Esquema de Certificación Abierto

Jim Reavis and Daniele Catteddu

Agosto 2013

Contenido

Antecedentes

Cloud Security Alliance (en adelante CSA) ha identificado carencias en el entorno de las TI (Tecnologías de la Información) que están inhibiendo la contratación de servicios seguros y confiables en la nube por parte del mercado. Los clientes no disponen de una vía sencilla y barata para evaluar y comparar la resiliencia, la capacidad de protección de datos y la portabilidad de sus proveedores (de servicios en la nube). Este problema se acentúa por la dimensión internacional de los servicios en la nube, que genera barreras para la adopción de dichos servicios, traspasando fronteras nacionales.

CSA reconoce tanto que una única certificación, regulación u otro régimen de cumplimiento, no puede suplantar a los demás en el gobierno del futuro de las Tecnologías de la Información (TI) como el riesgo de un incremento de costes y complejidad al ya sobrecargado ámbito del cumplimiento. Aun así, la consolidación de la nube como una utilidad global de computación genera la necesidad de armonizar los actuales requerimientos de cumplimiento.

Los estándares de gestión del grupo ISO SC27 tienen el potencial de ser globalmente aceptados; Aun así, existen preguntas relevantes, como la evolución futura de los estándares ISO 27017 y 27018 respecto a ISO 27001 y 27002. CSA está trabajando para influir positivamente en esos resultados aportando su propia propiedad intelectual (en nuestro papel de promotores de estándares).

El estándar AICPA SAS70 y sus sucesores han ganado fuerza como estándares de auditoría en compañías de servicios y son muy conocidos entre los proveedores de servicios en la nube. Sin embargo, carece de una serie de criterios estandarizados para los tipos de objetivos de control que puedan ser evaluados en un proveedor de servicios en la nube.

Los creadores de regulaciones legales, incluyendo el Gobierno Federal de los EEUU, la Comisión Europea y otras entidades también valoran positivamente un esquema de certificación para servicios en la nube.

Todos los intentos anteriores para aseguramiento, auditoría y certificación de tecnologías de la información han sido dificultados por los rápidos cambios y la naturaleza dinámica de la computación en la nube. Tanto los consumidores como los proveedores se beneficiarán del conocimiento de que sus ágiles actividades de cumplimiento respaldadas por CSA serán de aplicación general en los regímenes regulatorios globales.

Análisis de Estado

El Esquema de Certificación Abierto (*Open Certification Framework*, en adelante OCF) de CSA en una iniciativa de la industria para permitir una certificación global, acreditada y basada en la confianza para proveedores de servicios en la nube.

OCF de CSA es un programa flexible, incremental y con diferentes niveles para una certificación de proveedores de servicios en la nube, de acuerdo con los objetivos de control y guías de seguridad de liderazgo de la industria que aporta CSA.

El programa se integrará con las reconocidas auditorías de tercera parte y con los requisitos de informe desarrollados dentro de la comunidad para evitar duplicar costes y esfuerzos.

OCF de CSA está basado en los objetivos de control y estructuras de control continuo definidas dentro del proyecto de investigación STACK GRC (*Gobernance, Risk and Compliance*) de CSA.

OCF de CSA tendrá varios niveles, con reconocimiento de varios

requerimientos de seguridad y niveles de madurez en proveedores y clientes de servicios en la nube. Estos irán desde un nivel de autoevaluación CSA-STAR (*Security, Trust and Assurance Registry*) hasta especificaciones de alta seguridad de tipo control continuo.

OCF de CSA proporciona:

- Un camino aplicable en cualquier geografía para gestionar requerimientos legales con las mejores prácticas globales basadas en la confianza. Por ejemplo, esperamos que los Gobiernos sean firmes implementadores del OCF de CSA para plantear sus propias necesidades particulares como la capa más alta de las necesidades de Gobierno, Riesgo y Cumplimento (en adelante GRC), y proporcionar una certificación ágil para los usuarios de servicios en la nube del sector público.
- Una guía explícita para proveedores sobre cómo usar las herramientas GRC Stack para certificaciones múltiples. Por ejemplo, la documentación de definición de alcance articulará las razones por las que un proveedor puede seguir el camino de la certificación ISO 27001 que incorpore la CSA *Cloud Control Matrix* (en adelante CCM).
- Un "esquema de reconocimiento" que podría permitir a CSA soportar ISO, AICPA y potencialmente otros esquemas que incorporen Propiedad Intelectual de CSA dentro de sus certificaciones o marcos de certificación.

