Septiembre 5, 2014
Volumen 21, No. 23

Heads Up

En este número:

Desafíos relacionados con la implementación y prácticas líderes de *Control Interno – Estructura Conceptual Integrada* de COSO

Por *Jennifer Burns, Deloitte LLP; y Sandy Herrygers, Deloitte & Touche LLP*

Introducción

En respuesta a la confluencia de declaraciones regulatorias y actividades de emisión del estándar (e.g., por COSO,[1] la PCAOB, y la SEC), compañías, comités de auditoría, auditores, y reguladores han incrementado su centro de atención puesto en el control interno sobre la información financiera (CIIF). Las declaraciones de representantes de la SEC y de la PCAOB han enfatizado que las compañías y los auditores deben incrementar la atención que le prestan al control interno. Por ejemplo, en un discurso dado en diciembre de 2013, Brian Crouteau, SEC Deputy Chief Accountant, señaló lo siguiente:

> En la medida en que mantenemos o incrementamos la intensidad de nuestra atención puesta en el [CIIF]… Sigo convencido de que al menos algunos de los hallazgos de inspección de la PCAOB relacionados con las auditorías del control interno sobre la información financiera son probables indicadores de problemas similares con las evaluaciones que del CIIF hacen la administración, y por lo tanto potencialmente también son indicadores de riesgo de debilidades materiales no identificadas [y] continuaré preguntando si todas las debilidades materiales están siendo identificadas de la manera apropiada… Esto podría deberse ya sea a que las deficiencias no están siendo identificadas en primer lugar o de otra manera deberse a que la severidad de las deficiencias no estén siendo evaluadas de la manera apropiada.

Y en un discurso dado en marzo de 2014, Jeannette Franzel, PCAOB Board Member, anotó:

> Actualmente nos encontramos en una "tormenta perfecta" en el área del control interno sobre la información financiera, lo cual demanda acción efectiva de todos los participantes en la cadena de la información financiera y de la auditoría. La administración, los auditores internos, y los auditores externos estarán navegando la "*Control Interno – Estructura Conceptual Integrada"* del Committee of Sponsoring Organizations of the Treadway Commission (COSO) al mismo tiempo que las firmas de auditoría externa están dando pasos para responder a los hallazgos de inspección de la PCAOB asociados con sus auditorías del control interno.

Desde que COSO emitió en mayo de 2013 su *Control Interno – Estructura Conceptual Integrada* (la "Estructura Conceptual de 2013"),[2] los equipos de administración han estado dando los pasos para implementarla de acuerdo con la orientación para la implementación emitida por COSO.

Desde que COSO emitió la Estructura Conceptual de 2013, los equipos de administración han estado dando los pasos para implementarla de acuerdo con la orientación para la implementación emitida por COSO.

Si bien los componentes del control interno de la Estructura Conceptual de 2013 (i.e., ambiente de control, valoración del riesgo, actividades de control, información y comunicación, y actividades de monitoreo) son los mismos que los de la Estructura Conceptual de 1992, la nueva estructura requiere que las compañías valoren si los 17 principios están presentes y funcionando al determinar si su sistema de control interno es efectivo. Además, los 17 principios están respaldados por puntos de atención, los cuales son consideraciones importantes en la evaluación que la compañía hace del diseño y la efectividad de la

[1] COSO es el Committee of Sponsoring Organizations of the Treadway Commission. En mayo de 2013, COSO actualizó su *Control Interno – Estructura Conceptual Integrada*, que fue emitida originalmente en el año 1992.
[2] La Estructura Conceptual de 2013 y las Herramientas Ilustrativas pueden ser compradas en la AICPA Store. En el sitio web de COSO está disponible gratis el resumen ejecutivo de la Estructura Conceptual de COSO.

operación de los controles para abordar los principios. Esos desafíos orientarán la necesidad de un proceso diferente de evaluación de las deficiencias. Desde la perspectiva del CIIF, cuando uno o más de los 17 principios de la Estructura Conceptual de 2013 no está presente y funcionando, existe una deficiencia importante, que es igual a una debilidad material según la Sección 404 de la Ley Sarbanes-Oxley de 2002 ("SOX 404").[3] Además, es importante reconocer que los controles a nivel-de-entidad generalmente están relacionados indirectamente con los estados financieros y por consiguiente son más difíciles de evaluar cuantitativamente que los controles directos a nivel-de-procesos. Los controles a nivel-de-entidad típicamente también están más personalizados al tamaño, complejidad, y perfil de riesgo de la organización y por consiguiente su evaluación es más cualitativa.

Si bien las compañías usan la estructura conceptual de COSO en vinculación con el cumplimiento SOX 404 y el CIIF, ha surgido una tendencia importante en relación con la extensión de su aplicación a otros riesgos regulatorios y operacionales. En general, las compañías tienen tanto el impulso como la oportunidad para usar su implementación de la Estructura Conceptual de 2013 también significa re-evaluar objetivamente sus controles internos, identificar las áreas de mejoramiento y sinergia, e identificar las oportunidades para administrar de manera sistemática los riesgos regulatorios, operacionales, y de presentación de reportes.

Este *Heads Up* discute los problemas relacionados con la oportunidad de la implementación de la Estructura Conceptual de 2013 así como también los desafíos para la implementación y las prácticas líderes de CIIF. También proporciona observaciones y perspectivas en relación con la aplicación de la Estructura Conceptual de 2013 para los propósitos de cumplimiento operacional y regulatorio. Para una vista de conjunto de la Estructura Conceptual vea el *Heads Up* de junio 10. 2013, de Deloitte.

Oportunidad para la implementación

Han surgido preguntas acerca de si en el año corriente las compañías están requeridas a adoptar la Estructura Conceptual de 2013. COSO proporcionó orientación para la transición que recomienda la adopción de la Estructura Conceptual de 2013 para diciembre 15, 2014, tiempo en el cual la Estructura Conceptual de 1992 será reemplazada. La SEC requiere que las compañías usen una "estructura de control que sea reconocida, confiable."[4]

Este año la mayoría de las compañías están avanzando en la adopción de la Estructura Conceptual de 2013, de acuerdo con la orientación para la transición emitida por COSO.

