

Comparación de Controles Internos: COBIT®, SAC y COSO

En los años recientes, se dedicó una atención creciente al control interno por parte de los auditores, gerentes, contadores y legisladores. Tres documentos emitidos recientemente son el resultado de los esfuerzos continuos para definir, evaluar, reportar y mejorar el control interno. Estos son:

- COBIT (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Foundation,
- SAC (Systems Auditability and Control) del Institute of Internal Auditors Research Foundation,
- COSO - Internal Control - Integrated Framework del Committee of Sponsoring Organizations of the Treadway Commission

COBIT (1996) es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos.

SAC (1991, revisado en 1994) ofrece asistencia a los auditores internos sobre el control y auditoria de los sistemas y tecnología informática.

COSO (1992) brinda recomendaciones a la dirección sobre cómo evaluar, reportar y mejorar los sistemas de control.

Como diferentes cuerpos desarrollaron los documentos para encarar las necesidades específicas de sus propias audiencias, podrían existir algunas disparidades. No obstante, cada documento se enfoca en el control interno y cada audiencia, ej: los auditores internos, la dirección y los auditores externos, dedican mucho tiempo y esfuerzo hacia el establecimiento o evaluación de los controles internos. En consecuencia, comparar los conceptos de control interno presentados en esos documentos es de interés para los miembros de las tres audiencias.

Una comparación de los tres documentos revela que cada uno de ellos se construyó sobre la base de las contribuciones de los documentos previos. COBIT incorpora como parte de sus documentos fuentes tanto a COSO como a SAC. Toma su definición de control de COSO y su definición de Objetivos de Control de TI de SAC, COSO utiliza los conceptos de control interno de SAC.

Este artículo resume los tres documentos y compara los conceptos de control interno presentados en cada uno de ellos. La Tabla de la siguiente página denota los aspectos principales presentados.

**TABLA COMPARATIVA DE
DISTINTOS ATRIBUTOS DE CONTROL INTERNO**

Atributo	COBIT	SAC	COSO
Audiencia Primaria	Dirección, usuarios, auditores de SI	Audidores Internos	Dirección
CI visto como	Conjunto de procesos incluyendo políticas, procedimientos, prácticas estructuras organizacionales	Conjunto de procesos, subsistemas y gente	Procesos
Objetivos Organizacionales del CI	Operaciones Efectivas y eficientes Confidencialidad, Integridad y disponibilidad de información Informes financieros confiables Cumplimiento de las leyes y regulaciones	Operaciones Efectivas y eficientes Informes financieros confiables Cumplimiento de las leyes y regulaciones	Operaciones Efectivas y eficientes Informes financieros confiables Cumplimiento de las leyes y regulaciones
Componentes o Dominios	<u>Dominios:</u> Planeamiento y organización Adquisición e implementación Entrega y soporte Monitoreo	<u>Componentes:</u> Ambiente de Control Manual y Automatizado Procedimientos de Control de Sistemas	<u>Componentes:</u> Supervisión Ambiente de Control Administración de Riesgos Actividades de Control Información y Comunicación
Foco	Tecnología Informática	Tecnología Informática	Toda la Entidad
Efectividad del CI Evaluado	Por un período de tiempo	Por un período de tiempo	En un momento dado
Responsabilidad por el Sistema de CI	Dirección	Dirección	Dirección
Tamaño	187 páginas en cuatro documentos	1193 páginas en 12 módulos	353 páginas en cuatro volúmenes

Resúmenes de los Documentos

COBIT: Control Objectives for Information and related Technology

La Information Systems Audit and Control Foundation (ISACF) desarrolló los Objetivos de Control para la Información y Tecnología relacionada (COBIT) para servir como una estructura generalmente aplicable y prácticas de seguridad y control de SI para el control de la tecnología de la información. Esta estructura COBIT le permite a la gerencia comparar (benchmark) la seguridad y prácticas de control de los ambientes de TI, permite a los usuarios de los servicios de TI asegurarse que existe una adecuada seguridad y control y permite a los auditores sustanciar sus opiniones sobre el control interno y aconsejar sobre materias de seguridad y control de TI.

La motivación primaria para brindar esta estructura fue posibilitar el desarrollo de una política clara y buenas prácticas para el control de TI a través de toda la industria en todo el mundo.

