Security Certification for Cloud Services: The CSA STAR Certification

Damir Savanović, CISA, CISM, CCSK, PRIS
Senior Analyst and Researcher @ Cloud Security Alliance
About the Cloud Security Alliance

- Global, not-for-profit organisation
- Over 65,000 individual members, more than 200 corporate members, and 65 chapters
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”
About the Cloud Security Alliance

- Research
  - https://cloudsecurityalliance.org/research/
- Advise Governments and Private companies
- Education – Professional Certification – Training
  - https://cloudsecurityalliance.org/education/
- Providers Certification
  - https://cloudsecurityalliance.org/star/
- Standards
  - https://cloudsecurityalliance.org/isc/
- Events
  - https://cloudsecurityalliance.org/events/
Cloud BARRIERS

- (Perceived) Loss of control
- Lack of clarity around the definition and attribution of responsibilities and liabilities
- Difficulties achieving accountability across the cloud supply chain
- Incoherent global (and even sometimes regional and national) legal framework and compliance regimes
...and more barriers

- The lack of transparency of some service providers or brokers
- Lack of clarity in Service Level Agreements
- Lack of interoperability.
- Lack of awareness and expertise
OPENNESS & TRANSPARENCY
Certification for cloud services

- In the Agenda of the EC
- Requested from Art29 WP as a measure for privacy compliance
- Already part of the cloud strategy in countries such as USA, Singapore, Thailand, China, Honk Kong, Taiwan,
- In Europe various Member States are looking at a certification/accreditation schema for cloud service (especially in Public Procurement)
- The UK G-Cloud is based on a logic of companies accredited to offer service in the App Store
EC Cloud Strategy

The Cloud computing strategy

- The European Commission's strategy 'Unleashing the potential of cloud computing in Europe'
  - Adopted on 27/9/2012. Its aim is to speed up the cloud uptake across Europe

Cloud strategy's key actions

- Cutting through the jungle of standards
- Development of model safe and fair contract terms
- A European Cloud Partnership to drive innovation and growth for the public sector.

DG CONNECT working groups for the implementation of the strategy

- ETSI: Cloud Standards Coordination
  - Launched on 4/12/2012
- The Cloud Select Industry Group on Service Level Agreements
  - Launched on 21/03/2013
- The Cloud Select Industry Group on Certification Schemes
  - Launched on 10/04/2013
- The Cloud Selected Industry Group on Code of Conduct
  - Launched on 21/02/2013
- Research: The Cloud Expert Group
  - Now completed
- The European Cloud Partnership
  - Steering Board
    - Launched on 19/11/2012
- Cloud for Europe Initiative
  - Public Launch 14-15/11/2013
Certification Challenges

- Provide a globally relevant certification to reduce duplication of efforts
- Address localized, national-state and regional compliance needs
- Address industry specific requirements
- Address different assurance requirements
- Address “certification staleness” – assure provider is still secure after “point in time” certification
- Do all of the above while recognizing the dynamic and fast-changing world that is cloud
Debating around Certification for cloud

The debate around cloud certification has been based on the following key aspects:

- Suitability of existing security certification schemes (e.g. ISO 27001 or SSAE16/SOC1-2-3) for the cloud market vs. the needs to introduce new schemes
- Mandatory vs. voluntary industry driven approaches
- Global vs. Regional/National schemes
- Cost
- Transparency
- Assurance and maturity/capability models
CloudWatch

A European cloud observatory supporting cloud policies, standard profiles and services

D4.1 – Cloud certification guidelines and recommendations
"One of the main challenges, when it comes to cloud computing, consists of building trust and confidence in cloud computing services. The variety of existing standards, with a varying degree of maturity, as well as the lack of clarity around the suitability of currently available certification schemes, are not really helpful in these trust building efforts. Concerns are being voiced about compliance issues as well as the effectiveness and efficiency of traditional security governance and protection mechanisms applied to the cloud computing" and".?