Este año la mayoría de las compañías están avanzando en la adopción de la Estructura Conceptual de 2013, de acuerdo con la orientación para la transición emitida por COSO. Han citado una serie de razones para hacerlo, incluyendo:

- Las juntas, los comités de auditoría, y los equipos de la administración desean demostrar el uso de la última orientación y las prácticas líderes derivadas de COSO.
- Los principios y puntos de atención usados en la Estructura Conceptual del 2013 proporcionan una explicación más clara de los componentes del control interno (ambiente de control, valoración del riesgo, actividades de control, información y comunicación, y actividades de monitoreo) que la Estructura Conceptual anterior. La evaluación del estado del control interno de la organización contra los principios y puntos de atención pueden proporcionar valor a las organizaciones mediante racionalizar y mejorar la efectividad de los sistemas de control interno (i.e., mitigación de los riesgos).
- Las compañías no desean ser percibidas como que estén detrás de sus pares de la industria, quienes es probable que estén adoptando en el año corriente.
- La adopción de la Estructura Conceptual de 2013 de acuerdo con la orientación para la transición emitida por COSO puede ser esperada por inversionistas, banqueros, reguladores de la industria, y otros *stakeholders*.

En este momento esas compañías tienen en marcha su valoración de la brecha, con la meta de tener la valoración de la brecha y la prueba inicial del CIIF completada para el final del tercer trimestre. Esto deja el cuarto trimestre para remediación de las brechas del control interno y para remediación. Esta programación ayuda a la administración a asegurar a final de año un proceso eficiente y efectivo de atestación del CIIF.

Nosotros hemos observado algunos casos en los cuales compañías han decidido continuar aplicando la

[3] La Estructura Conceptual de 2013 contiene la siguiente orientación nueva sobre una deficiencia importante en el control interno: "Cuando existe una deficiencia importante, la organización no puede concluir que ha satisfecho los requerimientos para un sistema efectivo de control interno. Existe une deficiencia importante en el sistema de control interno cuando la administración determina que un componente y uno o más de los principios relevantes no está presente o funcionando o que los componentes no están operando juntos. Una deficiencia importante en un componente no puede ser mitigada a un nivel aceptable por la presencia y el funcionamiento de otro componente. De manera similar, una deficiencia importante en un principio relevante no puede ser mitigada a un nivel aceptable por la presencia y el funcionamiento de los otros principios."

[4] SEC Exchange Act Rule 13a-15(c).

Estructura Conceptual de 1992 para el año calendario corriente. Sus decisiones generalmente se basaron en consultas con una serie de *stakeholders*, incluyendo la junta, el comité de auditoría, y los auditores internos y externos. Independiente de su decisión, las compañías deben revelar de manera clara en su valoración anual del CIIF si usaron la Estructura Conceptual de 1992 o la Estructura Conceptual de 2013.

Nota del editor: Según las reglas de la SEC (17 CFR Section 240.13a-15(c)), la Estructura Conceptual en la cual se base la evaluación que la administración haga del control interno sobre la información financiera del emisor tiene que ser una estructura de control que sea reconocida, confiable, que esté establecida por un cuerpo o grupo que haya seguido procedimientos de debido proceso, incluyendo la distribución amplia de la estructura para comentario del público."

El Estándar de Auditoría 5 de la PCAOB[5] establece que el "para realizar su auditoría del control interno sobre la información financiera auditor debe usar la misma estructura de control, reconocida y confiable, que la administración use para su evaluación anual de la efectividad del control interno sobre la información financiera de la compañía." Como resultado, la oportunidad de cuándo el auditor hace la transición hacia la Estructura Conceptual del 2013 para auditar el CIIF dependerá de la oportunidad de la transición de la compañía. Nosotros consideramos que una manera consistente con el enfoque para revelar la estructura conceptual exacta de COSO usada en la valoración del CIIF que realiza la administración, sería apropiado señalar en el reporte del auditor la estructura conceptual exacta usada.

Independiente de su decisión, las compañías deben revelar de manera clara en su valoración anual del CIIF si usaron la Estructura Conceptual de 1992 o la Estructura Conceptual de 2013.

Desafíos relacionados con la implementación y prácticas líderes

En la medida en que las compañías abren camino en el proceso de implementación, en el cumplimiento con la nueva estructura algunas pueden recurrir a un enfoque de lista de verificación. Para desbloquear completamente el valor que puede lograrse mediante la adopción de la Estructura Conceptual de 2013, la administración debe dar un paso atrás y evaluar cómo está abordando los riesgos de su organización a la luz del tamaño, la complejidad, el alcance global, y el perfil del riesgo de la compañía. En la complementación que las compañías hacen de la Estructura Conceptual de 2013, hay una diferencia entre hacer lo mínimo para abordar los principios de la estructura y hacer lo *correcto* para abordar de manera efectiva los principios. Las compañías que escogen hacer lo *correcto* desbloquearán el valor, reducirán el riesgo de fraude, evitarán sorpresas con la información financiera, y respaldarán el desempeño sostenido del negocio en el largo plazo.

La tabla que se presenta a continuación resume los principios de la Estructura Conceptual del 2013 por componente, y los parágrafos que siguen discuten los desafíos comunes que las compañías están experimentando cuando trabajan para implementar la estructura para propósitos SOX 404, así como también las prácticas líderes en el control interno que pueden ayudar a abordar los desafíos de la implementación.

Componentes del control y principios resumidos				
Ambiente de control	**Valoración del riesgo**	**Actividades de control**	**Información y comunicación**	**Actividades de monitoreo**
1. Demuestra compromiso para con la integridad y los valores éticos. 2. Ejerce la responsabilidad de la vigilancia. 3. Establece estructura, autoridad, y responsabilidad 4. Demuestra compromiso para con la competencia. 5. Hace forzosa la *accountability.*	6. Especifica objetivos confiables. 7. Identifica y analiza el riesgo. 8. Valora el riesgo de fraude. 9. Identifica y analiza el cambio importante.	10. Selecciona y desarrolla las actividades de control. 11. Selecciona y desarrolla controles generales sobre la tecnología. 12. Despliega a través de políticas y procedimientos.	13. Usa información de calidad, relevante 14. Comunica internamente 15. Comunica externamente	16. Dirige evaluaciones continuas y/o separadas 17. Evalúa y comunica las deficiencias.

[5] PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements*.

Demuestra un programa efectivo de ética (Principios 1, 2)

En la medida en que las organizaciones evolucionan y cambian, sus programas de ética pueden volverse rancios o inadecuados, y el cumplimiento con ellos puede volverse ejercicios de “verifique la caja.” Además, si bien muchas organizaciones han establecido programas de ética, no siempre abordan la información financiera o el CIIF. El código de conducta de Enron era ampliamente reconocido como de clase mundial en el momento del escándalo de fraude que en últimas llevó al final de la compañía y afecto a muchos. En los casos materiales de fraude, a menudo hay otros mensajes alternativos y en conflicto además de los relacionados con la integridad y los valores éticos. En muchos casos, la presión sobre las ganancias y las personalidades que entregan mensajes alternativos son tan fuertes que sobrepasan el mensaje de la organización sobre la integridad y los valores éticos. El tono que permea tales organizaciones puede convertirse en un factor en las decisiones de los empleados para cometer y racionalizar el fraude que de otra manera no cometerían. Cuando se trata del tono desde lo alto, las acciones hablan más que las palabras.