La fase ya completada del proyecto COBIT provee un *Resumen Ejecutivo*, un *Marco* para el control de TI, una lista de *Objetivos de Control*, y un conjunto de *Guías de Auditoría*. (Los objetivos de control y las guías de auditoría están referenciadas a la estructura).

Las fases futuras del proyecto proveerán guías de auto-evaluación para la dirección e identificarán objetivos nuevos o actualizados mediante incorporación de otros estándares globales de control que se identifiquen. Además, agregar guías de control e identificar indicadores claves de desempeño.

Definición: COBIT adaptó su definición de control a partir de COSO: Las políticas, procedimientos, prácticas y estructuras organizacionales están diseñadas para proveer aseguramiento razonable de que se lograrán los objetivos del negocio y que se prevendrán, detectarán y corregirán los eventos no deseables.

COBIT adapta su definición de un objetivo de control de TI del SAC: Una declaración del resultado deseado o propósito a lograr implementando procedimientos de control en una actividad particular de TI.

COBIT enfatiza el rol e impacto del control de TI en lo relacionado con los procesos del negocio. El documento describe objetivos de control de TI independientes de plataformas y aplicaciones.

Recursos de TI: COBIT clasifica los recursos de TI como datos, sistemas de aplicación, tecnología, instalaciones y gente. Los datos son definidos en su sentido más amplio e incluyen no sólo números, textos y fechas, sino también objetos tales como gráficos y sonido. Los sistemas de aplicación son entendidos como la suma de procedimientos manuales y programados.

La tecnología se refiere al hardware, sistemas operativos, equipos de redes y otros. Instalaciones son los recursos utilizados para albergar y soportar los sistemas de información. Gente comprende las capacidades y habilidades individuales para planear, organizar, adquirir, entregar, apoyar y monitorear los servicios y sistemas de información.

Requerimientos: Para satisfacer los objetivos del negocio, la información necesita conformarse a ciertos criterios a los cuales COBIT se refiere como requerimientos del negocio respecto de la información. COBIT combina los principios incorporados en los modelos de referencia existentes en tres amplias categorías: calidad, responsabilidad fiduciaria y seguridad. De estos amplios requerimientos, el informe extrae siete categorías superpuestas de criterios para evaluar cuan bien están satisfaciendo los recursos de TI los requerimientos de información del negocio. Estos criterios son efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

Procesos y Dominios: En base al análisis de un documento del Reino Unido sobre prácticas de administración de TI de la biblioteca de infraestructura tecnológica (ITIL), COBIT clasifica los procesos de TI en cuatro dominios. Estos cuatro dominios son (1) planeamiento y organización, (2) adquisición e implementación, (3) entrega y soporte y (4) monitoreo. El agrupamiento natural de procesos en dominios es a menudo confirmado como dominios de responsabilidad en las estructuras organizacionales y sigue el ciclo gerencial o ciclo de vida aplicable a los procesos de TI en cualquier ambiente de TI.

COBIT presenta una estructura de control para los propietarios de los procesos del negocio. Cada vez más, la dirección está totalmente facultada con responsabilidad y autoridad completa por los procesos del negocio. COBIT incluye definiciones tanto de control interno como de los objetivos de control de TI, cuatro dominios de procesos y 32 declaraciones de control de alto nivel para esos procesos, 271 objetivos de control referenciados a esos 32 procesos y guías de auditoría vinculadas a los objetivos de control.

Estructura: La estructura COBIT provee declaraciones de control de alto nivel para los procesos particulares de TI. La estructura identifica la necesidad del negocio satisfecha por la declaración de control, identifica los recursos de TI administrados por los procesos, establece los controles habilitados y lista los principales objetivos de control aplicables.

Informe SAC

El informe SAC define el sistema de control interno, describe sus componentes, provee varias clasificaciones de los controles, describe objetivos de control y riesgos, y define el rol del auditor interno. El informe provee una guía sobre el uso, administración y protección de los recursos de tecnología informática y discute los efectos de la computación de usuario final, las telecomunicaciones y las tecnologías emergentes.

Definición: El informe SAC define a un sistema de control interno como: un conjunto de procesos, funciones, actividades, subsistemas, y gente que son agrupados o conscientemente segregados para asegurar el logro efectivo de los objetivos y metas.

El informe enfatiza el rol e impacto de los sistemas computarizados de información sobre el sistema de control interno. El mismo acentúa la necesidad de evaluar los riesgos, pesar los costos y beneficios y construir controles en los sistemas en lugar de agregarlos luego de la implementación.