CSA apoya el uso de un certificado para uso múltiple, cuando sea posible.

CSA quiere armonizar y simplificar la provisión de certificaciones, no complicarla.

Un esquema de certificación para servicios en la nube de confianza

Tanto las entidades gubernamentales, como las entidades privadas y el sector público demandan un procedimiento común para evaluar y certificar el nivel de seguridad y privacidad que proveedores de servicio de IaaS, PaaS, SaaS o (X)aaS están proporcionando.

Se supone que un estándar para la privacidad y la seguridad globalmente reconocido debe promover una extensa adopción global de servicios en la nube cubriendo la falta de confianza que actualmente se percibe dentro de los servicios en la nube.

Esta falta de confianza se basa principalmente en las dificultades que tienen los usuarios de la nube para gestionar elementos fundamentales de seguridad con sus proveedores de servicios en la nube, como por ejemplo:

- Comprensión de requerimientos legales y responsabilidades contractuales
- Definición y asignación de responsabilidades
- Garantizar la aplicación de controles.
- Traducción de requerimientos en pruebas/controles/conceptos propios de la nube
- Determinación de los medios para evaluar el análisis de los servicios en la nube y para un seguimiento continúo de la ejecución del contrato de servicios en la nube.

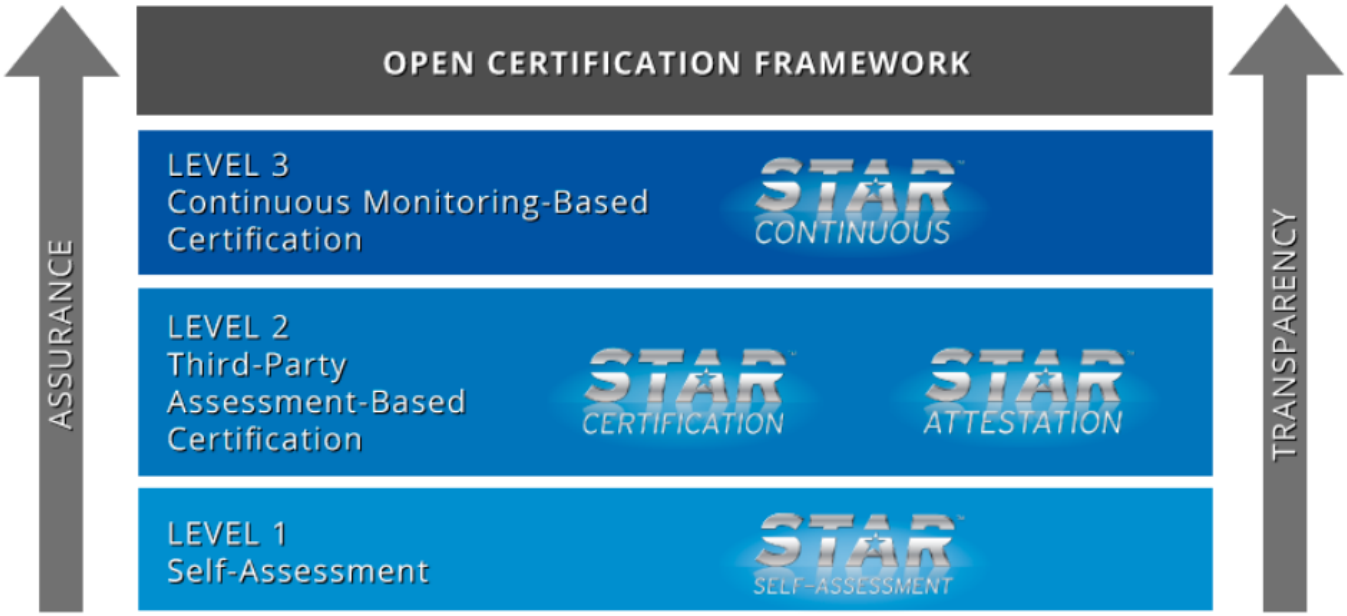
Estos son apoyados por ocho principios de gestión que aseguran que el alcance y los procesos son adecuados y que el Acuerdo de Nivel del Servicio (*Service Level Agreement*, en adelante SLA) gestiona:

- El enfoque a cliente

- Liderazgo
- Involucración de las personas
- Análisis por procesos
- Enfoque de sistemas para la gestión
- Mejora continua
- Toma de decisiones basadas en la evidencia
- Relaciones con suministradores de mutuo beneficio

Estructura del Esquema de Certificación Abierto

El OCF se estructura en 3 NIVELES de CONFIANZA, cada uno de los cuales proporciona un incremento gradual en los niveles de visibilidad y transparencia en las operaciones del Proveedor de Servicios en la Nube y un nivel mayor de seguridad en el cliente de servicios en la Nube.