Cuando se trata del tono desde lo alto, las acciones hablan más que las palabras.

Desafíos comunes de la implementación	Prácticas líderes de control interno
En la medida en que las organizaciones evolucionan y cambian, sus programas de ética pueden volverse rancios o convertirse en ejercicios de “verificación de la caja.” Además, si bien muchas organizaciones han establecido programas de ética, no siempre se centran en integrar sus expectativas relacionadas con la información financiera y el CIIF. Las organizaciones a menudo: • Carecen de un programa formal continuo de ética, que incluya mensajes centrados en la importancia de la información financiera confiable y del CIIF. • Carecen de vigilancia de sus programas de ética por parte del comité de auditoría. • Son negligentes en revisar el código de conducta por lo que se refiere a pertinencia o actualización en respuesta a su entorno cambiante, según se necesite. • Reciben refuerzo inadecuado de parte de la administración alta y mediana o no tienen programas continuos de entrenamiento que de manera específica incluyan la información financiera y el CIIF. • No tienen materiales y recursos relevantes y fácilmente disponibles para los empleados o no están en los lenguajes relevantes. • No comunican las expectativas de integridad y valores éticos a terceros y proveedores de servicios tercerizados. • Tienen programas inadecuados de entrenamiento continuo sobre ética, que incluyan la información financiera. • No realizan una valoración periódica de la efectividad. • Fallan en implementar de manera suficiente y monitorear el programa de ética en una adquisición. • Fallan en considerar de manera suficiente los riesgos para la ética efectiva, incluyendo la resistencia cultural, social, o del mercado ante la ética y la integridad (e.g., ciertos mercados emergentes en los cuales los sobornos pueden ser percibidos como una práctica aceptable de negocios).	*Ambiente de control:* • La administración, bajo la dirección y vigilancia del comité de auditoría, mantiene un programa continuo de ética con énfasis en la información financiera confiable y el CIIF. • La administración en todos los niveles emite comunicaciones para reforzar la importancia de una cultura ética fuerte, que incluyan temas relacionados con información financiera y CIIF. • La junta de directores (comité de auditoría) vigila la definición y creación de un código de conducta para establecer estándares y expectativas relacionados con integridad y valores éticos. • El código de conducta es proporcionado a y reconocido por los nuevos empleados cuando comienzan y luego anualmente. • El código de conducta es proporcionado a y reconocido por terceros. • La entidad proporciona varios protocolos para reportar el comportamiento no-ético relacionado con información financiera y CIIF. • El comportamiento no-ético relacionado con información financiera y CIIF es evaluado y resuelto de una manera oportuna. • La administración evalúa las tendencias en el volumen o la naturaleza del comportamiento ético reportado y determina si dar pasos para mejorar las acciones de remediación en relación con el programa de ética. • La administración realiza valoraciones periódicas de la ética, incluyendo auditorías de la ética de terceros. • Las violaciones del código de conducta son abordadas de manera oportuna. *Información y comunicación:* • El programa de ética de la entidad ofrece múltiples canales mediante los cuales el comportamiento no-ético puede ser reportado por los empleados internos. • El programa de ética de la entidad ofrece canales directos mediante los cuales el comportamiento no-ético de terceros puede ser reportado.

Valoración del riesgo, que incluye la realización de una valoración efectiva del riesgo de fraude (Principios 7, 8)

La atención de la administración ante la valoración del riesgo puede estar más centrada en los riesgos operacional o regulatorio que en los riesgos de la información financiera; y en el contexto de la información financiera, puede estar más centrada en la salvaguarda de activos y en el fraude, tal como el robo de inventarios o la presentación fraudulenta de reportes sobre los gastos (lo cual generalmente representa solo entre el 3 y 4 por ciento de los fraudes materiales actualmente identificados[6]), que en el riesgo de información financiera fraudulenta. La identificación cuidadosa de los riesgos de fraude de la entidad, particularmente cuando existen presiones de ganancias y programas agresivos de incentivos de compensación, es una parte importante de la valoración del riesgo de fraude. Además, como parte de la valoración del riesgo de fraude la administración a menudo no considera adecuadamente los riesgos específicos de la industria y los potenciales esquemas de fraude. Por ejemplo, el potencial para que la administración eluda el control interno y las áreas de información financiera que involucran juicio y estimados importantes debe ser un área específica de atención en la valoración del riesgo de fraude relacionado con el CIIF.

Dado que la valoración del riesgo apuntala el diseño y la implementación de los controles, un proceso incompleto o inefectivo de valoración del riesgo puede tener un efecto importante en la efectividad del CIIF. Además, los errores o deficiencias importantes (individualmente o en el agregado) pueden señalar que los principios relacionados con el componente valoración del riesgo no eran efectivos.

La identificación cuidadosa de los riesgos de fraude de la entidad, particularmente cuando existen presiones de ganancias y programas agresivos de incentivos de compensación, es una parte importante de la valoración del riesgo de fraude.

Desafíos comunes de la implementación	Prácticas líderes de control interno
En la medida en que las organizaciones evolucionan y cambian, sus procesos de valoración del riesgo pueden volverse rancios, y hacer actualizaciones, si se hacen, puede convertirse en un ejercicio de "verificación de la caja." Además, la valoración del riesgo de la entidad puede centrarse en materias operacionales o regulatorias sin adecuadamente tener en cuenta los riesgos relacionados con la información financiera y con el CIIF. Además, con relación a las valoraciones del riesgo de fraude, la entidad puede: • No considerar los tipos relevantes de fraude cuando realice la valoración del riesgo (i.e., información financiera fraudulenta, uso indebido de activos). • No considerar las maneras como la información financiera fraudulenta podría ocurrir, incluyendo: o Sesgo de la administración (e.g., en la selección de los principios de contabilidad). o Grado de estimados y juicios en la presentación de reportes externos. o Esquemas de fraude y escenarios comunes para los sectores de industria y para los mercados en los cuales la entidad opera. o Incentivos que puedan motivar el comportamiento fraudulento. o Naturaleza de la tecnología y capacidad de la administración para manipular la información. o Transacciones inusuales o complejas sujetas a influencia importante de la administración. o Vulnerabilidad para que la administración eluda y esquemas potenciales para pasar por alto las actividades de control existentes.	*Valoración del riesgo* • Anualmente la entidad revisa y actualiza su valoración del riesgo: o Los riesgos relevantes para los propósitos de la presentación de reportes externos son discutidos, revisados según sea necesario con input proveniente de los administradores funcionales y de componente claves. o Son identificadas las respuestas a cada uno de los riesgos relevantes. • La valoración del riesgo de fraude es realizada o actualizada anualmente para identificar los potenciales esquemas de fraude asociados con la presentación de reportes externos, teniendo en cuenta el input proveniente de los administradores funcionales y de componente claves. • Los resultados de la valoración del riesgo de fraude son discutidos con el comité de auditoría. *Actividades de control:* • La entidad selecciona las actividades de control que mitigan los riesgos identificados en la valoración del riesgo (también teniendo en cuenta la valoración del riesgo de fraude), incluyendo las actividades de control relacionadas con el entorno de TI.

