Deloitte.

Junio 10, 2013

Volumen 20, No. 17

Heads Up

En este número:

COSO mejora su Control Interno – *Estructura conceptual integrada*

Por Jennifer Burns y Brent Simer, Deloitte LLP.

El 14 de mayo de 2013, el Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] publicó una versión actualizada de su *Internal Control – Integrated Framework* [Control interno – Estructura conceptual integrada] (la "estructura 2013"). Además, COSO publicó dos documentos ilustrativos: *Illustrative Tools for Assessing Effectiveness of a System of Internal Control* [Herramientas ilustrativas para valorar la efectividad de un sistema de control interno] (las "Herramientas ilustrativas") e *Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples* [Control interno sobre la presentación de reportes financieros externos: un compendio de enfoques y ejemplos] (el "Compendio CIIF") así como también un resumen ejecutivo de la estructura 2013.

Emitida originalmente en 1992, *Internal Control – Integrated Framework* [Control interno – Estructura conceptual integrada] de COSO (la "estructura 1992") se convirtió en una de las estructuras de control interno más ampliamente aceptadas en el mundo. El objetivo principal de COSO al actualizar y mejorar la estructura es abordar los cambios importantes a los entornos de negocios y operación que han ocurrido durante los últimos 20 años.

La estructura 2013 y las herramientas ilustrativas pueden ser compradas en la AICPA Store. El resumen ejecutivo de la estructura 2013 está disponible gratis en el sitio web de COSO.

Este *Heads Up* ofrece una vista de conjunto de los mejoramientos contenidos en la estructura 2013, una discusión de las consideraciones para las entidades que usan la estructura 1992 para el cumplimiento con la Sección 404 de la Ley Sarbanes-Oxley de 2002 (SOX), e información acerca de cómo hacer la transición desde la estructura 1992 hacia la estructura 2013, incluyendo los impactos en otros documentos relacionados de COSO. Además, los apéndices de este *Heads Up* comparan la estructura 2013 con la estructura 1992 así como también resalta algunos de los conceptos ampliados contenidos en la estructura 2013. Para información adicional acerca de las estructuras, vea los boletines *Heads Up* de febrero 6 de 2012 y de agosto 7 de 2012, de Deloitte.

Mejoramientos en la estructura 2013

La estructura 2013 crea una estructura más formal para diseñar y evaluar la efectividad del control interno mediante:

1. *Usar principios para describir los componentes del control interno* – La estructura 2013 contiene 17 principios que explican los conceptos asociados con los cinco componentes de la estructura de COSO (ambiente de control, valoración del riesgo, actividades de control, información y comunicación, y actividades de monitoreo). En el desarrollo de los 17 principios, COSO se centró en los conceptos provenientes de la estructura 1992; consideró los principios que fueron desarrollados y articulados en *Internal Control Over Financial Reporting – Guidance for Smaller Public Companies* [Control interno sobre la presentación de reportes financieros – Orientación para las compañías públicas más pequeñas] que COSO emitió en el año 2006 ("Orientación para los negocios pequeños"); y consideró los cambios importantes en los negocios,

[1] COSO es una iniciativa conjunta de cinco organizaciones del sector privado y está dedicado a proporcionar liderazgo intelectual mediante el desarrollo de estructuras y orientación sobre administración del riesgo de la empresa, control interno, y disuasión del fraude. Las cinco organizaciones del sector privado son la American Accounting Association, el American Institute of Certified Public Accountants, Financial Executives International, el Institute of Management Accountants, y el Institute of Internal Auditors.

los entornos de operación, y el gobierno ocurridos desde 1992. COSO tiene la intención de que los principios les ayuden a las compañías a diseñar sistemas efectivos de control interno y a evaluar si esos sistemas están funcionando de manera efectiva. La estructura 2013 presume que dado que los 17 principios son conceptos fundamentales de los cinco componentes, todos los 17 son relevantes para todas las entidades. En consecuencia, si un principio no está presente y funcionando, el componente asociado no está presente y funcionando. En circunstancias raras, a causa de materias de industria, regulatorias, o de operación, la administración puede determinar que un principio no es relevante para un componente.

Para describir de manera adicional los principios, la estructura 2013 usa puntos de atención, los cuales típicamente son características importantes de los principios. Si bien los puntos de atención pueden ayudarle a la administración a diseñar, implementar, y evaluar el control interno y valorar si los principios relevantes están presentes y están funcionando, no son requeridos para valorar la efectividad del control interno. La administración puede determinar que algunos de los puntos de atención no son confiables o relevantes y puede identificar y considerar otros.

2. *Crear una manera más formal para diseñar y evaluar el control interno de acuerdo con los principios.* Vea abajo la discusión titulada "Sistemas efectivos de control interno."

Si bien los conceptos fundamentales contenidos en la estructura 2013 son similares a los contenidos en la estructura 1992, la estructura 2013 adiciona o amplía las discusiones acerca de cada componente y principio.

Si bien los conceptos fundamentales contenidos en la estructura 2013 son similares a los contenidos en la estructura 1992, la estructura 2013 adiciona o amplía las discusiones acerca de cada componente y principio, incluyendo mejoramientos tales como los puntos de atención detallados. Por ejemplo, si bien el concepto de identificar y responder ante los riesgos estaba presente en la estructura 1992, la estructura 2013 incluye discusiones más detalladas acerca de los conceptos de valoración del riesgo, incluyendo los relacionados con riesgo inherente, tolerancia frente al riesgo, cómo se pueden administrar los riesgos, y el vínculo entre la valoración del riesgo y las actividades de control.