Componentes: El sistema de control interno consiste en tres componentes: el ambiente de control, los sistemas manuales y automatizados y los procedimientos de control. El ambiente de control incluye la estructura de la organización, la estructura de control, las políticas y procedimientos y las influencias externas. Los sistemas automatizados consisten en sistemas y software de aplicación. SAC discute los riesgos de control asociados con los sistemas de usuario final y departamentales pero no describe ni define los sistemas manuales. Los procedimientos de control consisten en controles generales, de aplicaciones y compensatorios.

Clasificaciones: SAC provee cinco esquemas de clasificación para los controles internos en los sistemas informáticos: (1) preventivos, detectivos, y correctivos, (2) discrecionales y no-discrecionales, (3) voluntarios y obligatorios, (4) manuales y automatizados y (5) controles de aplicaciones y generales. Estos esquemas se enfocan en cuándo se aplica el control, si el control puede ser evitado, quién impone la necesidad del control, cómo se implementa el control, y dónde se implementa el control en el software.

Objetivos de Control y Riesgos: Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software. Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.

Rol del Auditor Interno: Las responsabilidades de los auditores internos incluyen asegurar la adecuación del sistema de control interno, la confiabilidad de los datos y el uso eficiente de los recursos de la organización. A los auditores internos también les concierne la prevención y detección de fraudes, y la coordinación de actividades con los auditores externos. Para los auditores internos es necesaria la integración de las habilidades de auditoría y sistemas de información y una comprensión del impacto de la tecnología informática sobre el proceso de auditoría. Estos profesionales realizan ahora auditorías financieras, operativas y de los sistemas de información.

Informe COSO

El informe COSO define el control interno, describe sus componentes, y provee criterios contra los cuales pueden evaluarse los sistemas de control. El informe ofrece una guía para la elaboración de informes públicos sobre control interno y provee materiales que la gerencia, los auditores y otros pueden utilizar para evaluar un sistema de control interno. Dos objetivos principales del informe son (1) establecer una definición común de control interno que sirva a muchas partes diferentes, y (2) provee un estándar contra el cual las organizaciones pueden evaluar sus sistemas de control y determinar como mejorarlos.

Definición: El informe COSO define control interno como: un proceso, efectuado por el directorio, la gerencia y otro personal de la entidad, diseñado para proveer un aseguramiento razonable en relación al logro de los objetivos en las siguientes categorías:

- efectividad y eficiencia de las operaciones
- confiabilidad de los reportes financieros
- cumplimiento con las leyes y regulaciones aplicables.

Aunque el informe define el control interno como un proceso, recomienda evaluar la efectividad del control interno a un momento dado.

Componentes: El sistema de control interno consiste en cinco componentes interrelacionados: (1) ambiente de control, (2) evaluación de riesgos, (3) actividades de control, (4) información y comunicación, y (5) monitoreo. El ambiente de control provee la base para los otros componentes. El mismo abarca factores tales como filosofía y estilo operativo de la gerencia, políticas y prácticas de recursos humanos, la integridad y valores éticos de los empleados, la estructura organizacional, y la atención y dirección del directorio. El informe COSO brinda una guía para evaluar cada uno de estos factores. Por ejemplo, la filosofía gerencial y el estilo operativo pueden ser evaluados examinando la naturaleza de los riesgos del negocio que acepta la

gerencia, la frecuencia de su interacción con los subordinados, y su actitud hacia los informes financieros.

La evaluación de riesgo consiste en la identificación del riesgo y el análisis del riesgo. La identificación del riesgo incluye examinar factores externos tales como los desarrollos tecnológicos, la competencia y los cambios económicos, y factores internos tales como calidad del personal, la naturaleza de las actividades de la entidad, y las características de procesamiento del sistema de información. El análisis de riesgo involucra estimar la significación del riesgo, evaluar la probabilidad de que ocurra y considerar cómo administrarlo.

Las actividades de control consisten en las políticas y procedimientos que aseguran que los empleados lleven a cabo las directivas de la gerencia. Las actividades de control incluyen revisiones del sistema de control, los controles físicos, la segregación de tareas y los controles de los sistemas de información. Los controles sobre los sistemas de información incluyen los controles generales y los controles de las aplicaciones. Controles generales son aquellos que cubren el acceso, el desarrollo de software y sistemas. Controles de las aplicaciones son aquellos que previenen que ingresen errores en el sistema o detectan y corrigen errores presentes en el sistema.