Our analysis has shown that cloud computing governance and assurance standards specifically developed for and aimed at the cloud already exist (e.g., cloud controls framework, security cloud architectures, continuous monitoring of cloud service provider’s) and some of them are considered as sufficiently mature to be adopted."
Certification SIG questionnaire

- Background: the Selected Industry Group (SIG) certification expert group supports the EC in implementing action 1 of the Europe Cloud Strategy.
- The SIG-certification agreed that the group will produce a list of security certification requirements and schemes which are fit-for-purpose to certify cloud computing services.
- The SIG-certification decided to launch a survey.
- Prepared by CSA/ENISA, reviewed by the SIG members and EC.
- Reporting data where captured by 13-APR-2013.
## Mapping schemes / Objectives

<table>
<thead>
<tr>
<th>Certification Scheme</th>
<th>Improve trust</th>
<th>Improve security</th>
<th>Efficiency of procurement</th>
<th>Compliance</th>
<th>Transparency</th>
<th>Cost-effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SOC 1-2-3-</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Partial</td>
<td>No</td>
<td>Partial</td>
</tr>
<tr>
<td>CSA STAR – OCF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EuroPrice</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>ECSA</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
</tr>
<tr>
<td>USA-FedRAMP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Singapore-MTCS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Mapping schemes / features

<table>
<thead>
<tr>
<th>Certification Scheme</th>
<th>Transparency</th>
<th>Scalability</th>
<th>Flexibility</th>
<th>Privacy-relevance</th>
<th>Comparability</th>
<th>Specific</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>No</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SOC 1-2-3-</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CSA STAR – OCF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EuroPrice</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ECSA</td>
<td>Partial</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>USA-FedRAMP</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Singapore-MTCS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Partial</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
A suitable certification scheme should:

1) Support **transparency** to the highest degree. Providing visibility into the security & privacy capabilities of a CSP and:
   - Supporting informed and risk based decisions
   - Transforming security and privacy capabilities in market differentiator
   - Avoiding unnecessary regulatory intervention
   - Increasing the level of trust in the cloud market

2) Be **scalable**, **flexible** and **cost efficient** to accommodate the needs of:
   - Organizations of different sizes, operating at the various layers of the cloud stack (...aaS) and in different sectors
   - Organizations with varying assurance requirements.
Most of the certification schemes considered provide scalability. Some seem to be cost efficient, only a few clearly provide the necessary level of flexibility.

Lack of flexibility might prevent the technical frameworks to keep the pace of change the cloud market, therefore failing to satisfy changing requirements.

Only a few certification schemes are able to address the needs of organizations with varying level of assurance.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
Launched in 2011, the CSA STAR is the first step in improving transparency and assurance in the cloud.

The STAR is a publicly accessible registry that documents the security controls provided by cloud computing offerings.

Helps users to assess the security of cloud providers.

Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading to higher quality procurement experiences.

It is based on a multilayered structure defined by Open Certification Framework Working Group.
Minimum Common Denominator
Cloud Control Matrix V3.0.1

- **Cloud specific**: Security Control Framework designed with Cloud in mind
- **Global effort**: developed with the contribution of more than 500 subject matter experts
- **Widely adopted** by thousands of companies and Government
- Structured in **16 domains and 133 controls**
- Ensure **due care** is taken in the cloud provider supply chain
- It is mapped against all the other relevant standards: ISO 27001, COBIT, HIPAA, NIST SP800-53, FedRamp, PCI, BITS, GAPP, Jericho Forum, NERC CIP, ENISA IAF, etc
- **Flexible**: It will be updated to keep pace with changes.
- Wants to drive continuous improvement
- Freely available on CSA web site: please download it, use it, try to break it if you can...and then tell us if we need to change anything..
CCM V3.0.1 – 16 CONTROL AREAS

136 CONTROLS
Cloud Controls Matrix v3.0

133 CONTROLS
Cloud Controls Matrix v3.0.1
CCM V3.0.1

» Current Version: Released July 10, 2014

» Builds upon the 5 new domains introduced in v3.0
  » Mobile Security
  » Supply Chain Management
  » Transparency & Accountability; Interoperability & Portability
  » Encryption & Key Management