Además, a diferencia de la estructura 1992, la estructura 2013 de manera explícita incluye el concepto de considerar el potencial por el riesgo de fraude cuando se valoran los riesgos para el logro de los objetivos de la organización (vea el Principio 8). La estructura 2013 explica que "como parte del proceso de valoración del riesgo, la organización debe identificar las diversas maneras como puede ocurrir la presentación fraudulenta de reportes [financieros] considerando:

- El sesgo de la administración, por ejemplo en la selección de los principios de contabilidad.
- Grado de estimados y juicios en la presentación de reportes externos
- Esquemas de fraude y escenarios comunes para los sectores de industria y los mercados en los cuales la entidad opera
- Regiones geográficas donde la entidad hace negocios
- Incentivos que pueden motivar el comportamiento fraudulento
- Naturaleza de la tecnología y capacidad de la administración para manipular la información
- Transacciones inusuales o complejas sujetas a influencia importante de la administración
- Vulnerabilidad ante la capacidad de la administración para eludir los controles y esquemas potenciales para eludir las actividades de control existentes"

El Principio 8 también discute consideraciones relacionadas con la capacidad de la administración para eludir los controles, salvaguarda de activos, incentivos y presiones, oportunidades para actos inapropiados, así como las actitudes y las racionalizaciones que pueden justificar acciones inapropiadas. (Vea discusión adicional del Principio 8 en el Apéndice A).

Además, COSO ha adicionado consideraciones a través de toda la estructura 2013 en relación con:

- El uso de proveedores de servicios tercerizados (vea Apéndice B).
- Relevancia incrementada de la tecnología de la información (vea Apéndice C).

La tabla que se presenta a continuación resume los principios por componente. El Apéndice A mapea los principios con las secciones temáticas contenidas en la estructura 1992 (según sea aplicable) y resume, a un nivel alto, algunos de los principios mejorados contenidos en la estructura 2013.

Componentes y principios del control

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.	6. Especifica objetivos confiables.	10. Selecciona y desarrolla las actividades de control.	13. Usa información relevante.	16. Dirige evaluaciones continuas y/o separadas.
2. Ejerce responsabilidad por la vigilancia.	7. Identifica y analiza el riesgo.	11. Selecciona y desarrolla los controles generales sobre la tecnología.	14. Comunica internamente.	17. Evalúa y comunica deficiencias
3. Establece estructura, autoridad, y responsabilidad	8. Valora el riesgo de fraude.	12. Despliega mediante políticas y procedimientos.	15. Comunica externamente	
4. Demuestra compromiso para con la competencia	9. Identifica y analiza el cambio importante.			
5. Hace forzosa la *accountability.*				

Se requiere que cada uno de los cinco componentes y los principios relevantes estén presentes y funcionando.

Sistemas efectivos de control interno

En un sistema efectivo de control interno según la estructura 2013:

1. Se requiere que cada uno de los cinco componentes y los principios relevantes estén presentes y funcionando. Según la estructura 2013:
   - **Presente** es definido como "la determinación de que los componentes y los principios relevantes existen en el diseño y la implementación del sistema de control interno para lograr los objetivos especificados."
   - **Funcionando** es definido como "la determinación de que los componentes y los principios relevantes continúan existiendo en la dirección del sistema de control interno para lograr los objetivos especificados."

2. Se requiere que los cinco componentes operen juntos de una manera integrada. La estructura 2013 explica que:
   - **Operen juntos** se refiere a "la determinación de que todos los cinco componentes colectivamente reducen, a un nivel aceptable, el riesgo de no lograr un objetivo."
   - La administración puede demostrar que los componentes operan juntos cuando:
     - Los "componentes están presentes y están funcionando."
     - "Las deficiencias de control interno agregadas a través de los componentes no resultan en la determinación de que existe una o más deficiencias importantes."

Nota del editor: Según las reglas de la SEC relacionadas con el cumplimiento con la Sección 404 de SOX, "la valoración del control interno sobre la presentación de reportes financieros de la compañía se tiene que basar en procedimientos suficientes tanto para evaluar su diseño como para probar la efectividad de su operación."[2] De igual manera, el Estándar de Auditoría 5 de la PCAOB[3] requiere que el auditor evalúe el diseño y la efectividad de la operación del control interno sobre la presentación de reportes financieros. Nosotros consideramos que "presente" y "funcionando" son equivalentes a "diseño" y "efectividad de la operación," respectivamente.

[2] Securities Act Release No. 33-8238, File Nos. S7-40-02 and S7-06-03 (August 14, 2003).
[3] PCAOB Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements.

La estructura 2013 usa los términos “deficiencia del control interno” y “deficiencia importante” para describir los grados de severidad de las deficiencias del control interno. Según la estructura 2013, una deficiencia del control interno se refiere a un “defecto en un componente o componentes y en el(los) principio(s) relevante(s) que reduce la probabilidad de que la entidad logre sus objetivos,” y una deficiencia importante se refiere a una “deficiencia del control interno o combinación de deficiencias que de manera severa reduce la probabilidad de que la entidad pueda lograr sus objetivos.” Además, la estructura 2013 explica que existe una deficiencia importante cuando “un componente y uno o más principios relevantes no está presente o no está funcionando” o cuando “los componentes no están operando juntos.” Además, si existe una deficiencia importante, la organización no puede concluir que ha logrado los requerimientos para un sistema efectivo de control interno.

Muy importante, la estructura 2013 reconoce que en la evaluación de las deficiencias en el control interno, los reguladores, emisores del estándar, y otras partes pueden establecer criterios para definir la severidad de, la evaluación, y la presentación de reportes sobre las deficiencias del control interno. Para cumplir con los requerimientos de presentación de reportes sobre el control interno según SOX, la administración continuaría usando la terminología de deficiencia importante y debilidad material, de la SEC, y los auditores continuarían usando la misma terminología según los estándares de la PCAOB. De acuerdo con ello, cuando la compañía esté evaluando el diseño y la efectividad de la operación de su control interno sobre la presentación de reportes financieros (CIIF) (i.e., si los principios están presentes y funcionando) e identifica una deficiencia, la compañía estaría requerida a usar las definiciones y la orientación de la SEC para valorar la severidad de la deficiencia, y el auditor estaría requerido a usar las definiciones y la orientación según los estándares de la PCAOB.

COSO ha señalado que “continuará teniendo disponible su estructura original durante el período de transición extendido hasta el 15 de diciembre de 2014, luego del cual COSO considerará que ha sido sustituido.”

