MAZARS

El nuevo SAS 70

Entendiendo los nuevos reportes de control para las organizaciones de servicio

Para los períodos de reporte posteriores al 15 de junio 2011, el informe sobre los controles de una organización de servicios basado en SAS 70 ya no aplicará. Ha sido reemplazado por SSAE 16 en EE.UU. y a nivel internacional por el ISAE 3402.

Antecedentes:

1. El propósito de SAS 70

La declaración sobre normas de auditoría No. 70 (SAS 70 – por sus siglas en inglés), que se desarrolló en 1992, es una norma de EE.UU. emitida por el Instituto Americano de Contadores Públicos (AICPA). El principal objetivo de este estándar es el de proporcionar, al auditor financiero, la evidencia suficiente acerca del estado que guarda el control interno dentro de una organización de servicio, que ha sido subcontratada por el cliente; limitando su alcance de revisión a los controles del cliente auditado: (i)que dependen del servicio subcontratado, (ii)que son relevantes para la producción de información financiera y (iii)que tienen un impacto significativo sobre los estados financieros del cliente. Con el fin de planificar una auditoría sobre los estados financieros del cliente, los auditores, pueden realizar los procedimientos de revisión del control interno en la organización de servicio o basarse en el informe de otro auditor; en dicho informe se incluye la descripción de los controles que han sido implementados por la organización de servicio para salvaguardar la información procesada del cliente. Para las organizaciones de servicio (outsourcing), constituye en muchas ocasiones una carga adicional el hecho de atender diferentes requerimientos de múltiples auditores; sin embargo, un informe del auditor de servicio asegura que todas las organizaciones a las que prestan servicio y sus auditores tengan acceso a la misma información y, en muchos casos, esto puede satisfacer las necesidades del auditor externo de los clientes de la organización de servicios. Además, un informe de auditoría, con una opinión favorable, emitido por una firma independiente de contabilidad, es un diferenciador de la organización de servicio ante sus competidores, al demostrar que ha establecido objetivos de control y opera bajo ellos. Un informe del auditor de servicio también ayuda a una organización de servicio a construir la confianza con sus usuarios (es decir, clientes).

2. Los nuevos estándares (SSAE 16 e ISAE 3402)

En reconocimiento de la necesidad de un estándar internacional de un nivel similar al SAS 70, el Comité Internacional de Normas y Estándares de Auditoría (IAASB) emitió la Norma Internacional sobre Aseguramiento No. 3402 (ISAE 3402), titulada *Informes de Aseguramiento sobre los Controles en una Organización de Servicio*, en diciembre de 2009. En abril de 2010, AICPA refleja esta norma mediante la emisión de la Declaración sobre Normas de Atestiguamiento No. 16 (SSAE 16), titulado *Informe sobre los Controles en una Organización de Servicio*. Ambos son efectivos para los períodos de reporte en el 15 de junio de 2011 o posteriormente y el, ampliamente utilizado, informe SAS 70 sobre los controles en una organización de servicio dejará de ser relevante después de esa fecha.

Los nuevos estándares son muy parecidos al ya conocido SAS 70. Ambos permiten al auditor de una organización de servicio realizar dos tipos diferentes de intervenciones:

- Tipo 2. El auditor de la organización de servicio informa acerca de la objetividad en la descripción del sistema de control interno, hecha por la administración de la organización de servicio; así como sobre la suficiencia en el diseño y la eficacia en la operación de los controles, para alcanzar los objetivos de control descritos, durante un período de tiempo específico.

- Tipo 1. El auditor de la organización de servicio informa acerca de la objetividad en la descripción del sistema de control interno, hecha por la administración de la organización de servicio; así como sobre la suficiencia sólo en el diseño de los controles, para alcanzar los objetivos de control descritos, para una fecha específica.

3. La necesidad de un cambio

El IAASB y AICPA no se están esforzando por revisar por completo las normas sobre la manera de informar acerca de los controles en una organización de servicio. Sin embargo, como se mencionó anteriormente, la necesidad de una norma internacional, en combinación con los esfuerzos de convergencia entre los PCGA de EE.UU. (US GAAP) y las NIIF (IFRS), originaron los nuevos estándares ISAE 3402 y SSAE 16. Por otra parte, el crecimiento en el número de empresas que utilizan servicios de terceros impulsó una actualización a la norma que tiene dos décadas de antigüedad, para satisfacer las demandas del mercado global actual.