[6] See *Ten Things About Financial Statement Fraud*, de Deloitte.

Desafíos comunes de la implementación	Prácticas líderes de control interno
• Considera de manera inapropiada el riesgo de fraude como opuesto al riesgo inherente. • No vuelve a evaluar periódicamente (e.g., anualmente) el riesgo de fraude y cuando ocurren cambios importantes en la entidad o en su entorno externo. • No considera los riesgos con relación a las actividades relevantes realizadas por proveedores de servicios tercerizados. No revisa, con el comité de auditoría, los resultados de la valoración del riesgo de fraude; o el comité de auditoría puede no desafiar de manera efectiva la valoración que la administración haga de los riesgos de fraude, incluyendo desafiar el riesgo de que la administración eluda los controles.	

Si bien las compañías típicamente tienen procesos robustos de cambio para los sistemas de TI, a menudo carecen de procesos definidos para administrar los otros cambios que podrían afectar la información financiera.

Identificación de los cambios y factorización apropiada de ellos en el proceso de valoración del riesgo (Principio 9)

El cambio crea riesgos; por consiguiente, la administración debe implementar oportunamente procesos que le permitan identificar y evaluar los cambios que afectan la organización. Si bien las compañías típicamente tienen procesos robustos de cambio para los sistemas de TI, a menudo carecen de procesos definidos para administrar los otros cambios que podrían afectar la información financiera, los cuales pueden originarse externamente (e.g., nuevos requerimientos de contabilidad) o internamente (e.g., contabilidad para transacciones no-rutinarias o complejas, rediseño o centralización de procesos de negocio, o tercerización de los proveedores de servicios). Algunas veces los roles y las responsabilidades asociados con esos cambios y los controles relacionados se distribuyen a través de múltiples partes y no son monitoreados de manera efectiva. Además, muchas compañías sub-enfatizan la importancia de proporcionarle entrenamiento al empleado sobre esos nuevos roles y responsabilidades durante el período de transición, por consiguiente creando un riesgo de control interno inefectivo.

En la práctica, las debilidades materiales frecuentemente están relacionadas con esos cambios y resultan en parte tanto de una valoración inadecuada de los riesgos relacionados como de despliegue y monitoreo insuficientes de los controles que de manera directa abordan los riesgos.

Desafíos comunes de la implementación	Prácticas líderes de control interno
• Carencia de valoración del riesgo reflexiva, detallada, que involucre las personas apropiadas (y por lo tanto falla en identificar y diseñar los controles apropiados). • Falla en que la administración apropiadamente valore la necesidad de competencia adicional o que actúe en la necesidad de involucrar otros, incluyendo terceros. • Falla en considerar y monitorear los cambios en el personal clave. • No-confiabilidad de los datos usados para evaluar o contabilizar las transacciones o eventos no-rutinarios (e.g., datos no sujetos a los controles normales de calidad pueden ser inexactos o incompletos). • Potencial incrementado para que la administración eluda (los incentivos o presiones pueden crear sesgo). • Carencia de consideración o de evaluación objetiva de los eventos o tendencias externos y su impacto en el CIIF de la entidad. • Carencia de comunicación y coordinación entre las funciones (e.g., operaciones, impuestos, e información financiera).	*Ambiente de control:* • Las líneas de presentación de reportes y las responsabilidades afectadas por los cambios o eventos son evaluadas y actualizadas. • La entidad monitorea las competencias relacionadas con la información financiera externa y el CIIF. *Valoración del riesgo:* • La administración (con input de la administración funcional o de componente, terceros especialistas, o ambos) determina si un cambio o evento da origen a riesgos nuevos o modificados, incluyendo los relacionados con fraude. *Actividades de control:* • En respuesta a los riesgos que surjan de cambios o eventos, la administración determina si (1) se necesitan nuevos controles o (2) los riesgos son abordados adecuadamente por los controles existentes (e.g., controles para la identificación y evaluación de términos de contratos complejos o no-rutinarios). • Controles sobre la aplicación de los US-GAAP.

Desafíos comunes de la implementación	Prácticas líderes de control interno
	• Controles sobre el cálculo del impacto de un cambio o evento (incluyendo cualquier IPE[7]). • Sistema de implementación de los controles del cambio. • Las políticas y los procedimientos son actualizados para reflejar el cambio o evento, según sea aplicable. *Información y comunicación:* • Las fuentes de información son identificadas, y canales de comunicación son establecidos, para facilitar la identificación oportuna de los cambios o eventos que puedan ser relevantes para el CIIF. *Actividades de monitoreo:* • Auditoría interna realiza oportunamente evaluaciones separadas de las actividades de control afectadas por los eventos o transacciones nuevos o no-rutinarios. El programa de certificación SOX requiere confirmación de que se ha proporcionado toda la información relevante.

Segregación de obligaciones (Principios 10, 11)

Las deficiencias en la segregación de obligaciones han sido una causa raíz de debilidades materiales y de actos materiales de fraude.

Muchos equipos de administración y juntas con razón se preocupan por el riesgo de que los empleados se coludan para cometer fraude. Sin embargo, la falla de la administración para segregar las obligaciones de la manera apropiada a través de los múltiples sistemas o procesos manuales genera el riesgo único de que los empleados serán capaces de cometer fraude u ocultar actividad fraudulenta sin colusión. La oportunidad para cometer fraude y la posibilidad de su ocurrencia son mucho mayores cuando la colusión no es necesaria, así como cuando las obligaciones no están segregadas de la manera apropiada. Esto es particularmente verdadero en la era de sistemas grandes de planeación de recursos de la empresa [ERP = enterprise resource planning] que individualmente procesan un número importante de transacciones financieras. Los solos controles de detección, que pueden ser imprecisos y más operacionalmente centrados, son, por su naturaleza, a menudo inefectivos en prevenir o detectar el fraude, especialmente dado que muchos actos materiales de fraude no son el resultado de una sola transacción material y solo se vuelven materiales en el agregado con el tiempo.