Orientación, de COSO, para la transición e impacto en otros documentos de COSO

Durante el proceso público de comentarios sobre el borrador para discusión pública de la estructura 2013, varios *stakeholders* solicitaron que COSO proporcione una fecha específica para la transición desde la estructura 1992 hacia la estructura 2013. Con base en esta retroalimentación, COSO ha proporcionado algunos detalles sobre la transición y está fomentando que los usuarios “hagan la transición de sus aplicaciones y documentación relacionada hacia la *Estructura* actualizada tan pronto como sea posible según sus circunstancias particulares.” COSO ha señalado que “continuará teniendo disponible su estructura original durante el período de transición extendido hasta el 15 de diciembre de 2014, luego del cual COSO considerará que ha sido sustituido.” Además, Paul Beswick, contador jefe de la SEC ha señalado que el “personal de la SEC planea monitorear la transición para los emisores que usen la estructura 1992 a fin de evaluar si son necesarias o apropiadas cualesquiera acciones del personal o de la Comisión en algún punto en el futuro.” Adicionalmente señaló que en este momento, “simplemente refiere a los usuarios a la estructura de COSO para las declaraciones que COSO ha hecho acerca de su nueva estructura y sus pensamientos acerca de la transición.”

Durante el período de transición (mayo 14 de 2012 a diciembre 15 de 2014), COSO sugiere que cualquier “aplicación de su *Control interno – Estructura conceptual integrada* que implique presentación de reportes externos debe revelar de manera clara si se utilizó la versión original o la versión 2013.” Como resultado, cuando las compañías proporcionen su valoración anual del CIIF de acuerdo con SOX, sería apropiado señalar la estructura exacta de COSO que usaron al realizar la valoración.

Nota del editor: El Estándar de Auditoría 5 de la PCAOB señala que “el auditor debe usar la misma estructura de control reconocida, confiable, para realizar su auditoría del control interno sobre la presentación de reportes financieros que la administración use para su evaluación anual de la efectividad del control interno sobre la presentación de reportes financieros de la compañía.” Como resultado, la oportunidad de cuándo el auditor hace la transición hacia la estructura 2013 para auditar el CIIF dependerá de la oportunidad de la transición de la compañía. Si la compañía usa la estructura 1992 para el año calendario que termina el 31 de diciembre de 2013, el auditor también usaría la estructura 1992. Nosotros consideramos que de una manera consistente con el enfoque para revelar la estructura exacta de COSO usada en la valoración del CIIF que realice la administración, sería apropiado señalar en el reporte del auditor la estructura exacta usada.

La orientación para negocios pequeños, de COSO, será reemplazada por el Compendio CIIF después del 15 de diciembre de 2014.

Enterprise Risk Management – Integrated Framework [Administración del riesgo de la empresa – Estructura conceptual integrada] de COSO (la "estructura ERM") no ha sido reemplazada por la estructura 2013. Si bien la estructura ERM y la estructura 2013 tienen la intención de tener diferentes centros de atención, las dos estructuras están diseñadas para complementarse una con la otra. COSO considera que si bien la estructura ERM incluye porciones del texto de la estructura 1992, la estructura ERM continúa siendo confiable para diseñar, implementar, dirigir, y valorar la administración del riesgo de la empresa.

Guidance on Monitoring Internal Control Systems [Orientación sobre el monitoreo de sistemas de control interno], de COSO, que fue escrita para ayudarles a las organizaciones para entender y aplicar las actividades de monitoreo contenidas en un sistema de control interno, también continúa siendo relevante (i.e., no ha sido reemplazada por la estructura 2013). El Apéndice F de la estructura 2013 señala que los "cambios a los principios contenidos en la estructura no modificarán de manera sustancial los enfoques desarrollados por la Orientación sobre el monitoreo de los sistemas de control interno, de COSO."

Las compañías deben considerar usar las actividades 2013, tales como recorridos y pruebas de los controles relevantes, para identificar los cambios necesarios y la aplicación de las pruebas de campo de la estructura 2013.

Control interno sobre la presentación de reportes financieros externos

El impacto que la estructura 2013 tenga en la valoración que la administración hace de la efectividad del CIIF (i.e., para cumplir con la Sección 404 de SOX) dependerá de cómo la compañía aplicó e interpretó los conceptos contenidos en la estructura 1992. Por ejemplo, un sistema existente de control interno puede no demostrar o documentar de manera clara que todos los principios relevantes estén presentes y funcionando.

COSO desarrolló el Compendio CIIF para ayudar a las compañías a aplicar la estructura 2013. Los enfoques que se discuten en el documento describen cómo las organizaciones pueden aplicar los principios en su sistema de CIIF, y sus ejemplos ilustran la aplicación de cada principio.

Las compañías que usen COSO para reportar sobre el CIIF pueden querer considerar:

1. Leer la estructura 2013 e identificar los nuevos conceptos y los cambios.
2. Valorar sus necesidades de entrenamiento y educación.
3. Determinar cómo la estructura 2013 afecta el diseño y la evaluación del CIIF mediante:
   a. Valorar la cobertura de los principios por parte de los procesos existentes y los controles relacionados y considerar los puntos de atención.
   b. Valorar los procesos corrientes, actividades, y documentación disponible relacionados con la aplicación de los principios.
   c. Identificar cualesquiera brechas en lo anterior.
4. Identificar los pasos, si los hay, a ser dados al hacer la transición hacia la estructura 2013, y
   a. Formular un plan para completar la transición para el 15 de diciembre de 2014 (i.e., las compañías de final de año calendario que cumplen con la Sección 404 de SOX deben hacer la transición hacia la estructura 2013 para los período de reporte que terminen después del 31 de diciembre de 2014).
   b. Considerar usar las actividades realizadas en 2013 (i.e., recorridos, pruebas de los controles relevantes, evaluación de las deficiencias) para identificar los cambios necesarios y las pruebas piloto o de campo para la aplicación de la estructura 2013.
   c. Confirmar la revelación adecuada de la estructura usada durante el período de transición y el tiempo en el cual se adoptó la estructura 2013.
5. Coordinar y comunicar internamente con todos los grupos que sean responsables por implementar, monitorear, y reportar sobre el CIIF de la organización.
6. Discutir y coordinar las actividades con la auditoría interna (si es aplicable) y el auditor externo.

