Norma 2600 – Comunicación de la aceptación de los riesgos

Cuando el Director Ejecutivo de Auditoría concluya que la alta dirección ha aceptado un nivel de riesgo que pueda ser inaceptable para la organización, debe tratar este asunto con la alta dirección. Si el Director Ejecutivo de Auditoría determina que el asunto no ha sido resuelto, el Director Ejecutivo de Auditoría debe informar esta situación al Consejo.

Interpretación:

La identificación del riesgo aceptado por la Dirección puede observarse a través de un trabajo de aseguramiento o de consultoría, a través del seguimiento del progreso sobre las acciones tomadas por la Dirección como resultado de anteriores trabajos, o a través de otros medios. El Director Ejecutivo de Auditoría no tiene la responsabilidad de resolver el riesgo.

Introducción

Para lograr implementar esta Norma, el Director Ejecutivo de Auditoría (DEA) debe primero comprender la visión de la organización y su tolerancia a los distintos tipos de riesgos. Las organizaciones difieren en la cantidad y el tipo de riesgos que consideran aceptables. Por ejemplo, algunas organizaciones pueden aceptar un mayor nivel de riesgos financieros con acciones como expandirse en una nueva localización geográfica con un gobierno inestable; o realizar una inversión importante en un nuevo producto fantástico que tiene una probabilidad de éxito bastante baja, pero unos suculentos beneficios en caso de éxito. Otras organizaciones tienen más aversión a estos riesgos financieros, y evitan estas situaciones. Además, las entidades tienen en cuenta distintos factores para determinar el nivel de riesgos aceptable; por ejemplo, el impacto potencial y la probabilidad del evento de riesgo, la vulnerabilidad de la organización, y el tiempo que tardaría la Dirección en resolver un riesgo inaceptable.

Si la organización tiene una política formal de gestión de riesgos, que puede incluir un proceso de aceptación de riesgos, es importante que el DEA y la actividad de auditoría interna la conozcan.

Como se requiere en la Norma 2500, el DEA también puede establecer y mantener un sistema de supervisión de la situación de los resultados de las auditorías internas.

También resulta útil para el DEA conocer como se comunican habitualmente dentro de la organización, las cuestiones relacionadas con los riesgos más graves. Puede que existan políticas que definan el enfoque de comunicación que se prefiere; por ejemplo, la política de gestión de riesgos de una organización

puede regular cuestiones como la oportunidad en el tiempo, la jerarquía de los informes, y consideraciones similares.

Consideraciones para la implementación

Para supervisar la situación de los resultados y de las acciones correctivas asociadas, el DEA puede estar al tanto de las observaciones de alto riesgo que no han sido corregidas en el tiempo previsto o que pueden representar un riesgo mayor del que la organización normalmente toleraría y que, por lo tanto, son inaceptables para la organización.

Sin embargo, el proceso de supervisión continua no es la única forma que tiene el DEA de identificar riesgos inaceptables. Un DEA eficaz puede emplear varias formas de conocer los riesgos de la organización. Por ejemplo, puede recibir información de miembros de la actividad de auditoría interna sobre los riesgos significativos que hayan identificado durante sus trabajos de aseguramiento o consultoría. O la organización puede utilizar un proceso de Gestión de Riesgos Empresariales (ERM por sus siglas en inglés) para identificar y supervisar los riesgos significativos, y el DEA puede estar involucrado en ese proceso. Además, el DEA puede crear y mantener una red de comunicación colaborativa con los directores, para estar al tanto de las áreas de riesgos emergentes de la organización. Los DEAs también se deben esforzar por mantenerse informados sobre las tendencias del sector y sobre los cambios normativos, lo que les ayudará a reconocer riesgos potenciales y emergentes.

Independientemente de como se identifique el riesgo inaceptable, si el DEA reconoce que el riesgo está en un nivel tan alto que la organización normalmente no lo toleraría, y si cree que el riesgo no está siendo mitigado para situarlo en un nivel aceptable, entonces está obligado a comunicar esta situación a la alta dirección. Con carácter previo a esa comunicación, el DEA habitualmente tratará esta cuestión con los miembros de la Dirección responsable del área del riesgo de que se trate, para compartir los aspectos que les preocupen, comprender la perspectiva de la Dirección y acordar la forma de subsanar el riesgo. Sin embargo, si no se llega a ningún acuerdo, el DEA debe escalar el problema a la alta dirección. Y, después de mantener con ella un debate similar, si el riesgo continúa sin ser subsanado, deberá comunicar el problema al Consejo. Entonces, corresponderá al Consejo decidir sobre como resolver este asunto con la Dirección responsable del riesgo en cuestión.

El DEA emplea su juicio profesional para determinar como y a quién comunicar estas cuestiones de la forma mejor y más rápida, teniendo en cuenta el tipo del asunto que tenga que ser comunicado, la urgencia, las potenciales ra-

mificaciones y las políticas que pueda haber sobre la cuestión. Por ejemplo, en el caso de que una ley o regulación haya podido ser incumplida, ¿debería el DEA consultar al director de la asesoría jurídica? Y ¿debería ser comunicado el riesgo en privado a un miembro de la alta dirección o debería informarse sobre él en una reunión con directivos de distintos departamentos a la que asistan muchos especialistas en la materia?

Esta Norma aplica a los riesgos que sean muy relevantes que, según la opinión del DEA, deban estar dentro del nivel de tolerancia de la organización, entre los que podemos incluir:

- Los que puedan dañar la reputación de la organización.
- Los que podrían dañar a las personas.
- Los que puedan tener como consecuencia sanciones importantes, limitaciones a las actividades de negocio, u otras penalizaciones financieras o mercantiles.
- Errores materiales.
- Fraudes u otros actos ilegales.
- Obstáculos significativos para lograr los objetivos estratégicos.

Consideraciones para demostrar conformidad

La evidencia de conformidad puede encontrarse en actas de reuniones en las que se haya tratado un problema relacionado con un riesgo significativo con el equipo formado por los directores ejecutivos, el Consejo o con el comité de riesgos. Si el DEA ha informado sobre una situación de riesgo inaceptable en una sesión con un solo responsable o durante una conversación privada, se puede utilizar un memorando que se añada al expediente para documentar los pasos que se han dado para alertar a la Dirección y al Consejo sobre la situación detectada. También se puede contemplar dentro de las políticas del Manual de auditoría interna que una indicación indirecta de conformidad sea suficiente para cumplir los requisitos de esta Norma y el proceso de reporte de la organización.