vuelta atrás de una transformación digital, y las opciones para una organización son sencillas: adoptarla o quedarse atrás. Este sentimiento se extiende a todos los elementos de la organización, desde la alta dirección y la sala de juntas hasta el GRC, las operaciones y la auditoría interna.

Además, especialmente en un mundo cada vez más interconectado y globalizado, debe fluir a través de sectores y fronteras geográficas. Esto significa no sólo realizar tareas dentro de los límites de una organización, sino también ir más allá para participar activamente en debates globales sobre auditoría. Participar en las secciones locales del IIA puede ser un buen lugar para forjar estas conexiones, al igual que la asistencia regular a seminarios web y conferencias del IIA..

“El mejor aprendizaje de auditoría interna que se puede tener es escuchar de primera mano las experiencias de otras funciones", dijo Nariunaite. "Aprendo mucho simplemente 'frikeando' sobre temas actuales de auditoría y tendencias tecnológicas con otros profesionales en Twitter. La profesión ha cambiado tanto desde que yo empecé; es muy importante mantener esas conexiones con el sector y seguir el pulso de cómo otros están superando con éxito los retos a los que tú te enfrentas.”

Aunque la tecnología ha avanzado mucho -y seguirá avanzando-, es reconfortante saber que, cuando se trata de aprender y crecer profesionalmente, no hay nada que pueda sustituir a una auténtica conexión humana. Ante el cambio incesante, será importante recordarlo.

Sobre el IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin ánimo de lucro que cuenta con más de 235.000 miembros en todo el mundo y ha concedido más de 190.000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite: theiia.org.

Disclaimer

Copyright

Junio 2023

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad.

Traducción al Español Auspiciada por:
FLAI
Fundación Latinoamericana de Auditores Internos

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101