Herramientas ilustrativas

Las herramientas ilustrativas, de COSO, ofrecen ejemplos de cómo la compañía puede aplicar la estructura 2013 en la valoración de la efectividad de su sistema de control interno. El documento ofrece plantillas ilustrativas e incluye escenarios con ejemplos de cómo completar diversas plantillas. Sin embargo, las herramientas ilustrativas no tienen la intención de:

- Satisfacer cualesquiera requerimientos regulatorios para la evaluación de las deficiencias del control interno.
- Ilustrar la selección que la administración hace de los controles para poner en efecto los principios o abordar los riesgos identificados.
- Ilustrar las decisiones acerca de la naturaleza, oportunidad, o extensión de las pruebas de los controles para asegurar un sistema efectivo de control interno.

Apéndice A – Comparación de los principios contenidos en la estructura 2013 con las secciones relacionadas contenidas en la estructura 1992, y resumen de los conceptos mejorados contenidos en la estructura de 2013

La tabla que se presenta a continuación mapea los principios contenidos en la estructura 2013 con las secciones temáticas contenidas en la estructura 1992. La tabla demuestra que, para la mayor parte, los conceptos representados en los principios contenidos en la estructura 2013 son similares a los contenidos en la estructura 1992. Sin embargo, la orientación que subyace a los principios ha sido ampliada, tal y como se señala en la columna derecha, que resume a un nivel alto algunos de los conceptos mejorados contenidos en la estructura 2013.

Principios contenidos en la estructura 2013	Secciones relacionadas contenidas en la estructura 1992		Resumen de los conceptos mejorados contenidos en la estructura 2013
	Capítulo	Sección	
Ambiente de control			
1. La organización demuestra compromiso para con la integridad y los valores éticos.	• Ambiente de control	• Integridad y valores éticos • Políticas y procedimientos de recursos humanos	• La integridad como pre-requisito para el comportamiento ético y para un sistema efectivo de control interno. • Necesidad para considerar los impactos del ambiente de control a través de la estructura. • Importancia de: o Tono desde lo alto tal y como es establecido por la junta de directores y la administración o Establecer estándares de conducta para los empleados y para los proveedores de servicios tercerizados (OSP♦) o Evaluar la adherencia a los estándares esperados y abordar oportunamente cualesquiera desviaciones.
2. La junta de directores demuestra independencia de la administración y ejerce vigilancia del desarrollo y ejecución del control interno	• Ambiente de control	• Junta de directores o comité de auditoría	• Discusión ampliada de los conceptos de gobierno, incluyendo la necesidad de establecer responsabilidades de vigilancia para la junta y sus comités. • Materias relacionadas con independencia, habilidades y experticia de la junta. • Incluye una tabla detallada que ilustra las responsabilidades de vigilancia por cada uno de los cinco componentes del control interno.
	• Roles y responsabilidades	• Administración, junta de directores	
3. La administración establece, con la vigilancia de la junta, estructuras, líneas de presentación de reportes, y autoridades y responsabilidades apropiadas en la búsqueda de los objetivos.	• Ambiente de control	• Filosofía de la administración y estilo de operación • Estructura organizacional • Asignación ad autoridad y responsabilidad	• Definición, asignación y limitación de la autoridad y responsabilidad en los diferentes niveles organizacionales y a lo largo de las diversas líneas de presentación de reportes (e.g., considerar líneas de producto o servicio, estructuras de la entidad legal, mercados geográficos, y acuerdos con OSP).
	• Roles y responsabilidades	• Administración, junta de directores, auditores internos, otro personal de la entidad	
4. La organización demuestra el compromiso para atraer, desarrollar, y retener individuos competentes en alineación con los objetivos.	• Ambiente de control	• Compromiso para con la competencia • Políticas y prácticas de recursos humanos	• Planeación y preparación para la sucesión por los roles que sean importantes para la efectividad del control interno. • Expectativa y evaluación de las competencias. • Incorpora la consideración de los OSP.
5. La organización hace que los individuos sean responsables por sus responsabilidades de control interno en la búsqueda de los objetivos	• Ambiente de control	• Integridad y valores éticos • Políticas y prácticas de recursos humanos	• La importancia de hacer que los individuos sean responsables por sus responsabilidades de control interno. • Alineación de incentivos y recompensas con las responsabilidades de control interno • Considerar presiones excesivas • Incorpora la consideración de los OSP.
	• Roles y responsabilidades	• Administración, junta de directores, auditores internos, otro personal de la entidad	

♦ OSP = outsourced service providers = proveedores de servicios tercerizados (N del t)