Nivel 1: Autoevaluación: CSA STAR

Los proveedores de servicios en la nube pueden presentar dos tipos diferentes de informes para indicar su cumplimiento con las mejores prácticas de CSA.

- El Cuestionario CAIQ (Consensus Assessment Initiative Questionnaire)
- Matriz CSA-CCM

Nivel 2: CERTIFICACION STAR (Auditoría de Tercera Parte)

El concepto del esquema es utilizar los requerimientos de la norma de sistemas de gestión ISO 27001 integrado con la CCM de CSA y los propios requisitos internos o las

especificaciones de la organización para evaluar la madurez de sus sistemas. Las respuestas son registradas y posteriormente analizadas por su nivel de madurez. A esta madurez se le asigna una puntuación. Todas las puntuaciones son evaluadas conjuntamente para puntuar los diferentes dominios del sistema de gestión y una puntuación global de todo el sistema de gestión.

Además de lo anterior, también existe la posibilidad para los clientes de tener su propio criterio de rendimiento interno incluido en el proceso para su examen y puntuación por los auditores.

Nivel 2: Testeo STAR (Auditoría de Terceros)

El concepto del esquema es utilizar los requerimientos para testeos AICPA SOC2, ejecutados de acuerdo con la sección AT 101, de los test estándar AICPA, ampliados con la CSA-CCM. Puede encontrarse información adicional en el posicionamiento de CSA sobre este tema, disponible en https://downloads.cloudsecurityalliance.org/initiatives/collaborate/aicpa/CSA_Position_Paper_on_AICPA_Service_Organization_Control_Reports.pdf

Nivel 3: La certificación basada en el seguimiento continuo

Se encuentra actualmente en desarrollo y su concepto busca implementar un seguimiento en tiempo cuasi-real del cumplimiento de los requisitos de cliente, basado en la recogida continua de evidencias de auditoría.

CERTIFICACION STAR (Nivel 2)

La nube tiene unos riesgos de información únicos, en tanto que los usuarios finales están más preocupados por la seguridad de su información y si pueden confiar en los Proveedores de Servicios en la Nube (Cloud Service Providers, CSPs,)

Por ello, es necesario un rigor adicional para asegurar que los riesgos están siendo gestionados y el alcance es determinado por un SLA.

La Certificación STAR evalúa la eficiencia del sistema de gestión de una organización y asegura que el alcance, los procesos y los objetivos son "Adecuados para su Propósito". El uso de niveles de madurez ayudará a la organización a priorizar áreas de mejora y conducirla a la excelencia empresarial, mejor que un modelo de "aprobar o suspender". También permite una comparación efectiva con otras organizaciones del mismo sector.

Este servicio mejorado de evaluación es un enfoque centrado en los beneficios empresariales estratégicos y operativos, así como en las relaciones eficaces de colaboración. Basado en el enfoque del ciclo PDCA (Plan, Do, Check, Act) y el conjunto de criterios específico incluidos en la CCM, este servicio permite al auditor puntuar numéricamente el desempeño de la compañía, la sostenibilidad a largo plazo y los riesgos, además de asegurar que los SLAs son determinados, permitiendo una gestión madura para cuantificar y medir la mejora año tras año.

A través de la aplicación de principios de gestión y controles, tal y como se indica en la CCM, el auditor puede centrarse en proporcionar oportunidades reales para la mejora del desempeño que permitan a la organización concentrarse en desarrollar sistemas de gestión de negocio existentes e incorporar las mejores prácticas empresariales.

La CCM está específicamente diseñada para proporcionar los principios fundamentales de seguridad, para orientar a los proveedores de servicios en la nube y para asistir a los clientes potenciales de estos servicios en la evaluación del riesgo global de seguridad de un

proveedor de servicios en la nube. Como marco, la CCM proporciona a las organizaciones la estructura, el detalle y la transparencia requeridos en relación con la seguridad de la información de manera personalizada para la industria de servicios en la nube. La CCM refuerza los controles de seguridad de la información existentes, enfatizando en los requisitos de control de seguridad de la información del negocio, reduciendo e identificando amenazas y vulnerabilidades de seguridad consistentes en la nube. Proporciona una seguridad estandarizada y una gestión del riesgo operacional y busca normalizar las expectativas de seguridad, taxonomía y terminología y la implantación de medidas de seguridad en la nube.