Diferencias significativas con SAS 70:

1. Aseveración de la administración

Similares a los requisitos de Sarbanes-Oxley, SSAE 16 e ISAE 3402 requieren de la aseveración por escrito de la administración de la organización de servicio acerca del alcance y objetivos de contratación de un auditor de servicio. Esto implica la asignación de responsabilidades adicionales a la administración de las organizaciones de servicio. Bajo SAS 70, este tipo de servicio fue considerado como de “reporte directo” en el que los auditores de servicio reportaban directamente sobre los controles en la organización de servicio y la administración no estaba obligada a proporcionar una aseveración por escrito. En el marco de las nuevas normas, las intervenciones de los auditores de servicio serán "basadas en las aseveraciones”, por lo que la administración requiere proporcionar una aseveración por escrito, aún cuando el auditor siga informando sobre el tema.

ISAE 3402 y el SSAE 16 detallan de manera específica los requisitos que debe cumplir la administración a fin de proporcionar una aseveración por escrito. Algunos aspectos destacados de la aseveración de la administración son:

- Se incluirá en, o de manera adjunta, la descripción del sistema y se documentará en el informe

- Debe basarse en criterios adecuados que la administración elija para hacer su aseveración y debe indicar cuáles son los criterios utilizados

- Un auditor de servicio no está autorizado a emitir un informe cuando no cuenta con dicha aseveración.

- La administración debe tener una base razonable para su aseveración, lo que puede lograrse a través de: actividades de monitoreo continuo que proporcionan evidencia del diseño y la eficacia operativa de los controles.

La administración debe tomar en cuenta los riesgos que amenazan el logro de los objetivos de control y si los controles existentes son suficientes para mitigar los riesgos. Un proceso formal o informal puede ser utilizado por la administración para evaluar tales riesgos, pero estos riesgos no deben ser incluidos en el informe. Las nuevas normas contienen esquemas de orientación para la aseveración que debe realizar la administración, lo que debe hacer que este proceso sea sencillo de aplicar.

2. Descripción del sistema

A diferencia de la SAS 70, en la que la organización de servicio debe proporcionar una descripción de los controles, las nuevas normas ISAE 3402 y SSAE 16 requieren de una descripción más completa del sistema de la organización de servicio. La descripción del sistema debe incluir lo siguiente:

- Objetivos de control y controles relacionados

- Aspectos del marco de control interno de la organización alineado con COSO (evaluación de riesgos, información y la comunicación, monitoreo, y el ambiente de control)

- Los tipos de servicios prestados, incluidas las diferentes clases de transacciones procesadas

- Los controles compensatorios pertinentes de las entidades usuarias

- Procedimientos y registros contables relacionados con los servicios prestados, incluido el inicio, autorización, registro, procesamiento y corrección de las transacciones

- Cualquier cambio en el sistema durante el período cubierto por el informe

- Hechos y condiciones relevantes adicionales a las transacciones

- El proceso utilizado para elaborar reportes y otra información para las entidades usuarias

Se reconoce que muchas organizaciones de servicio que han obtenido reportes bajo SAS 70 en el pasado, puede encontrar que sus descripciones actuales ya satisfacen los requisitos de las nuevas normas.

3. Alcance en los períodos de diseño de controles (informes Tipo 2)

Para los reportes Tipo 2 de SAS 70, el informe sobre la descripción y la suficiencia del diseño de los controles abarca una fecha determinada, que normalmente, se consideraba el último día del período de presentación de reportes. Sin embargo, las nuevas normas requieren de la opinión sobre el diseño de los controles para todo el período que se examina y no sólo de un punto en el tiempo.