Las deficiencias en la segregación de obligaciones han sido una causa raíz de debilidades materiales y de actos materiales de fraude. Los siguientes son unos pocos ejemplos de numerosas revelaciones del control interno de compañías públicas reportados durante los últimos 10 años acerca de las debilidades materiales que involucran tales deficiencias:

- “De manera específica, la compañía identificó deficiencias con relación a los controles sobre obligación de obligaciones, acceso restringido, cambios a datos maestros de vendedor y cliente, nivel de transacción y cierre financiero que son agregados a una debilidad material en el control interno sobre la información financiera.”
- “Hay debilidades materiales relacionadas con la segregación inefectiva de obligaciones y los controles generales de tecnología de la información para restringir el acceso del usuario y para revisar el desarrollo, la administración del cambio, y el mantenimiento de las aplicaciones del sistema.”
- “[La falla en realizar la prueba adecuada de aceptación del usuario antes de implementar una aplicación de ERP] resultó en una segregación inadecuada de obligaciones y controles inadecuados sobre la aprobación de ciertos asientos de diario con base en los roles asignados a los usuarios del ERP:”
- “[Las debilidades materiales identificadas en la valoración que realiza la administración incluyen la] ausencia de apropiada segregación de obligaciones dentro de cuentas y procesos importantes y controles inefectivos sobre la vigilancia que realiza la administración, incluyendo programas y controles anti-fraude.”
- “Las debilidades materiales en el control interno sobre la información financiera [estuvieron]

[7] Información producida por la entidad [Information produced by the entity].

relacionadas con… carencia de segregación de obligaciones y debilidades alrededor de la revisión oportuna y consistente de los estados financieros por parte de la administración."

Desafíos comunes de la implementación	Prácticas líderes de control interno
• Las obligaciones pueden no estar segregadas de la manera apropiada a través de los sistemas múltiples o procesos manuales (e.g., acceso tanto a los libros auxiliares como al libro mayor). • El acceso al sistema de TI puede dar origen a problemas importantes o materiales a causa de la incapacidad para controlar los cambios a la funcionalidad del sistema o a los datos (e.g., acceso para hacer y mover un cambio). Esto puede menoscabar la confianza del usuario en (1) controles automatizados del sistema, (2) reportes financieros o de control, y (3) la validez de los datos fuente para las transacciones en los sistemas relevantes. • Los controles para asegurar la segregación de obligaciones pueden no ser forzados adecuadamente a nivel global, especialmente en localizaciones más pequeñas o más descentralizadas. • Los controles de mitigación (e.g., revisiones de nivel alto de los resultados financieros) pueden no ser suficientemente precisos para mitigar el riesgo asociado con la segregación de obligaciones.	*Ambiente de control:* • Controles relacionados con la vigilancia que el comité de auditoría hace respecto del riesgo de que la administración eluda los controles. • Controles que valoran y monitorean la magnitud de las presiones para que la administración logre objetivos específicos. *Valoración del riesgo:* • Controles relacionados con el desempeño de una valoración efectiva del riesgo de fraude, que tengan en cuenta oportunidades, racionalizaciones, e incentivos o presiones para cometer fraude. *Actividades de control:* • Controles que definan y aborden la segregación de obligaciones incompatibles. • Controles que mitiguen el riesgo asociado con obligaciones incompatibles que no puedan estar siendo segregadas. • Controles que identifiquen los controles de TI para los sistemas relevantes que apoyen el CIIF, incluyendo: o Controles a la infraestructura de tecnología. o Controles a la administración de la seguridad. o Controles a adquisición, desarrollo, y mantenimiento de tecnología. *Actividades de monitoreo:* • Monitoreo de controles que periódicamente identifiquen, evalúen, y remedien los conflictos en el acceso del usuario que impidan la segregación de obligaciones. • Monitoreo de controles que periódicamente evalúen el acceso del personal de TI a los sistemas relacionados con CIIF.

Diseño efectivo de controles de revisión de la administración (Principios 10, 12, 13, 16)

El diseño que la administración hace de procesos y controles típicamente consiste de controles tanto preventivos como de detección (e.g., controles de revisión de la administración). Sin embargo, la administración puede estar confiando excesivamente en tales controles para propósitos SOX 404 dado que a menudo no son suficientemente precisos por sí mismos para detectar declaraciones equivocadas materiales, particularmente errores más pequeños o sistémicos que podrían con convertirse en una cantidad material. Algunas veces hay un sesgo operacional en esos controles (e.g., controles que comparan lo actual con el presupuesto); si bien un control puede identificar un error potencial cuando ocurre una variación, puede no estar diseñado para identificar errores cuando no exista una variación. Por esta razón, el diseño de controles de revisión de la administración y la evidencia de su efectividad operacional han sido un área importante de atención para administración, auditores, y reguladores, particularmente con relación a los controles de revisión de la administración relacionados con estimados y la aplicación de los US GAAP a transacciones o eventos nuevos o infrecuentes.

Cuando selecciona los controles para mitigar los riesgos para propósitos de CIIF, la administración valora la precisión de la revisión que la administración hace del control mediante considerar varios factores.