La entidad obtiene información pertinente y la comunica a través de la organización. El sistema de información identifica, captura y reporta información financiera y operativa que es útil para controlar las actividades de la organización. Dentro de la organización, el personal debe recibir el mensaje que ellos deben comprender sus roles en el sistema de control interno, tomar seriamente sus responsabilidades por el control interno, y, si es necesario, reportar problemas a los altos niveles de gerencia. Fuera de la entidad, los individuos y organizaciones que suministran o reciben bienes o servicios deben recibir el mensaje de que la entidad no tolerará acciones impropias.

La gerencia monitorea el sistema de control revisando el output generado por las actividades regulares de control y realizando evaluaciones especiales. Las actividades regulares de control incluyen comparar los activos físicos con los datos registrados, seminarios de entrenamiento, y exámenes realizados por auditores internos y externos. Las evaluaciones especiales pueden ser de distinto alcance y frecuencia. Las deficiencias encontradas durante las actividades regulares de control son normalmente reportadas al supervisor a cargo; las deficiencias detectadas durante evaluaciones especiales son normalmente comunicadas a los niveles altos de la organización.

Otros Conceptos: El informe COSO encara las limitaciones de un sistema de control interno y los roles y responsabilidades de las partes que afectan a un sistema. Las limitaciones incluyen el juicio humano defectuoso, falta de comprensión de las instrucciones, errores, atropellos de la gerencia, colusión, y consideraciones de costo versus beneficio.

El informe COSO define deficiencias como "condiciones dentro de un sistema de control interno digno de atención". Las deficiencias deberían ser reportadas a la persona responsable por la actividad y a la gerencia que está como mínimo un nivel por encima del individuo responsable.

Un sistema de control interno es juzgado efectivo si están presentes y funcionando efectivamente los cinco componentes respecto de las operaciones, los reportes financieros y el cumplimiento.

Comparación de COBIT, SAC y COSO

COBIT, SAC y COSO definen el control interno, describen sus componentes y proveen herramientas de evaluación. SAC y COSO también sugieren formas de reportar los problemas de control interno. Adicionalmente COBIT provee una estructura amplia facilitando el análisis y comunicación de las observaciones de control interno. Esta sección compara las contribuciones que hacen los documentos individuales a cada una de estas áreas.

Definiciones

Aunque las tres definiciones de control contienen esencialmente los mismos conceptos, el énfasis es algo diferente. COBIT ve el control interno como un proceso que incluye políticas, procedimientos, prácticas y estructuras organizacionales que soportan procesos y objetivos de negocio. SAC enfatiza que el control interno es un sistema, ej. que el control interno es un conjunto de funciones, subsistemas, y gente y sus interrelaciones. COSO acentúa el control interno como un proceso, ej. el control interno debería ser una parte integrante de las actividades del negocio en curso.

La gente es parte del sistema de control interno. COBIT clasifica a la gente (definida como habilidad, concientización y productividad del personal para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información) como uno de los recursos primarios administrados por distintos procesos de tecnología informática. El involucramiento de la gente se ha hecho más explícito a medida que los documentos evolucionaron. SAC define explícitamente a la gente como una parte integral del sistema de control interno. COSO denota que la gente involucrada con el control interno son miembros del Directorio, la gerencia, u otro personal de la entidad. Los documentos acuerdan que la gerencia es la parte responsable por establecer, mantener y monitorear el sistema de control interno.

Los tres documentos acentúan el concepto de aseguramiento razonable en lo que se relaciona con el control interno. El control interno no garantiza que la

entidad logrará sus objetivos ni que permanecerá en el negocio. Por lo contrario, el control interno está diseñado para proveer a la dirección con un aseguramiento razonable respecto del logro de los objetivos. Los documentos también reconocen que hay limitaciones inherentes al control interno y que, por consideraciones de costo/beneficio, no serán implementados todos los controles posibles. Las limitaciones inherentes pueden causar que los controles internos sean menos efectivos que lo planeado.