Principios contenidos en la estructura 2013	Secciones relacionadas contenidas en la estructura 1992		Resumen de los conceptos mejorados contenidos en la estructura 2013
	Capítulo	Sección	
Valoración del riesgo			
6. La organización especifica los objetivos con suficiente claridad para permitir la identificación y valoración de los riesgos en relación con los objetivos.	• Valoración del riesgo	• Categorías de objetivos • Superposición de objetivos • Vínculo • Logro de objetivos	• Separa en tres objetivos la categoría de presentación de reportes financieros: (1) presentación de reportes financieros externos; (2) presentación de reportes no-financieros externos, y (3) presentación de reportes internos.
7. La organización identifica los riesgos para el logro de sus objetivos a través de la entidad y analiza los riesgos como base para determinar cómo se deben administrar los riesgos.	• Valoración del riesgo	• Identificación del riesgo • Análisis del riesgo	• Explica que el proceso de valoración del riesgo incluye identificación del riesgo, análisis, y respuesta. • Incorpora el concepto de riesgo inherente. • Expande la discusión de la tolerancia frente al riesgo y cómo el riesgo puede ser administrado, incluyendo mediante aceptar, evitar, reducir, y compartir el riesgo. • Considera la velocidad y persistencia del riesgo (además del impacto y la probabilidad). • Incorpora la consideración de los OSP.
8. En la valoración de los riesgos para el logro de los objetivos la organización considera el potencial por el fraude	• Adenda a "Presentación de reportes a partes externas"	• Discusión[4]	• Incorpora el concepto de valoración del riesgo de fraude. • Consideraciones relacionadas con los diversos tipos de fraude, incluyendo presentación fraudulenta de reportes financieros, presentación fraudulenta de reportes no-financieros, uso indebido de activos, salvaguarda de activos, capacidad que tiene la administración para eludir los controles, y corrupción. • Evaluación de incentivos, presiones, oportunidades, actitudes, y racionalizaciones. • Incorpora la consideración de los OSP.
9. La organización identifica y valora los cambios que podrían impactar de manera importante el sistema de control interno.	• Valoración del riesgo	• Circunstancias que requieren atención especial • Mecanismos • Prospectiva	• Importancia de valorar los cambios en el entorno externo, modelo de negocios, operaciones, tecnología, relaciones con OSP, liderazgo, y cómo tales cambios pueden afectar el control interno.
Actividades de control			
10. La organización selecciona y desarrolla actividades de control que contribuyen a la mitigación, a niveles aceptables, de los riesgos para el logro de los objetivos.	• Actividades de control	• Tipos de actividades de control • Integración con la valoración del riesgo • Entidad específica	• El vínculo entre la valoración del riesgo y las actividades de control. • Consideración del nivel en el cual se aplican las actividades de control (incluyendo los diversos niveles de la organización). • Los tipos de controles aplicados (incluyendo considerar los controles preventivos vs. de detección). • Diferencia entre las actividades de control de los procesos de negocio y las actividades de control de la transacción.
11. La organización selecciona y desarrolla actividades generales de control sobre la tecnología para apoyar el logro de los objetivos.	• Actividades de control	• Controles sobre los sistemas de información – controles generales, controles de aplicación, relación entre controles generales y de aplicación, problemas en evolución.	• Incorpora conceptos actualizados de tecnología, incluyendo los relacionados con infraestructura de tecnología, seguridad, adquisición, desarrollo, mantenimiento, y uso de OSP. • Discute la relación entre las actividades de control automatizadas y los controles generales de tecnología de información.
12. La organización despliega actividades de control mediante políticas que establecen qué se espera y los procedimientos que ponen esas políticas en acción.	• Actividades de control	• Tipo de actividades de control – políticas y procedimientos	• Establecimiento de políticas y procedimientos para apoyar el despliegue de las directivas de la administración. • Establecimiento de responsabilidad y *accountability* por la ejecución de políticas y procedimientos. • Volver a valorar políticas y procedimientos sobre una base periódica para determinar su relevancia continuada y si se necesitan revisiones.

[4] La adenda a "Presentación de reportes a partes externas" incluye sólo una discusión de la salvaguarda de los activos. La valoración del riesgo de fraude no es abordada de manera directa en la estructura 1992.

Principios contenidos en la estructura 2013	Secciones relacionadas contenidas en la estructura 1992		Resumen de los conceptos mejorados contenidos en la estructura 2013
	Capítulo	Sección	
Información y comunicación			
13. La organización obtiene o genera y usa información de calidad, relevante, para apoyar el funcionamiento del control interno.	• Información y comunicación	• Sistemas estratégicos e integrados • Calidad de la información	• Identificación de los requerimientos de información, verificación de fuentes de datos, procesamiento de datos relevantes, mantenimiento de la calidad mediante el procesamiento, y uso de OSP. • Consideración de los costos y beneficios de la información así como también el impacto de la tecnología. • Consideración de la confiabilidad y protección de los datos. • Re-evaluación de las necesidades de información. • Consideración de cómo la información apoya el funcionamiento del control interno.
14. La organización comunica internamente información, incluyendo objetivos y responsabilidades por el control interno, necesaria para apoyar el funcionamiento del control interno.	• Información y comunicación	• Comunicación – interna • Medios de comunicación	• Importancia de la comunicación entre la administración y la junta de directores tal que ambos tengan información suficiente para cumplir de manera exitosa sus roles con relación a los objetivos de la entidad. • Proporcionar canales de comunicación separados por la comunicación anónima o confidencial cuando los canales normales de comunicación sean inoperativos o inefectivos (e.g., mediante líneas directas para las denuncias anónimas).
15. La organización comunica con partes externas en relación con las materias que afecten el funcionamiento del control interno.	• Información y comunicación	• Comunicación – externa • Medios de comunicación	• Importancia de canales de comunicación abierta para permitir el input proveniente de los *stakeholders*, incluyendo los resultados de la valoración de parte externa, para la junta de directores. • Proporcionar canales de comunicación separados para la comunicación anónima o confidencial cuando los canales normales de comunicación sean inoperativos o inefectivos (e.g., mediante líneas directas para denuncias anónimas). • Consideraciones relacionadas con OSP.
Actividades de monitoreo			
16. La organización selecciona, desarrolla, y realiza evaluaciones continuas y/o separadas para afirmar si los componentes del control interno están presentes y funcionando.	• Monitoreo	• Actividades de monitoreo continuo • Evaluaciones separadas – alcance y frecuencia, quién evalúa el proceso de evaluación, métodos, documentación, plan de acción	• Consideración de la tasa de cambio cuando se desarrollan actividades de monitoreo • Usando una base de entendimiento del control interno para establecer planes para las evaluaciones continuas y separadas. • Consideraciones relacionadas con el monitoreo en los diferentes niveles de la organización y el monitoreo de los OSP. • Uso de la tecnología en el contexto del monitoreo.
17. La organización evalúa y comunica oportunamente las deficiencias del control interno a las partes responsables por realizar la acción correctiva, incluyendo la administración principal y la junta de directores, según sea apropiado.	• Monitoreo	• Presentación de reportes sobre las deficiencias – fuentes de información, qué debe ser reportado, a quién reportar, directivas para la presentación de reportes	• Comunicación de las deficiencias • Monitoreo de acciones correctivas.

Apéndice B – Resumen de los conceptos y la discusión contenidos en la estructura 2013 relacionados con el uso de proveedores de servicios tercerizados

La estructura 2013 adiciona o amplía las discusiones acerca de cada componente y principio, haciéndolo mediante incluir mejoramientos tales como los puntos de atención detallados. Una de las adiciones importantes a la estructura 2013 es la incorporación de las consideraciones relacionadas con los OSP. La tabla que se presenta a continuación ofrece un resumen de los conceptos y discusiones de la estructura 2013 relacionados con el uso de los OSP. Los usuarios de la estructura 2013 deben considerar cómo esos cambios aplican a sus acuerdos con los OSP.