Desafíos comunes de la implementación	Prácticas líderes de control interno
La administración puede confiar excesivamente en un control de revisión de la administración que no sea suficientemente preciso, tal y como ocurre en los siguientes ejemplos: • El propósito del control es solo explicar variaciones, no valorar si las cantidades registradas son apropiadas. • Dado que los estándares y las expectativas del desempeño no eran claros, el control no operó como se tuvo la intención. • El revisor no evalúa los datos subyacentes o los soportes a un nivel suficientemente detallado o desagregado. • La confiabilidad de los datos (reporte) usados en los controles no fue considerada de la manera apropiada por el usuario. • El revisor no tiene una suficiente base de conocimiento y respaldo para evaluar los datos o identificar errores. • Los criterios para la investigación usados por el revisor son demasiado altos, no están bien definidos, o no son seguidos de manera consistente. • El revisor raramente hace preguntas o no es suficientemente diligente acerca del seguimiento para determinar si han ocurrido errores. • La evidencia de la conducta de los controles es insuficiente para permitir que la función de monitoreo determine de manera efectiva lo que el revisor consideró y la base para las conclusiones del revisor. • Hay evidencia insuficiente respecto de las consideraciones de la administración según los US GAAP (e.g., la evaluación que el auditor hace de los US GAAAP tiene en cuenta materias no abordadas por la administración).	*Ambiente de control:* • Todos los propietarios del control, incluyendo el personal de nivel administrativo responsable por los controles de revisión de la administración, son hechos responsables por el desempeño que no está a la altura de las expectativas. *Actividades de control:* • Cuando selecciona los controles para mitigar los riesgos para propósitos de CIIF, la administración valora la precisión de la revisión que la administración hace del control mediante considerar varios factores, que incluyen los siguientes: o El propósito del control. o La naturaleza e importancia del riesgo que el control está diseñado para mitigar. o El nivel en la organización en el cual el control es ejecutado (e.g., saldo de cuenta, unidad de negocio/localización, o el nivel corporativo sobre una base altamente agregada). o La naturaleza de los datos y reportes usados en el control, incluyendo el nivel de detalle y respaldo. o La confiabilidad de los datos y reportes usados en el control. o Qué tan frecuente y consistentemente es ejecutado el control. o La competencia y el conocimiento necesarios para que el propietario del control ejecute el control de manera efectiva. o Los criterios y procesos usados para investigación. o Si el control depende de otros controles, señalando entonces qué otros controles más precisos deben ser identificados. *Información y comunicación:* • Políticas y procedimientos de control son mantenidos y comunicados en la página web intranet de control interno de la entidad. *Actividades de monitoreo:* • Cada trimestre, los propietarios del control certifican que han ejecutado los controles, por los cuales son responsables, de acuerdo con las políticas y procedimientos establecidos. • Auditoría interna periódicamente realiza una revisión de la efectividad de los controles de revisión de la administración.

Proveedores de servicios tercerizados (Múltiples principios)

Dado el importante incremento que las relaciones de tercerización se han vuelto críticas para la información, los procesos de negocio, y la TI, los controles internos relacionados con los proveedores de servicios tercerizados [OSP = outsourced service providers] se han vuelto críticos. Si bien la mayoría de las compañías tiene en funcionamiento procesos para evaluar los reportes SSAE 16[8] obtenidos de organizaciones de servicio para abordar el componente actividades de control de la Estructura Conceptual de 2013, la mayoría de las

[8] AICPA Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization.

organizaciones usuario carecen de controles formales y auditables para abordar las consideraciones de OSP relacionadas con los otros cuatro componentes de la estructura (e.g., controles sobre la comunicación de expectativas en relación con el código de conducta, responsabilidades, y autoridad; y controles para monitorear los acuerdos y comunicaciones a nivel de servicio). Además, las compañías pueden directamente registrar los asientos de diario importantes basados en los reportes provenientes de las OSP sin mecanismos apropiados de monitoreo para determinar si esos reportes son materialmente exactos y completos. Para la administración es importante establecer controles robustos de monitoreo sobre las OSP. Sin tales controles, podrían darse sorpresas desafortunadas en el año cuando se entreguen los reportes SSAE 16, tales como calificaciones inesperadas del reporte.

Desafíos comunes de la implementación	Prácticas líderes de control interno
• Expectativas de integridad y valores éticas no comunicadas a las OSP. • Carencia de comunicación efectiva de la autoridad y de las políticas de aprobación; y monitoreo inadecuado de los roles delegados a otros, incluyendo las OSP. • Falla en identificar las actividades de control realizadas por las OSP. • Falla en establecer líneas de comunicación con las OSP. • Falla en monitorear las actividades de control realizadas por las OSP.	*Ambiente de control:* • La administración y la junta de directores consideran las OSP cuando establecen estructuras organizacionales, líneas de presentación de reportes, y autoridades y responsabilidades apropiadas. • A las OSP se les proporciona términos contractuales claros y concisos relacionados con las expectativas de la entidad respecto de conducta y desempeño, niveles de competencia, información esperada, alcance de la autoridad delegada, y flujo de comunicación. • La administración evalúa la competencia de las OSP. • La administración evalúa el desempeño de las OSP contra los acuerdos a nivel de servicio u otros estándares acordados. *Valoración del riesgo* • El proceso de valoración del riesgo tiene en cuenta los riesgos que se originan en las OSP, incluyendo los posibles actos de corrupción por las OSP. • La entidad actualiza su valoración del riesgo por los cambios en el negocio, incluyendo las relaciones con las OSP. *Actividades de control:* • La administración identifica (1) los controles relevantes en la OSP, (2) los controles relevantes dentro de la entidad, o (3) ambos. *Información y comunicación:* • Canales de comunicación para reportar el comportamiento no-ético están disponibles para las OSP. • La información obtenida de las OSP que administra procesos de negocio a nombre de la entidad está sujeta a las mismas expectativas de calidad que la información generada internamente por la entidad. *Actividades de monitoreo:* • La entidad monitorea las actividades de la OSP, incluyendo obtener y evaluar los reportes SSAE 16 según sea aplicable (e.g., monitoreo más frecuentes es realizado para las nuevas relaciones de OSP hasta que se alcance un estado estable).

Para la administración es importante establecer controles robustos de monitoreo sobre las OSP.

Calidad de la información (Principio 13)

Declaraciones equivocadas de información financiera pueden resultar de confianza inapropiada en datos o reportes erróneos, lo cual podría ser originado por fallas en el diseño o efectividad operacional relacionada con cualquiera de los siguientes:

- Controles sobre las fuentes de datos (i.e., controles manuales o automatizados).
- Controles sobre interfaces y transferencias de datos.

- Controles generales indirectos de TI [GITC = Indirect general IT controls] que respaldan la confiabilidad e integridad de la información generada por el sistema.

Algunas veces, las compañías ya sea carecen de controles apropiados para abordar los riesgos asociados con información importante de la cual dependen para propósitos SOX 404 o fallan en identificar y probar los controles sobre tal información. Una solución a este problema es asegurar que la administración tenga en funcionamiento controles específicos sobre los datos, incluyendo reportes no generados por el sistema y datos a y desde las OSP. Además, las compañías necesitan mirar más allá de los GITC básicos y también centrarse en los controles a nivel de proceso sobre la información y los datos de la presentación de reportes financieros.

Algunas veces, las compañías carecen de controles apropiados sobre los datos de los cuales dependen para propósitos SOX 404.