Al presentar las definiciones de control interno, los documentos asumen que la entidad ha establecido objetivos para sus operaciones. COBIT establece la premisa de que estos objetivos son soportados por procesos de negocio. Estos procesos, a la vez, son soportados por la información provista mediante el uso de recursos de tecnología informática. Los requerimientos del negocio para esa información sólo son satisfechos mediante medidas adecuadas de control. SAC establece que el logro de los objetivos del negocio debería ser realizado efectivamente y acentúa que los objetivos deberían ser traducidos en metas mensurables. COSO categoriza los objetivos como operacionales, reportes financieros y cumplimiento. Mientras que SAC y COSO se interesan con objetivos en las tres categorías.

Componentes

El informe SAC describe tres componentes del sistema de control interno. El informe COSO considera cinco componentes. COBIT incorpora los cinco componentes considerados en el informe COSO y los focaliza dentro del entorno de los control interno de tecnología informática. El diseño de COBIT salta la brecha entre los modelos de control de negocios tales como COSO y los sistemas los modelos de control de sistemas de información más altamente técnicos disponibles en todo el mundo. Aunque pueden parecer que los documentos difieren en sus enfoques de los controles, los estudios posteriores revelan muchas similitudes.

Ambiente de Control: COBIT, SAC y COSO todos incluyen el ambiente de control como un componente y discuten esencialmente los mismos conceptos. Los factores que impactan el ambiente de control incluyen la integridad y valores éticos de la gerencia, la competencia del personal, la filosofía gerencial y el estilo operativo, cómo se asignan la autoridad y responsabilidades, y la guía que provee el directorio. COBIT entrelaza las implicancias del ambiente de control en todos los objetivos de control aplicables. Categoriza los procesos dentro de planeamiento y organización, adquisición e implementación, entrega y soporte, y monitoreo. También habla del ambiente de control donde es apropiado. SAC divide el ambiente de control en unas pocas categorías, está más orientado a los sistemas de información, e incluye ideas como parte del ambiente de control que los otros dos documentos discuten como parte de otros componentes. En la

mayoría de las áreas, los conceptos de control interno se desarrollaron de SAC (1991, 1994) a COSO (1992) a COBIT (1996). COSO utiliza una mayor cantidad de categorías de conceptos ambientales y en consecuencia define bien al ambiente de control.

Sistemas de Información y Comunicación: COBIT, SAC y COSO difieren en sus focos y profundidad de tratamiento de los sistemas de información. El foco exclusivo de COBIT es el establecimiento de una estructura de referencia para seguridad y control en tecnología informática. Define un vínculo claro entre los controles de los sistemas de información y los objetivos del negocio. Además, provee objetivos de control validados globalmente para cada proceso de tecnología informática lo cual brinda una guía pragmática de control para todas las partes interesadas. COBIT también provee un vehículo para facilitar las comunicaciones entre la gerencia, los usuarios y los auditores en relación a los controles de los sistemas de información.

SAC se enfoca en los sistemas de información automatizados. El documento examina las relaciones entre control interno y software de sistemas, sistemas de aplicación, y los sistemas departamentales de usuarios finales. El software de sistemas provee el sistema operativo, telecomunicaciones, administración de datos, y otras funciones de utilidad requeridas por los sistemas de aplicación. Los sistemas de aplicación incluyen los sistemas de negocios, financieros y operativos de la entidad (ej: recursos humanos, cuentas a cobrar, y programación de la producción, respectivamente). Los sistemas departamentales y de usuarios finales sirven a las necesidades de grupos específicos de usuarios. Muchos de los volúmenes del informe SAC proveen guías del control interno necesario en cada una de estas áreas.

COSO discute tanto información como comunicación. En su discusión sobre información, COSO revisa la necesidad de capturar la información pertinente interna y externa, el potencial de sistemas estratégicos e integrados, y la necesidad de calidad en los datos. La discusión sobre comunicación se focaliza en transmitir asuntos de control interno, y recoger información competitiva, económica y legislativa.

Actividades de Control: COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad; COSO discute los procedimientos y actividades de control utilizados en toda la entidad. COBIT clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente de procesamiento de información. SAC utiliza cinco esquemas de clasificación diferentes para los procedimientos de control de SI. COSO utiliza solo un esquema de clasificación para los procedimientos de control del sistema de información (SI). La discusión de COSO sobre las actividades de control enfatiza en quién realiza las actividades y en lo operativo más que en los objetivos de informes financieros. COSO también enfatiza la deseabilidad de integrar las actividades de control con la evaluación de riesgos.