4. Sub-contrato de servicios

Las nuevas normas permiten a las organizaciones de servicios describir el uso de cualquiera servicio sub-contratado, ya sea a través del método inclusivo, o el método de separación. Esto es similar a SAS 70; sin embargo, si la administración opta por utilizar el método inclusivo, por el que la descripción del sistema incluye los controles en la organización sub-contratada; la administración de la organización de servicio debe determinar si los controles en las organizaciones sub-contratadas están adecuadamente diseñados y / o funcionan con eficacia. Por lo tanto, con el fin de hacer esta determinación y en apoyo de su propia aseveración, la administración tendría que obtener una aseveración por escrito de la organización sub-contratada. Una descripción completa de los objetivos de control asociados y los controles de la Organización sub-contratada, así como una carta de representación.

5. Uso de auditoría interna

Un auditor de servicio puede utilizar el trabajo de auditoría interna; sin embargo, el auditor de servicio debe identificar, en las pruebas a los controles, el trabajo realizado por el auditor interno y una descripción de los procedimientos aplicados con respecto a ese trabajo. No se requiere tal divulgación si los miembros de la auditoría interna se utilizan bajo la dirección del auditor de servicio.

6. Reducción de pruebas: uso de evidencia previa

La evaluación del diseño de los controles (tipo 1) o la efectividad operativa de los controles (tipo 2) únicamente debe basarse en pruebas obtenidas durante el período objeto de examen. Como tal, cualquier prueba obtenida en los compromisos anteriores con respecto a la suficiencia del diseño y / o funcionamiento de los controles en períodos anteriores no proporciona una base para una reducción en la evaluación del diseño o las pruebas de los controles, aún cuando puedan ser complementados con las pruebas obtenidas durante el período en curso.

Diferencia entre SSAE 16 e ISAE 3402

1. Lista de diferencias

Aunque la norma de EE.UU. fue escrita para reflejar la norma internacional, algunos requisitos adicionales y aclaraciones por escrito se incluyeron en SSAE 16. A continuación se muestra un resumen de las diferencias identificadas:

	SSAE 16	ISAE 3402
Actos intencionales	Si un auditor de servicio se da cuenta de que existen desviaciones, como resultado de actos intencionales por personal de la organización de servicio, el auditor de servicio deberá evaluar el riesgo de que la descripción del sistema de la empresa de servicio no se presente adecuadamente y que los controles no están adecuadamente diseñados o no funcionan con eficacia.	No existe el requerimiento
Anomalías	Las desviaciones no pueden ser consideradas como anomalías al realizar las pruebas de control.	Permite considerar como anomalías a las desviaciones identificadas en las pruebas de los controles, siempre que no sean representativas de la población.
Asistencia directa	El auditor de servicio puede utilizar la asistencia directa del auditor interno de la organización de servicio.	No se ha considerado
Eventos posteriores	Los eventos posteriores a la fecha del informe deben darse a conocer, si la naturaleza e importancia es tal, que su divulgación sea necesaria para impedir que el informe hacia los usuarios induzca a un error.	No existe el requerimiento
Uso restringido	El informe incluye una declaración que restringe su uso para la administración de la organización de servicio, las entidades usuarias del sistema de la organización de servicio y los auditores del usuario.	La norma no exige la inclusión de una declaración que restringe el uso del informe, pero no prohíbe la inclusión de la declaratoria de uso restringido. Sólo requiere una declaración que indique el uso previsto por el usuario y sus auditores.
Cierre de documentación	Requiere que la documentación de la intervención sea completada a más tardar 60 días después de la emisión del informe	Especifica que la documentación debe ser completada de manera oportuna, pero no especifica un número máximo de días para completarla.
Aceptación y continuidad de la intervención	La administración de la organización de servicio debe proveer, al auditor, una confirmación por escrito de su reconocimiento y aceptación de la responsabilidad al término de la intervención.	No se requiere del reconocimiento pero si de la confirmación por escrito. En caso que la confirmación no sea entregada, el auditor debe abstenerse de opinar.
Abstención de opinión	Si la confirmación no es entregada, el auditor puede abstenerse de opinar o retirarse de la intervención	
Elementos de reporte	La norma SSAE 16 tiene ciertos requerimientos adicionales para los reportes de los auditores de servicio que van más allá de los requerimientos de ISAE 3402	

Cuando la norma de EE.UU. se publicó, el AICPA realizó un análisis para destacar las diferencias entre los dos estándares. La explicación detallada detrás del análisis puede encontrarse en el Anexo B de SSAE 16.