Capítulo en la estructura 2013	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con los OSP
Definición de control interno	N/A	4	• Reconoce que el modelo de operación de la administración puede usar OSP para apoyar el logro de los objetivos.
Objetivos, componentes, y principios	N/A	17	• Una limitación del control interno es que mediante colusión los terceros pueden eludir los controles.
Control interno efectivo	N/A	22	• Si bien la organización puede confiar en los OSP, la administración retiene la responsabilidad última por satisfacer los requerimientos para un sistema efectivo de control interno.
Consideraciones adicionales	N/A	24-25	• La dependencia en los OSP cambia los riesgos de las actividades de negocio, incrementa la importancia de la información y las comunicaciones provenientes de fuera de la organización, y crea desafíos en la vigilancia de las actividades y los controles relacionados.
Ambiente de control	Principio 1	33-38	• Las expectativas de la organización relacionadas con la integridad y los valores éticos son entendidas por los OSP. • Los estándares de conducta de la organización son comunicados regularmente a los OSP y reforzados. • La conducta inapropiada de los OSP puede reflejarse de manera negativa en la administración principal y afectar a la entidad misma mediante causar daños a los clientes, otros *stakeholders*, o a la reputación de la organización, requiriendo costosa acción correctiva. • La administración retiene la *accountability* última por las actividades y el desempeño de los procesos que delegue a los OSP. • Los estándares de conducta de la organización proporcionan la base para la evaluación de la adherencia a la integridad y los valores éticos por parte de los OSP. • La organización comunica a los OSP los niveles de tolerancia establecidos. • La organización define un conjunto de indicadores para identificar los problemas y las tendencias relacionados con los estándares de conducta por parte de los OSP. La organización también establece los procedimientos de cumplimiento.
	Principio 3	44-48	• La administración y la junta de directores consideran los OSP cuando establecen las estructuras organizacionales, las líneas de presentación de reporte, y las autoridades y responsabilidades que sean apropiadas. • La administración asegura que no hay conflicto de intereses en la organización y con los OSP. • A los OSP se les proporciona términos contractuales claros y concisos relacionados con los objetivos de la entidad y las expectativas de conducta y desempeño, niveles de competencia, información esperada, y flujo de la comunicación. • Los OSP se adhieren a la definición que tiene la administración sobre el alcance de la autoridad y responsabilidad delegadas, así como sobre el entendimiento de las limitaciones en sus derechos de toma de decisiones.
	Principio 4	49-52	• El compromiso que la organización tiene para con la competencia, tal y como es comunicado en las políticas y en las prácticas, facilita la medición del logro de los objetivos por parte de los OSP. • La administración evalúa la competencia de los OSP en relación con las políticas y prácticas establecidas y luego actúa según sea necesario para abordar cualesquiera interrupciones o excesos. • El compromiso que la organización tiene para con la competencia es apoyado mediante atraer, desarrollar, evaluar, y retener los OSP correctos. • La administración evalúa el desempeño de los OSP contra los acuerdos de nivel de servicio u otros estándares acordados. • La planeación de la sucesión es llevada a cabo por la administración cuando funciones importantes sean delegadas mediante acuerdos contractuales con los OSP.

Capítulo en la estructura 2013	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con los OSP
Ambiente de control	Principio 5	53-58	• Si bien los OSP pueden ser usados para llevar a cabo responsabilidades junto con o a nombre de la organización, la administración retiene la *accountability* última por el control interno. • El tono desde lo alto ayuda a establecer y forzar la *accountability*, la moral, y el propósito común, por ejemplo mediante tener disponibles para los OSP canales de comunicación ascendentes y de otro tipo para la presentación de reportes sobre las violaciones de los estándares éticos. • La administración y la junta de directores considera la interrelación entre los OSP y las medidas, incentivos, recompensas, y presiones del desempeño. • Se espera que los OSP preserven la calidad de los productos o servicios entregados, la seguridad del personal, y otros factores que podrían crear daño moral o daño en la reputación de la organización.
Valoración del riesgo	Principio 7	70-71	• La identificación del riesgo tiene que ser comprensiva y tiene que tener en cuenta las interacciones importantes entre la organización y los OSP. • El proceso de valoración del riesgo de la entidad tiene en cuenta los riesgos que se originan en los OSP.
	Principio 8	78-80	• Durante su valoración del riesgo de fraude la organización considera los posibles actos de corrupción por parte de los OSP, lo cual se debe basar en la presunción de que se han adherido a los estándares de conducta ética esperados por la entidad. • Al valorar la posible corrupción, no se espera que la entidad administre de manera directa las acciones del personal de los OSP; sin embargo, la administración puede estipular los niveles de desempeño esperados y los estándares de conducta, haciéndolo mediante las relaciones contractuales, y puede desarrollar actividades de control que mantengan la vigilancia de los OSP.
	Principio 9	83-85	• La administración valora los cambios en las relaciones con los OSP a fin de determinar la relevancia de los controles internos previamente efectivos.
Actividades de control	Principio 10	89	• Cuando considera las acciones apropiadas para mitigar el riesgo, la administración valora los procesos o funciones desempeñados en los OSP.
	Principio 11	98-100	• Las infraestructuras de la tecnología de la organización pueden ser tercerizadas con organizaciones de servicio y pueden presentar riesgos que la administración necesita entender y abordar. • El desarrollo de la tecnología de la organización puede ser realizado por los OSP. Esto representa riesgos únicos y a menudo requiere seleccionar y desarrollar controles adicionales sobre la información presentada a y recibida de los OSP.
Información y comunicación	Principio 13	109-112	• La administración puede generar información útil relevante para los controles internos, proveniente de datos recibidos de los OSP. • Los sistemas de información pueden ser administrados mediante relaciones con los OSP. • La información que es obtenida de los OSP que administren procesos de negocio a nombre de la entidad está sujeta a las mismas expectativas de control interno (i.e., calidad) que la información generada internamente por la organización.
	Principio 15	119-120	• Una valoración independiente de los controles internos del OSP puede darle a la organización información importante acerca del funcionamiento de su sistema de control interno. • La interdependencia de los procesos de negocio entre la entidad y los OSP puede distorsionar las líneas de responsabilidad entre el sistema de control interno de la entidad y los de los OSP. • La comunicación con los OSP responsables por las actividades que apoyan los objetivos de la entidad puede facilitar el proceso de valoración del riesgo, la vigilancia de las actividades de negocio, la toma de decisiones, y la identificación de la responsabilidad por el control interno. • Pueden surgir complejidades de las relaciones de negocio entre la entidad y los OSP. La entidad debe tener disponibles para los OSP canales de comunicación separados para permitir la comunicación directa con la administración y otro personal.
Actividades de monitoreo	Principio 16	132	• Las entidades que usan OSP necesitan entender las actividades y los controles asociados con el OSP y cómo el sistema de control interno del OSP afecta al sistema de control interno de la entidad. Las entidades pueden obtener un entendimiento del sistema de control interno del OSP mediante: o Dirigir sus propias evaluaciones separadas sobre el sistema de control interno del OSP. o Revisar el reporte de una auditoría o examen independiente. o Considerar la naturaleza y el alcance de la información transferida y la naturaleza del procesamiento y de la presentación de reportes.