Desafíos comunes de la implementación	Prácticas líderes de control interno
• La entidad carece de una estrategia de gobierno de los datos, de políticas, o estándares que definan las expectativas de control por la información. • La falla de que los propietarios y usuarios de la información diseñen o implementen controles sobre datos fuente, lógica de reporte, o parámetros compromete la confiabilidad de la información (i.e., completitud o exactitud). • Los requerimientos de información no han sido actualizados para reflejar el estado actual de la organización (e.g., cambio en estructura de la unidad de negocios y reportes generados por el sistema). • Los canales de comunicación y los controles para la información operacional y regulatoria relevante para el CIIF son inefectivos. • La administración no ha considerado apropiadamente los controles sobre la información proveniente de partes externas (e.g., organizaciones de servicio o expertos de la administración) que sean usados en el CIIF.	*Actividades de control:* • Varias actividades de control son realizadas dependiendo de los datos y reportes específicos. Por ejemplo: o Son establecidos controles automatizados y/o manuales para verificar que la información transaccional (datos fuente) sea válida y exacta (e.g., verificación de la validación del número del vendedor y de la orden de compra). o La administración realiza conciliaciones manuales de la información entre los sistemas para validar la transferencia completa y exacta de la información entre los sistemas de información financiera. o GITC sobre seguridad de la información y el control del programa de cambio son diseñados e implementados para las aplicaciones de la información financiera y la infraestructura relacionada. o Controles de las hojas de cálculo son diseñados e implementados para todas las hojas de cálculo usadas para información financiera externa y CIIF. o La administración implementa controles sobre la información transferida entre la entidad y partes externas (e.g., organizaciones de servicio, clientes, y vendedores). *Información y comunicación:* • La administración establece estrategias de gobierno de los datos, políticas, y estándares para verificar la calidad de la información usada en la información financiera externa y en el CIIF. • La administración respalda el funcionamiento de los controles sobre la integridad de los datos mediante el mantenimiento de la información, incluyendo diagramas de flujo, diagramas de flujo de datos, narrativas de procesos, manuales de procedimientos, y procedimientos de control (e.g., controles sobre la preparación y el mantenimiento de información usada en los controles). *Actividades de monitoreo:* • Cada trimestre, los propietarios del control certifican que han cumplido con la política y el procedimiento establecido para el gobierno de los datos. • Auditoría interna periódicamente realiza pruebas de acuerdo con las políticas y procedimientos de control establecidos.

Evaluación del diseño del control interno (Múltiples principios)

Si el diseño de los controles a nivel de entidad no es evaluado completamente, se pueden pasar por alto las deficiencias en tales controles. Dado los requerimientos para determinar por separado si cada uno de los 17 principios contenidos en la Estructura Conceptual de 2013 está presente y funcionando, los controles a nivel de entidad son controles fundacionales importantes. De acuerdo con nuestra experiencia, la mayoría de las brechas se identifican como resultado de evaluar el diseño de los controles y la capacidad de la administración, los auditores internos, y los auditores externos para probar esos controles más que como resultado de realizar un ejercicio de mapeo (i.e., mapeo de los controles actuales para con la Estructura Conceptual de 2013). Es importante que la administración dirija una evaluación robusta del diseño para mejorar sus controles internos y soportar la atestación de su CIIF.

Desafíos comunes de la implementación	Prácticas líderes de control interno
• Falla en evaluar de la manera apropiada el diseño de, y la capacidad para probar, los controles a nivel de entidad.	• Los siguientes criterios son evaluados en la valoración del diseño de los controles indirectos a nivel de entidad: o Descripción detallada de cómo se espera que el control sea ejecutado. o Cómo el control aborda el(os) centro(s) de atención(s) y el(os) principio(s) relacionados. o Autoridad y competencia del propietario del control. o Frecuencia y consistencia de la operación del control. o Consideraciones de lo apropiado de los criterios usados para investigación (i.e., umbral) y los procesos de seguimiento. o Dependencias de otros controles o datos de respaldo. • Las siguientes son preguntas consideradas y abordadas en relación con la capacidad para probar los controles: o ¿Cómo se probará la efectividad de la operación del control? o ¿Pueden ser probados todos los atributos del control? o ¿Hay suficiente evidencia documentaria, consistentemente disponible, de que el control esté operando?

El uso de la Estructura Conceptual de 2013 para propósitos operacionales y de cumplimiento (además de para el CIIF) es una tendencia creciente entre las compañías.

Uso de la Estructura Conceptual de 2013 para el cumplimiento operacional y regulatorio

El uso de la Estructura Conceptual de 2013 para propósitos operacionales y de cumplimiento (además de para el CIIF) es una tendencia creciente entre las compañías. La implementación de la estructura actualizada proporciona una buena oportunidad, independiente de qué tan maduro pueda ser el sistema de control interno de la compañía, para dar una mirada fresca a los controles internos con el potencial para creación de valor para la organización. Los mejoramientos en la efectividad del sistema de control interno de la compañía pueden conducir a operaciones más eficientes, mayores tasas de cumplimiento, e información administrativa interna más efectiva. Los ejemplos de usos voluntarios de la Estructura Conceptual de 2013 incluyen los siguientes:

- *Cumplimiento regulatorio de la banca* – Si bien la mayoría de las firmas de la banca y de los mercados de capital han usado la estructura conceptual de controles internos de COSO para diseñar su sistema de cumplimiento SOX 404 CIIF, muchas ahora están dando una mirada más amplia a la estructura actualizada. Muchas firmas de la banca y de los mercados de capital están aplicando los principios de la estructura de COSO para diseñar funciones de revisión del aseguramiento de la calidad sobre otras áreas, incluyendo la presentación de reportes operacional y regulatoria. Para más información acerca de las tendencias del cumplimiento en la industria de servicios financieros, vea *In Focus: Compliance Trends Survey 2014*, de Deloitte.

- *Seguridad cibernética* – Toda organización enfrenta una variedad de riesgos cibernéticos

provenientes de fuentes externas e internas. Los riesgos cibernéticos son evaluados contra la posibilidad de que un evento ocurrirá y afectará de manera adversa el logro de los objetivos de la organización.

El Principio 6 en la Estructura Conceptual de 2013 proporciona varios puntos de atención que les dan a las organizaciones perspectiva de cómo evaluar sus objetivos de una manera que podría influir el proceso de valoración del riesgo cibernético.

Dado que la valoración del riesgo cibernético informa las decisiones acerca de las actividades de control que se despliegan contra los sistemas de información y los activos que respaldan los objetivos de la entidad, es importante que la administración principal y otros *stakeholders* críticos dirijan el proceso de valoración del riesgo para identificar qué tiene que ser protegido en alineación con los objetivos de la entidad. Para información adicional, vea *Changing the Game on Cyber Risk*, de Deloitte.