2. Decidir sobre el estándar que debe aplicarse

La decisión de las organizaciones de servicios de si seguir SSAE 16 o ISAE 3402 será evidente en la mayoría de los casos. Si la empresa de servicio se encuentra dentro de los EE.UU., o cuenta con clientes en los EE.UU. que requieren un informe de los controles de la empresa de servicio, SSAE 16 se aplicaría. Sin embargo, con la creciente economía mundial, muchas organizaciones de servicios pueden tener operaciones y / o clientes de todo el mundo y la decisión puede ser más difícil. Por suerte, sólo existen pequeñas diferencias. Sin embargo, una organización de servicio mundial que cuenta con una amplia base de clientes podría tener que llevar a cabo un examen con ambos estándares.

3. Reportes de control para organizaciones de servicio 1,2 y 3 (SOC1, 2, 3)

SSAE 16 realiza una nueva clasificación de la los informes sobre los Controles en Organizaciones de Servicio (SOC). AICPA ha diseñado tres clasificaciones de informes que tienen por objeto proporcionar a los usuarios información valiosa para hacer frente a los riesgos asociados a un servicio externalizado. Han reconocido la creciente demanda de informes sobre los controles ajenos a la información financiera. Los ejemplos incluyen la presentación de informes sobre los controles que rodean la privacidad de la información del cliente o presentación de informes sobre controles que garanticen la disponibilidad y la seguridad de las instalaciones de procesamiento. El establecimiento de esta clasificación hizo hincapié en el uso de los informes SSAE 16. Anteriormente, los informes SAS 70 a menudo fueron mal utilizados como un medio para obtener una seguridad sobre asuntos diferentes a la información financiera. Las nuevas categorías que se han elaborado para corregir estos malos usos son las siguientes:

- SOC 1 – Informe sobre los controles en una organización de servicio alrededor de la información financiera del usuario. Se trata de un informe del 16 de SSAE descrito anteriormente en detalle.

- SOC2 – Informe sobre los controles en una organización de servicio alrededor de la seguridad, disponibilidad, integridad en el procesamiento, confidencialidad o privacidad.

- SOC3 – Informe sobre la confianza en organizaciones de servicios, comúnmente conocidos como “SysTrust”.

Los informes SOC1 y SOC2 parecen ser similares; sin embargo, el reporte tiene un alcance diferente. El informe SOC2 involucra específicamente a uno o más de los 5 principales atributos del sistema:

A) Seguridad – El sistema está protegido en contra de acceso no autorizado (de manera física y lógica).

B) Disponibilidad – El sistema está disponible para su operación y uso de

acuerdo a los términos contratados o acordados.

C) Integridad en el procesamiento – El procesamiento del sistema es completo, correcto, oportuno y autorizado.

D) Confidencialidad – La información clasificada como confidencial, es protegida de acuerdo a los términos contratados o acordados.

E) Privacidad – La información personal es recolectada, usada, retenida, divulgada y eliminada en conformidad con los criterios definidos en los Principios de Privacidad Generalmente Aceptados (GAPP) emitidos por AICPA.

Tanto para SOC1 como para SOC2 existen dos tipos de reportes: el Tipo 1 y Tipo 2, que han sido descritos a detalle con anterioridad.

¿Qué hacer para estar preparado?:

- Determinar el tipo de reporte y el estándar que se va a aplicar.
- Revisar los sub-contratos y las definiciones de auditoría establecidas en el contrato o acordadas.
- Revisar la descripción actual de los sistemas y controles para validar si es adecuada de acuerdo a los nuevos estándares.
- Revisar los estándares para obtener conocimiento adicional acerca de los requerimientos, puede realizarse una evaluación previa para conocer los pasos o actividades necesarias para alcanzar el cumplimiento con las nuevas normas.

MAZARS

Contacto:

Jorge Valencia del Toro
Socio de Consultoría
jorge.valencia@mazars.com.mx
T: +52 (55) 5980 5228

David Mariche
Gerente Senior de Consultoría
david.mariche@mazars.com.mx
T: +52 (55) 5980 5249

Praxity
GLOBAL ALLIANCE OF INDEPENDENT FIRMS