Capítulo en la estructura 2013	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con los OSP
Apéndice B: roles y responsabilidades	N/A	147	• Cuando los OSP ejecutan controles a nombre de la entidad, la administración retiene la responsabilidad por esos controles.
		149-150	• Las responsabilidades del CEO en relación con el control interno incluyen dirigir la administración y otro personal para considerar el ritmo de cambio siempre creciente y las interacciones que en la red tienen los OSP, así como los factores de riesgo resultantes. La administración principal apoya al CEO en esta capacidad.
		155	• Cuando los OSP ejecuten actividades para o a nombre de la organización, la administración no puede abdicar a su responsabilidad para administrar los riesgos asociados. La administración tiene que implementar un programa para evaluar las actividades realizadas por los OSP a su nombre para valorar la efectividad del sistema de control interno.

Apéndice C – Resumen de los conceptos y la discusión contenidos en la estructura 2013 relacionados con la tecnología de la información

La estructura 2013 adiciona o amplía las discusiones acerca de cada componente y principio, haciéndolo mediante incluir mejoramientos tales como los puntos de atención detallados. Además, la estructura 2013 refleja los cambios importantes en los negocios y en los entornos de operación, incluyendo los cambios en la tecnología de la información (TI), que han ocurrido desde que fue escrita la estructura 1992. Una de las adiciones importantes a la estructura 2013 es la discusión ampliada de la TI reflejando su relevancia incrementada para las organizaciones y sus sistemas de control interno. La tabla que aparece a continuación proporciona un resumen de los conceptos y discusiones de la estructura 2013 relacionados con la TI.

Capítulo	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con la TI
Objetivos, componentes, y principios	N/A	6	• Dos entidades no tendrán, ni deben tener, el mismo sistema de control interno; esto se debe, en parte, a los diferentes grados de confianza en la TI.
Consideraciones adicionales	N/A	24-26	• Los controles específicos se seleccionan con base en los juicios de la administración y factores únicos para cada organización, tal como el uso y la dependencia de la TI. • Los OSP pueden realizar actividades de TI que apoyen los procesos de negocio. Los avances en la TI han creado oportunidades de ahorro de costos mediante el acceso a arquitectura comprensiva que proporciona tecnología compartida según la demanda y escalable que de otra manera puede ser prohibitiva en términos de costo para que la administración invierta internamente en ella. • La TI puede ser esencial para apoyar la búsqueda que la administración hace de los objetivos de la entidad y para controlar de mejor manera las actividades de la organización. • Los términos “tecnología,” “sistemas de información de la administración,” y “tecnología de la información” se usan de manera sinónima y comparten las ideas de usar una combinación de (1) procesos automatizados y manuales y (2) hardware, software, métodos, y procesos de computador. • Los entornos de TI varían de manera importante en tamaño, complejidad, y extensión de la integración. • La innovación en TI crea tanto oportunidades como riesgos. • Los principios que se presentan en la estructura 2013 no cambian con la aplicación de la TI. Ciertamente, la TI afecta cómo una organización diseña, implementa, y dirige el control interno.
		28	• Cuando selecciona y desarrolla los controles internos la administración considera una variedad de factores de costo relacionados con los beneficios esperados, tal como la valoración de los impactos de la confianza adicional puesta en la TI.
Ambiente de control	Principio 2	39-43	• La administración valora continuamente los riesgos generados por los cambios en el entorno de operación, tal como el surgimiento de nuevas capacidades de TI. • La composición de la junta de directores se espera que incluya habilidades más especializadas, tales como las relacionadas con TI.
	Principio 3	44	• La administración y la junta usan procesos y tecnología apropiados para asignar responsabilidad y para segregar las funciones.
		45	• La administración es apoyada por los procesos y la tecnología requeridos para proporcionar *accountability* clara y flujos de información a través de toda la entidad y sus sub-unidades.
		48	• La TI es aprovechada según sea apropiado para facilitar la definición y limitación de los roles y responsabilidades en los flujos del trabajo de los procesos de negocio.
	Principio 4	49	• Las políticas y las prácticas de la organización proporcionan las habilidades y la conducta necesarias para apoyar el control interno (e.g., conocimiento de la operación de TI).
Valoración del riesgo	Principio 6	68	• Muchas organizaciones aplican estándares externos de TI para ayudar a administrar sus operaciones.
	Principio 7	72	• Los riesgos a nivel de entidad pueden surgir de factores internos o externos de TI.
	Principio 8	79	• Como parte de sus procesos de valoración del riesgo, la organización debe considerar la naturaleza de la TI y la capacidad de la administración para manipular la información.
		81	• La probabilidad de una pérdida de activos o de presentación fraudulenta de reportes externos se incrementa cuando hay: o Tasas altas de rotación del personal de TI o Sistemas de TI inefectivos
	Principio 9	85	• La organización identifica y valora los cambios a la TI a fin de determinar si su sistema de control interno necesitará ser modificado.