Evaluación de Riesgos: COSO identifica la evaluación de riesgos como un componente importante del control interno. COBIT identifica un proceso dentro del ambiente de tecnología informática como evaluando riesgos. Este proceso en particular cae dentro del dominio de planeamiento y organización y tiene seis objetivos específicos de control asociados al mismo. Aunque la evaluación de riesgos no es un componente explícito del sistema de control interno de SAC, el documento contiene amplias discusiones sobre riesgo.

COBIT considera en profundidad varios componentes de evaluación de riesgos en un ambiente de tecnología informática. Esto incluye evaluación de riesgos del negocio, el enfoque de evaluación de riesgos, identificación de riesgos, medición de los riesgos, plan de acción sobre riesgos y aceptación de riesgos. Trata directamente con tipos de riesgos de tecnología informática tales como riesgos de tecnología, seguridad, continuidad y regulatorios. Adicionalmente, considera el riesgo tanto desde la perspectiva global como los específicos de sistemas.

Los conceptos de riesgo presentados en SAC y COSO son similares. Además del riesgo de fallar en satisfacer los objetivos de informes financieros, SAC y COSO tratan los riesgos de fallar en el cumplimiento y especialmente, en los objetivos operativos. COSO discute la identificación de los riesgos internos y externos para toda la entidad y para las actividades individuales. COSO considera también el análisis del riesgo por la gerencia: estimando la significación del riesgo, evaluando su probabilidad de ocurrencia, y considerando como administrarlo. SAC examina los riesgos para el sistema automatizado de información. SAC provee un análisis detallado de los riesgos de SI y explora cómo podría mitigarse cada uno de estos riesgos. SAC y COSO enfatizan en consideraciones de costo/beneficio, la necesidad de interrelacionar los objetivos de la entidad y los controles, la naturaleza “sobre la marcha” de la identificación y evaluación de riesgos, y la habilidad gerencial para ajustar el sistema de control interno de la entidad.

Monitoreo: En contraste con COBIT y COSO, SAC no incluye explícitamente el monitoreo como un componente del sistema de control interno. Todos los documentos asignan a la gerencia la responsabilidad de asegurar que los controles continúen operando apropiadamente. COBIT considera la responsabilidad gerencial de monitorear todos los procesos de tecnología informática y la necesidad de obtener un aseguramiento independiente sobre los controles. Clasifica monitoreo como un dominio – en línea con el ciclo gerencial. SAC reconoce las responsabilidades de los auditores internos para seleccionar áreas de tecnología informática en las cuales una revisión independiente puede producir mayores beneficios y para verificar controles para obtener evidencia del cumplimiento y eficacia vigentes. Como los controles internos deberían evolucionar y evolucionan con el tiempo, COSO reconoce la necesidad de que la gerencia monitoree todo el sistema de control interno de las actividades en marcha incorporadas en el sistema de control en si mismo y mediante evaluaciones especiales dirigidas a áreas o actividades específicas.

Aunque SAC y COSO compartan la misma perspectiva (interna), COSO discute el monitoreo de actividades en términos amplios y SAC discute actividades específicas de monitoreo que deberían ser realizadas por o dentro de los sistemas automatizados de información de la entidad. COBIT en forma parecida, pero de manera más profunda, define los requerimientos y responsabilidades específicas de monitoreo dentro de la función de tecnología informática.

Reportar Problemas de Control Interno

Como marco, COBIT brinda la definición de controles y objetivos de control para procesos específicos de tecnología informática. En forma similar a COSO, los informes de COBIT sobre problemas de control interno se asume que están disponibles para el propietario del proceso de negocio responsable desde distintas fuentes. Estas pueden ir desde la auto-evaluación del control hasta revisiones de auditorías externas – todas realizadas utilizando la estructura COBIT.

SAC asigna a los auditores internos la responsabilidad de evaluar si hay vigentes controles apropiados y si estos controles están funcionando como fueron diseñados. Los auditores internos envían los resultados de sus auditorías financieras, operativas y de los sistemas de información a la gerencia y al comité de auditoría. Ellos deberían articular los costos y beneficios de los cambios propuestos para remediar las deficiencias en el sistema de control interno.