El uso de la Estructura Conceptual de 2013 fuera del contexto de la información financiera puede proporcionar disciplina útil y necesaria para las juntas y para los comités de auditoría cuando aborden el conjunto crecientemente complejo de riesgos que vigilan.

- *Administración de la cadena de suministro* – Como resultado de ciertos riesgos regulatorios y operacionales tales como seguridad de alimentos y producto, minerales del conflicto, y descontento del consumidor con el desempeño del producto, las compañías han incrementado su centro de atención puesto en identificar y administrar de manera proactiva los riesgos en la cadena de suministro. Para muchas compañías los riesgos de la cadena de suministro se están convirtiendo en riesgos estratégicos a nivel de la junta. De acuerdo con ello, muchas compañías están valorando su exposición actual frente al riesgo, implementando estructuras más formales de gobierno, y diseñando enfoques más disciplinados para administrar los riesgos en la cadena de suministro. Esas actividades pueden ayudar a las compañías a posicionar su cadena de suministro como una ventaja competitiva, administrar el riesgo regulatorio, reducir o eliminar sorpresas operacionales, reducir el costo de hacer negocios, y tomar decisiones informadas sobre asignación del capital. Para más información, vea *From Risk to Resilience: Using Analytics and Visualization to Reduce Supply Chain Vulnerability*, de Deloitte.

- *Administración del vendedor* – La aplicación de la Estructura Conceptual de 2013 a los programas de administración del vendedor para las OSP a fin de respaldar sus operaciones y sus objetivos de cumplimento (además de los objetivos de información financiera) puede proporcionar la disciplina necesaria para abordar el conjunto crecientemente complejo de riesgos operacionales y de cumplimiento. Además, esta disciplina puede permitirles a las organizaciones controlar o reducir costos, mitigar riesgos, y dirigir la excelencia del servicio. Como resultado, las compañías están usando los conceptos de la Estructura Conceptual de 2013 para establecer nuevos programas o para mejorar los existentes. Tales mejoramientos incluyen pero no están limitados a:

    - Asegurar que las OSP entienden el compromiso de la administración para con la integridad y los valores éticos.
    - Incorporar, en el proceso de valoración del riesgo de la compañía, los riesgos que se originan en las OSP.
    - Desarrollar procedimientos de monitoreo para los indicadores clave de desempeño relacionados con los acuerdos a nivel de servicio como medios para la identificación de problemas.

- *Administración del cambio* – El Principio 9 de la Estructura Conceptual de 2013 puede ayudar de manera amplia a que la compañía administre de manera efectiva los controles internos relacionados con los cambios operacionales o regulatorios. Las compañías pueden querer considerar desarrollar un proceso para aplicar el principio 9 y los conceptos relacionados cuando se identifiquen cambios importantes, a fin de sostener y continuamente mejorar los controles internos relacionados con el cumplimiento operacional o regulatorio.

Nota del editor: Para ejemplos adicionales en la aplicación de la Estructura Conceptual de 2013 para propósitos operacionales y de cumplimiento, vea *Audit Committee Brief*, de marzo de 2014, de Deloitte.

El uso de la Estructura Conceptual de 2013 fuera del contexto de la información financiera puede proporcionar disciplina útil y necesaria para las juntas y para los comités de auditoría cuando aborden el conjunto crecientemente complejo de riesgos que vigilan. También puede proporcionarle a la administración una estructura consistente y eficiente para definir, implementar, y monitorear su estructura de control y ayudarle a mejorar continuamente sus procesos generales de administración del riesgo.

Suscripciones

Si usted desea recibir *Heads Up* y otras publicaciones de contabilidad emitidas por el Accounting Standards and Communications Group, de Deloitte, por favor regístrese en www.deloitte.com/us/subscriptions.

***Dbriefs* para ejecutivos financieros**

Lo invitamos a que participe en *Dbriefs*, la serie de webcast de Deloitte que entrega las estrategias prácticas que usted necesita para mantenerse en la cima de los problemas que son importantes. Tenga acceso a ideas valiosas e información crítica de los webcast en las series "Ejecutivos Financieros" sobre los siguientes temas:

- Estrategia de negocios e impuestos
- Gobierno corporativo
- Orientando el valor de la empresa
- Información financiera
- Información financiera para impuestos
- Inteligencia frente al riesgo
- Sostenibilidad
- Tecnología
- Transacciones & eventos de negocio

Dbriefs también proporciona una manera conveniente y flexible para ganar créditos de CPE – directo en su escritorio. Únase a *Dbriefs* para recibir notificaciones sobre futuros webcast en www.deloitte.com/us/dbriefs.

Está disponible el registro para este próximo webcast de *Dbriefs.* Use el vínculo para registrarse:

- EITF Roundup: Highlights From the September Meeting (September 23, 2 p.m. (EST)).

Technical Library y US GAAP Plus

[Biblioteca técnica y US GAAP Plus]

Deloitte tiene disponible, sobre la base de suscripción, el acceso a su biblioteca en línea de literatura sobre contabilidad y revelación financiera. Denominada Technical Library: The Deloitte Accounting Research Tool, la biblioteca incluye material de FASB, EITF, AICPA, PCAOB, IASB y SEC, además de los manuales de contabilidad propios de la SEC y los manuales de la SEC y otra orientación interpretativa de la contabilidad y de la SEC.

Actualizada cada día de negocios, Technical Library tiene un diseño intuitivo y un sistema de navegación que, junto con sus poderosas características de búsqueda, le permiten a los usuarios localizar rápidamente información en cualquier momento, desde cualquier computador. Además, los suscriptores de Technical Library reciben *Technically Speaking*, la publicación semanal que resalta las adiciones recientes a la librería. Para más información, incluyendo detalles sobre la suscripción y una demostración en línea, visite www.deloitte.com/us/techlibrary.

Además, asegúrese de visitar US GAAP Plus, nuestro nuevo sitio web gratis que destaca noticias de contabilidad, información, y publicaciones con un centro de atención puesto en los US GAAP. Contiene artículos sobre las actividades de FASB y actualizaciones a la *FASB Accounting Standards Codification*™ así como también desarrollos de otros emisores del estándar y reguladores de los Estados Unidos, tales como PCAOB, AICPA, SEC, IASB y el IFRS Interpretations Committee. ¡Dele un vistazo hoy!

Esta es una traducción al español de la versión oficial en inglés de **Heads Up – September 5, 2014 – Volume 21, Issue 23 – Challenges and Leading Practices Related to Implementing COSO's *Internal Control – Integrated Framework* –** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.