Open Certification Framework

Vision Statement, Rev. 1

August 2013

BACKGROUND

The Cloud Security Alliance has identified gaps within the IT ecosystem that are inhibiting market adoption of secure and reliable cloud services. Consumers do not have simple, cost effective ways to evaluate and compare their providers' resilience, data protection capabilities and service portability. This problem is exacerbated by the international dimension of cloud services, causing significant barriers to adoption of cloud services spanning national boundaries.

CSA recognizes that no single certification, regulation or other compliance regime will supplant all others in governing the future of IT as well as the risk of adding more cost and complexity to the already overloaded compliance landscape. However, the rise of cloud as a global compute utility creates a mandate to better harmonize compliance concerns.

Standards inside ISO SC27 have potential for being globally accepted; however, there are significant questions as to the future of 27017/8 versus 27001/2. CSA is working to positively influence these outcomes with its own IP (in our role of Standards Incubator)

AICPA SAS70 and its successors have gained significant traction as a standard for auditing statements for services companies and is popular with many cloud providers. However, it lacks a standard set of criteria for the types of control objectives which should be evaluated within a cloud provider.

Policy Makers, including USA Federal Government, the European Commission and others support a cloud service certification scheme.

All of the above traditional approaches to IT assurance, audit and certification are challenged by the rapid changes and dynamic nature of cloud computing. Both consumers and providers alike will benefit from the knowledge that their agile CSA-backed compliance activities will be broadly applicable within global regulatory regimes.

Vision statement

The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

The CSA Open Certification Framework is a program for flexible, incremental and multi-layered cloud provider certification according to the Cloud Security Alliance's industry leading security guidance and control objectives.

The program will integrate with popular third-party assessment and attestation statements developed within the public accounting community to avoid duplication of effort and cost.

The CSA Open Certification Framework is based upon the control objectives and continuous monitoring structure as defined within the CSA GRC (Governance, Risk and Compliance) Stack research projects.

The CSA Open Certification Framework will support several tiers, recognizing the varying assurance requirements and maturity levels of providers and consumers. These will range from the CSA Security, Trust and Assurance Registry (STAR) self-assessment to high-assurance specifications that are continuously monitored.

The CSA Open Certification Framework provides:

- A path for any region to address compliance concerns with trusted, global best practices. For example, we expect governments to be heavy adopters of the CSA Open Certification Framework to layer their own unique requirements on top of the GRC Stack and provide agile certification of public sector cloud usage.
- An explicit guidance for providers on how to use GRC Stack tools for multiple certification efforts. For example, scoping documentation will articulate the means by which a provider may follow an ISO/IEC 27001 certification path that incorporates the CSA Cloud Controls Matrix (CCM).
- A "recognition scheme" that would allow us to support ISO, AICPA and potentially others that incorporate CSA IP inside of their certifications/framework.

CSA supports certify-once, use-often, where possible.

CSA wants to harmonize and simplifying provider certifications, not complicate them.

A certification schema for trusted cloud services

Governments, Private and Public sectors users demand a standard way to evaluate and certify the level of security and privacy that a certain IaaS, PaaS, SaaS or (X)aaS is providing.

Such a globally recognized standard for security and privacy is supposed to foster an extensive global adoption of Cloud Computing by filling the gap of trust currently perceived within cloud computing services.

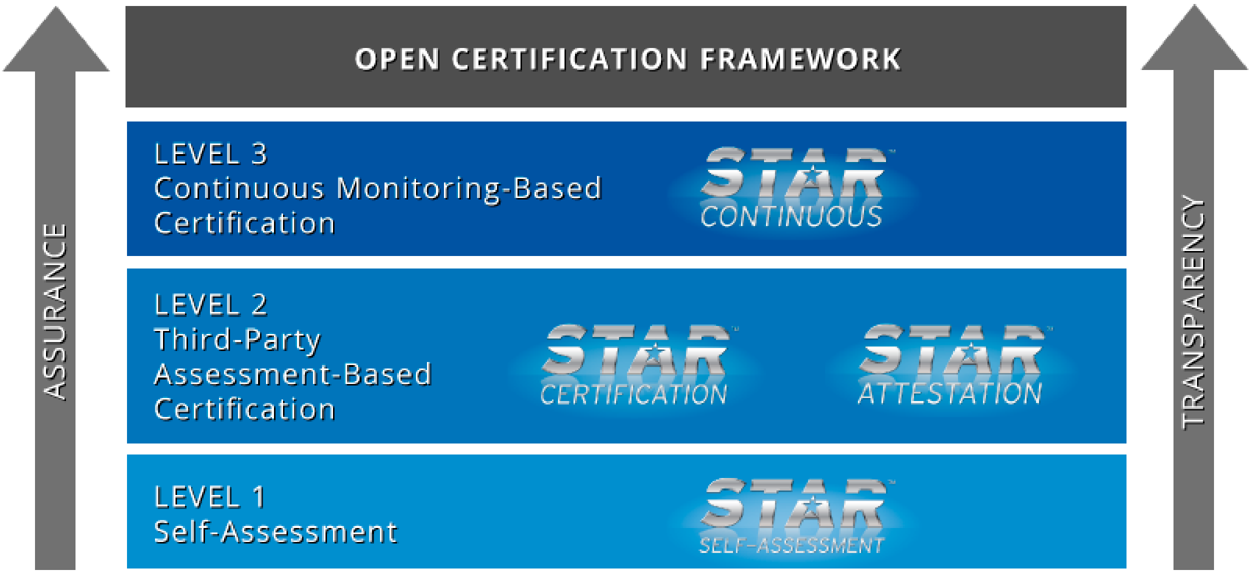
This gap of trust mainly lies down in the difficulties of cloud users in addressing fundamental assurance issues with cloud providers, such as:

- Understanding legal compliance and contractual liabilities,
- Defining and allocating responsibilities
- Enforcing accountability
- Translating requirements into cloud language/controls/checks
- Identifying means for an ex-ante analysis assessment of cloud services and for a
- Continuous monitoring of cloud service contract execution

These are supported by eight management principles that ensure the scope and processes are fit for purpose and SLA driven:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- Systems approach to management
- Continual improvement
- Evidence-based approach to decision making
- Mutually beneficial supplier relationships

Open Certification Framework Structure



The open certification framework is structured on three levels of trust, each one of them providing an incremental level of visibility and transparency into the operations of the cloud service provider and a higher level of assurance to the cloud consumer.

LEVEL 1: The STAR Self-Assessment
Cloud providers can submit two different types of reports to indicate their compliance with CSA best practices:

The Consensus Assessments Initiative Questionnaire (CAIQ),
Cloud Controls Matrix (CCM)

LEVEL 2: STAR CERTIFICATION (Third Party Assessment)
The concept of the scheme is to use the requirements of the ISO/IEC 27001:2005 management systems standard integrated with the CSA Cloud Control Matrix (CCM) and an organization's own internal requirements or specifications to assess how mature their systems are. The answers are recorded and later analyzed for their level of maturity. This maturity is given a score. All the scores are then brought together to give scores for the different domains of their management system and an overall score for their whole system.

In addition to the above, there is also the opportunity for clients to have their own internal performance criteria included into the process to be looked at and scored by the assessors.

LEVEL 2: STAR Attestation (Third Party Assessment)
The concept of the scheme is to use the requirements of an AICPA SOC 2 attestation examination conducted in accordance with AT section 101 of the AICPA attestation standards supplemented by CSA Cloud Controls Matrix (CCM). Further details can be found in the CSA Position Paper on AICPA Service Organization Control Reports https://downloads.cloudsecurityalliance.org/initiatives/collaborate/aicpa/CSA_Position_Paper_on_AICPA_Service_Organization_Control_Reports.pdf

LEVEL 3: Continuous Monitoring based certification, is currently under development, and its concept is to implement a near real time monitoring of the fulfillment of consumer requirements, based on continuous collection of auditing evidence.

STAR CERTIFICATION (Level 2)

The Cloud has unique information risks while end users are concerned with the security of their information and whether they can trust cloud service providers (CSPs).

Additional rigor is required to ensure that risks are being addressed and the scope is SLA driven.

STAR CERTIFICATION evaluates the efficiency of an organization's information management system and ensures the scope, processes and objectives are fit for purpose. Using maturity levels, it will help organizations prioritize areas for improvement and lead them towards business excellence, rather than using a pass or fail model. It also enables effective comparison across other organizations in the applicable sector.

This enhanced assessment service is an approach focused on the strategic & operational business benefits as well as effective partnership relationships. Based upon the Plan, Do, Check, Act (PDCA) approach and the specified set of criteria as outlined in the Cloud Controls Matrix (CCM), this service enables the assessor to numerically score a company's performance, on long-term sustainability and risks, in addition to ensuring they are SLA driven, allowing senior management to quantify and measure improvement year on year,

Through the application of the management principles and controls, as outlined in the CCM, the assessor can focus on providing key performance improvement opportunities that will allow the organization to concentrate on advancing existing business management systems and incorporating business best practice.

The CCM is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. As a framework, the CCM provides organizations with the required structure, detail and clarity relating to information security tailored to the cloud industry. The CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

The Cloud Controls Matrix is meant to be integrated into the assessment by the assessor, referencing the applicable CCM control to the associated ISO 27001 controls using the matrix cross-reference provided. The output will be the result of the overall performance of the organization within the scope of certification.