COSO discute cómo recolecta y disemina la gerencia la información sobre las deficiencias de control interno. La gerencia puede tomar conocimiento de las deficiencias a través de los reportes generados por el sistema de control interno en sí mismo, las evaluaciones realizadas por la gerencia o los auditores internos, o comunicaciones de terceras partes tales como clientes, reguladores, o auditores externos. La gerencia quiere información relacionada con cualquier deficiencia que podría afectar la habilidad de la entidad para lograr sus objetivos operativos, de información financiera, o de cumplimiento. COSO recomienda que el personal de la entidad reporte las deficiencias a los supervisores inmediatos y a la gerencia ubicada como mínimo un nivel por encima de la persona directamente responsable. Deberían existir canales de comunicación separados para reportar información sensible.

Período de Tiempo versus Un Momento Dado

COBIT es una estructura modelo. Soporta evaluaciones a un momento dado o durante períodos de tiempo, dependiendo de la preferencia del revisor.

Aunque SAC no establece explícitamente si la efectividad interna debería evaluarse a un momento dado o durante un período de tiempo, parece favorecer más las evaluaciones por períodos de tiempo. Por ejemplo, SAC habla de asegurar la confiabilidad de los datos financieros y operativos, describe el uso de módulos de auditoría incorporados para monitorear y analizar transacciones en forma continuada, y recomienda emplear controles de cambios para asegurar la estabilidad de las aplicaciones y el software de los sistemas.

Aunque COSO acentúa al control interno como un proceso, el informe establece que la efectividad del control interno es un estado o condición del proceso a un momento dado. Si las deficiencias de control interno han sido corregidas a la fecha de emitir un informe, COSO aprueba los informes gerenciales dirigidos a terceros que describen que el control interno es efectivo.

Herramientas

COBIT provee explícitamente una guía para los 32 procesos que define. Esta guía toma la forma de más de 250 objetivos de control. Luego provee ayudas de navegación que todos los usuarios, dependiendo de su perspectiva particular, implementan para organizar y categorizar los objetivos de control de acuerdo con las vistas de control de los procesos de TI, los criterios de información o los recursos de TI.

SAC provee una guía detallada sobre los controles necesarios en el desarrollo, implementación y operación de sistemas automatizados de información a través de la mayoría de sus 12 módulos. Muchos módulos contienen secciones particulares sobre los riesgos y controles asociados a los tópicos discutidos en ese módulo.

El informe COSO brinda al lector herramientas que se pueden utilizar para evaluar el sistema de control interno. Un volumen entero está dedicado a las formas sugeridas para utilizar en el examen de los controles y a muestras de formularios completados.

Conclusión

Presiones internas y externas motivan a las profesiones contables y gerenciales a continuar desarrollando y refinando conceptos de control interno. Este artículo resume y compara documentos importantes resultantes de estos esfuerzos: COBIT, SAC y COSO.

COBIT es una colección de objetivos de control validados globalmente, organizados en procesos y dominios y vinculados a requerimientos de información del negocio. SAC ofrece una guía detallada sobre los efectos de distintos aspectos de la tecnología informática en el sistema de controles internos. COSO presenta una definición común de control interno y enfatiza que los controles internos ayudan a las organizaciones a lograr operaciones eficaces y eficientes, informes financieros confiables, y el cumplimiento de las leyes y regulaciones aplicables. El documento provee una guía sobre la evaluación de sistemas de control, informar públicamente sobre control interno, y realizar evaluaciones de sistemas de control.

COBIT, COSO y SAC contienen muchos de los mismos conceptos de control interno; desde luego, los documentos posteriores trabajaron sobre conceptos de control interno desarrollados por los anteriores. Los documentos difieren en la audiencia a los que van dirigidos, en el propósito del documento, y el nivel de detalle que proveen como guía. Aunque otras partes encontrarán útiles a cada uno de estos documentos, COBIT está dirigido a tres audiencias distintas: la gerencia, los usuarios y los auditores de sistemas de información; SAC está primariamente dirigido a los auditores internos y COSO a los gerentes y directorios.

COBIT está focalizado exclusivamente en los controles sobre la tecnología informática en soporte de los objetivos del negocio. SAC se enfatiza en tecnología informática y COSO provee una visión amplia, a nivel de entidad. SAC y COSO son documentos auto contenidos. Los cuatro documentos se complementan y soportan unos a otros. SAC y COSO son útiles para la audiencia primaria de COBIT, para los legisladores y en general para los interesados en comprender o mejorar el control interno.