La CCM está pensada para poder ser integrada en la auditoría por el auditor, referenciando los controles aplicables de la CCM con los controles asociados de ISO 27001 y utilizando la matriz de referencia cruzada proporcionada. Los datos de salida deberán ser el resultado del desempeño global de la organización dentro del alcance de la certificación.

Evaluadores Cualificados (Auditores) para la CERTIFICACION STAR

Un comité de certificación definirá los requisitos y el proceso de certificación del auditor. El proceso de certificación del auditor será gestionado por British Standards Institution (BSI).

Cronograma del Esquema de Certificación Abierto (OCF):

- El Nivel 1 está actualmente disponible a través de STAR
- El Esquema de Certificación Abierto está disponible desde el 1er trimestre de 2013
- El esquema de Certificación de Auditores está disponible desde el 3er trimestre de 2013
- La Certificación STAR para proveedores está disponible desde el 3er trimestre de 2013
- El Nivel 3 de Seguimiento Continuo no estará disponible antes de 2015

Estructura de Gobierno

El OCF estará bajo el control directo de CSA, que será apoyado por la Junta Directiva del OCF y la Junta Directiva del GRC Stack. El Comité de dirección del OCF y la Junta Directiva GRC Stack proporcionarán asesoramiento estratégico a CSA en el desarrollo e implementación del OCF.

La Junta Directiva del GRC Stack proporcionará asesoramiento y sugerirá la dirección técnica para:

- Mejorar el marco conceptual del GRC Stack
- Mejorar los componentes existentes del GRC Stack
- Implementación del marco del GRC Stack (desde el uso de la CCM hasta una solución de seguimiento continuo completa)

Los miembros de la Junta Directiva del GRC Stack también actuarán como embajadores del GRC Stack en la comunidad.

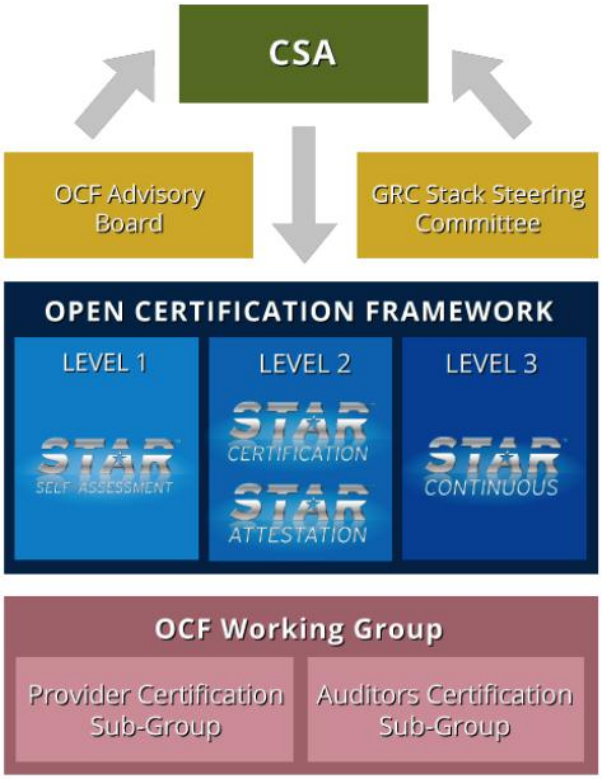
La Junta Directiva el Esquema de Certificación Abierto (OCF SC) proporcionará asesoramiento y dirección estratégica en:

- Mejorar el marco conceptual del OCF.

(Definir y mejorar el Nivel 2 del esquema de certificación)

(Definir y mejorar el Nivel 3 del esquema de certificación)

- Definición de los requisitos de transparencia (requisito de divulgación mínima en el alcance de certificación y los resultados de auditoría)
- Gestión de los requisitos de cumplimiento legal y regulatorio (definición, en cooperación con GRC SC del cumplimiento legal y normativo nacional y con las capas de control específicas del sector).
- Mejorar STAR
- Mejorar los componentes existentes del GRC Stack
- Implantación del OCF



Los miembros de la Junta Directiva del Esquema de Certificación Abierta (OCF SC) también actuarán como embajadores del OCF en la comunidad.

El Grupo de Trabajo del OCF, compuesto por el Subgrupo de Trabajo Proveedor de Certificación y el Subgrupo de Auditores de Certificación, definirán el Nivel del Esquema de Certificación STAR y el esquema de certificación del auditor (ver Capitulo del Grupo de Trabajo del OCF).