Qualified Assessors (Auditors) for STAR CERTIFICATION

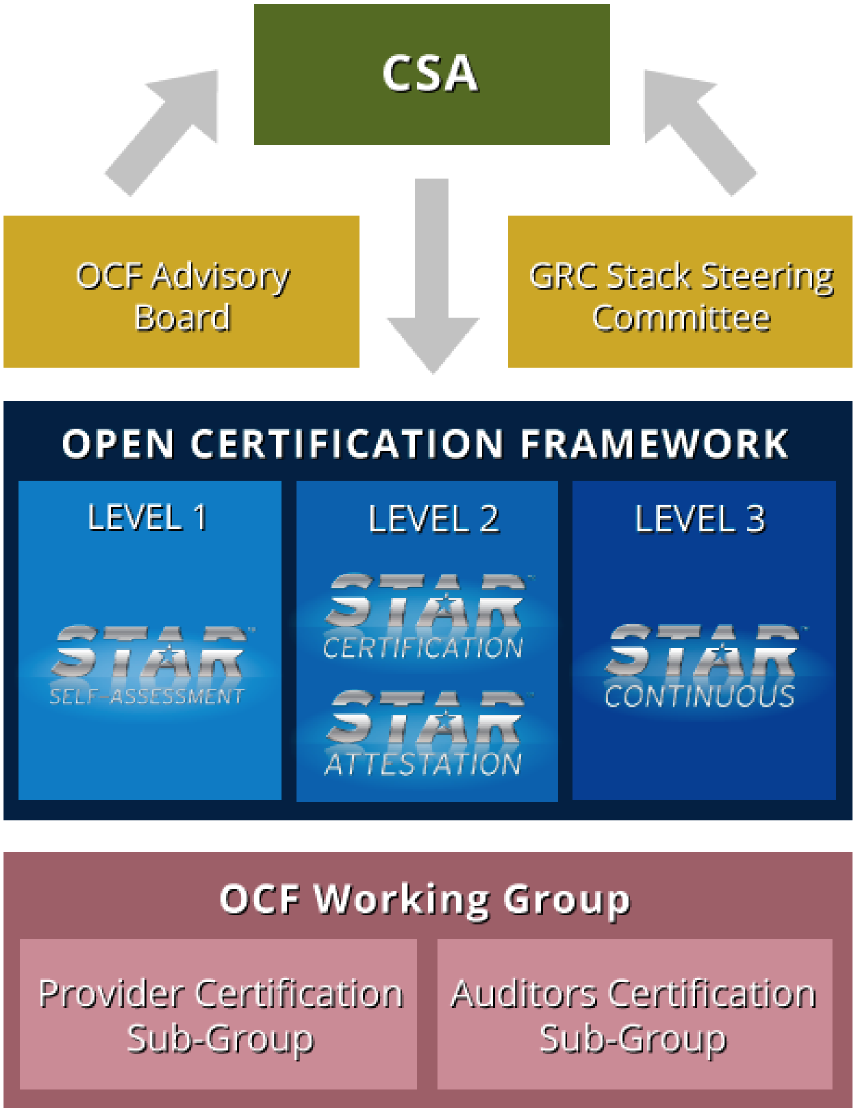
An auditor certification board will define auditor requirements and the auditor certification process.
The auditor certification process will be managed by the British Standards Institution (BSI)

OCF Timeline

- LEVEL 1 is currently available through STAR
- The Open Certification Framework will be available in Q1 2013
- The Auditor Certification scheme will be available in Q3 2013
- The STAR Certification for provider will be available in Q3 2013

- The STAR Attestation schema will be available in Q1 2014
- The LEVEL 3 Continuous Monitoring will be available not earlier than 2015

Governance Structure



OCF will be under the direct control of CSA, which will be supported by an OCF Steering Committee (SC) and GRC Stack Steering Committee. The OCF SC and GRC Stack SC will provide strategic advice to CSA Management on the development and implementation of the OCF.

The GRC Stack SC will provide advice and suggest technical direction for:

- Improving the conceptual GRC Stack framework
- Improving the existing components of GRC Stack
- Implementation of the GRC Stack framework (from the use of CCM to full continuous monitoring solutions).

GRC Stack SC members will also act as ambassadors of GRC Stack in the community.

The OCF SC will provide advice and strategic direction on:

- Improving the OCF conceptual framework.
  (Define and improve LEVEL 2 certification scheme)
  (Define and improve LEVEL 3 certification scheme)
- Defining transparency requirements (minimal disclosure requirement on the scope of the certification and assessment/audit results).
- Addressing legal and regulatory compliance requirements (definition, in cooperation with GRC SC of the national legal and regulatory compliance, and sector specific controls layers)
- Improving STAR
- Improving the existing components of GRC Stack
- Implementation of the OCF.

OCF SC members will also act as ambassadors of OCF in the community.

The OCF Working Group, composed by Provider Certification Sub-Working Group and Auditors Certification Sub-Group will define the Level STAR Certification scheme and auditor certification scheme (see the OCF Working Group Charter).