Capítulo	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con la TI
Actividades de control	N/A	87	• Las actividades de control se realizan en todos los niveles de la entidad, en las diversas etapas de los procesos de negocio, y sobre el entorno de TI.
	Principio 10	89	• Cuando determina cómo mitigar el riesgo, la administración considera todos los aspectos de los componentes del control interno de la entidad y los procesos de negocio relevantes, la TI, y las localizaciones donde se necesitan actividades de control.
		91	• El acceso restringido es importante cuando la TI es parte integral para un proceso o negocio de la organización.
		94	• Las actividades de control y la TI se relacionan una con otra de dos manera si: o TI apoya los procesos de negocio. o TI es usada para automatizar actividades de control. • La mayoría de los procesos de negocio tienen una mezcla de controles manuales y automatizados, dependiendo de la disponibilidad de TI en la entidad.
	Principio 11	97-100	• La confiabilidad de la TI en los procesos de negocio depende de la selección, desarrollo, y despliegue de las actividades generales de control de la TI; las consideraciones importantes incluyen: o Entender y determinar la dependencia y el vínculo entre procesos de negocio, actividades de control automatizadas, y controles generales de TI. o Selección y desarrollo de actividades de control sobre la infraestructura de TI. o Selección y desarrollo de actividades de control que estén diseñadas e implementadas para restringir los derechos de acceso de TI a los usuarios autorizados. o Selección y desarrollo de actividades de control sobre la adquisición, desarrollo, y mantenimiento de la TI y su infraestructura.
	Principio 12	102-103	• Los cambios en la TI pueden reducir la efectividad de las actividades de control o hacer redundantes algunas actividades de control. Siempre que ocurra cambio, la administración debe volver a valorar la relevancia de los controles existentes y refrescarlos cuando sea necesario.
Información y comunicación	Principio 13	110	• Los sistemas de información comprenden una combinación de personas, procesos, datos, y TI. • La naturaleza y extensión de los requerimientos de información, la complejidad y el volumen de la información, y la dependencia de partes externas afecta la extensión de la TI desplegada. • Los sistemas de información desarrollados con procesos integrados, facilitados por la TI, ofrecen oportunidades para mejorar la eficiencia, velocidad, y accesibilidad de la información para los usuarios. • Las soluciones de TI ofrecen oportunidades para que la administración aproveche la TI en el desarrollo e implementación de sistemas de información efectivos y eficientes.
		112	• Los controles sobre la retención de la información del control interno tienen en cuenta los desafíos de los avances en la TI, incluyendo las tecnologías de comunicación y colaboración usadas para apoyar los otros componentes del control interno y el logro de los objetivos de la entidad.
	Principio 14	116	• Cuando selecciona los métodos de comunicación, la administración considera las diferencias culturales, étnicas y generacionales que afectan la manera como se reciben los mensajes (e.g., mediante usar medios de comunicación basados en TI).
	Principio 15	119	• La TI permite que partes externas tengan acceso a foros públicos para publicar y discutir los negocios, las actividades y los controles de la entidad. Los controles son necesarios para guiar las expectativas por el uso apropiado a fin de evitar poner en peligro los objetivos de la entidad.
Actividades de monitoreo	Principio 16	128-129	• Las compañías frecuentemente usan la TI para apoyar las evaluaciones continuas. • Las técnicas computarizadas para el monitoreo continuo tienen un estándar alto de objetividad y permiten la revisión eficiente de grandes volúmenes de datos a un costo bajo. Tales técnicas, combinadas con una revisión y análisis robustos de los resultados por personal conocedor, resulta en monitoreo eficiente y efectivo.
Limitaciones de los controles	N/A	139	• Los sistemas de control interno bien diseñados se pueden romper cuando los cambios en los controles de aplicación de TI son implementados antes que el personal haya sido entrenado de la manera adecuada.
Apéndice A: Glosario	N/A	146	• El glosario incluye las siguientes definiciones relacionadas con la tecnología: o *Controles automatizados* – Las actividades de control principal o totalmente realizadas mediante TI. o *Tecnología* – Aplicaciones de software que operan en un computador, en sistemas de controles de fabricación, etc. o *Controles generales de tecnología* – Actividades de control que ayudan a asegurar la operación continuada, apropiada, de la TI. Incluyen los controles sobre la infraestructura de TI, administración de la seguridad, y adquisición, desarrollo, y mantenimiento de TI. También se les puede referir como “controles generales computarizados” o “controles de TI.”

Capítulo	Principio	Página(s)	Resumen de los conceptos y discusiones, contenidos en la estructura 2013, relacionados con la TI
Apéndice C: Consideraciones para las entidades más pequeñas	N/A	159-162	• Los desafíos para el control interno costo-efectivo incluyen controlar la TI y mantener, con recursos técnicos limitados, los controles generales y de aplicación que sean apropiados sobre los sistemas de información computarizados. • Las entidades más pequeñas a menudo usan software desarrollado y mantenido por otros. Tal software requiere la implementación y operación controladas, pero se reducen muchos de los riesgos asociados con los sistemas desarrollados en caso. • Los paquetes de software desarrollados comercialmente pueden ofrecer ventajas adicionales para las entidades más pequeñas, tales como facilidad integrada, relacionada con el control de cuáles empleados pueden tener acceso o modificar datos especificados.
Apéndice E: Cartas comentario del público	N/A	170	• La estructura 2013 no discute de manera extensiva iniciativas específicas de TI o los riesgos asociados con ellas a causa de la naturaleza en evolución de la TI y de las preocupaciones de que la estructura 2013 pudiera volverse anticuada.

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:

- Quarterly Accounting Roundup: An Update of Important Developments (June 27, 2 p.m. (EDT)).

Technical Library: The Deloitte Accounting Research Tool

[Biblioteca técnica: la herramienta de investigación contable de Deloitte]

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.

Además, los suscriptores de Technical Library tienen acceso al *Deloitte Accounting Journal*, que de manera breve resume los recientes desarrollos en el establecimiento del estándar de contabilidad.

Para más información, incluyendo detalles sobre la suscripción y una demostración en línea, visite www.deloitte.com/us/techlibrary.

Esta es una traducción al español de la versión oficial en inglés de **Heads Up – Volume 20, Issue 17 – June 10, 2013 COSO Enhances Its 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.