» Continued improvements in controls including:
  » Language and auditability
  » Reduction of overlapping controls
  » Removed Customer and Provider references within the language
New and Updated Mappings including:
- AICPA 2014 TSC
- ISO/IEC 27001-2013
- PCI DSS v3.0
- NIST SP800-53 R3 App J
- ENISA IAF
- 95/46/EC - European Union Data Protection Directive
- HIPAA / HITECH Act
- COBIT 5.0
- Canada PIPEDA
- COPPA
- ODCA UM: PA R2.0
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
Self Assessments based on Consensus Assessments Initiative Questionnaire and Cloud Control Matrix
Voluntary industry action promoting transparency
Open to ALL cloud providers
Since the initial launch had tremendous growth
92 entries: including Amazon Web Services, Box.com, HP, Microsoft, Ping Identity, Red Hat, IntracomTelecom, Symantec, Terremark and many others
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
CSA STAR Continuous will be based on a continuous auditing/assessment of relevant security properties.

It will built on the following CSA best practices/standards:

- Cloud Control Matrix (CCM)
- Cloud Trust Protocol (CTP)
- CloudAudit (A6)

CSA STAR Continuous is currently under development and the target date of delivery is 2015.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
What is CSA STAR Certification?
What is CSA STAR Certification?

- The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider.
- Technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 & the CSA CCM
- Integrates ISO/IEC 27001:2013 with the CSA CCM as additional or compensating controls.
- Measures the capability levels of the cloud service.
- Evaluates the efficiency of an organization’s ISMS and ensures the scope, processes and objectives are “Fit for Purpose.”
- Based upon the Plan, Do, Check, Act (PDCA) approach
- Enables the auditor to assess a company’s performance, on long-term sustainability and risks, in addition to ensuring they are SLA driven.
WHY CSA STAR Certification builds on ISO27001?

- Help organizations prioritize areas for improvement and lead them towards business excellence.
- ISO 27001 is the international standard for information security
- Considered as Gold Standard for information security
- There are over 20,000 organisations certified globally in over 120 countries.
ISO 27001: Criticisms

- ISO 27001 is updated every 8 years – the controls become obsolete faster than that
- It is a one size fits all standard but there are some industry specific concerns it does not cover, ie it is not Cloud relevant
- Any standard can become a lowest common denominator
- People can certify any scope they like within their organisation to mislead clients
- It doesn't support transparency
When an Organization is audited a Management Capability Score will be assigned to each of the control areas in the CCM.

This will indicate the capability of the management in this area to ensure the control is operating effectively.

The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

<table>
<thead>
<tr>
<th>Score</th>
<th>Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>No Formal Approach</td>
</tr>
<tr>
<td>4-6</td>
<td>Reactive Approach</td>
</tr>
<tr>
<td>7-9</td>
<td>Proactive Approach</td>
</tr>
<tr>
<td>10-12</td>
<td>Improvement Based Approach</td>
</tr>
<tr>
<td>13-15</td>
<td>Optimising Approach</td>
</tr>
</tbody>
</table>
They must demonstrate knowledge of the Cloud Sector

- Either through verifiable industry experience – this can include through assessing organizations
- Or through completing CCSK certification or equivalent

They must be a qualified auditor working a ISO 27006 accredited CB

- Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.

They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification
Accredited certification bodies

bsi.  SGS  BRIGHTLINE

www.tuv.com  TÜV Rheinland  TÜV NORD
Benefits of STAR Certification?

Sales and Marketing Benefits:

- Added to the current management system.
- A ISO 27001 certification plus a STAR certificate as evidence of both compliance and performance to both suppliers, customers and other interested parties.
- The ability to benchmark your organization’s performance and gauge your improvement from year to year.
- An independently validated report from an external Certified Body (CB) body which can be used to demonstrate an organization’s progress & performance levels.
- Exclusive to the STAR Registry.
Benefits of STAR Certification?

Strategic Benefits:

- A 360° enhanced assessment giving senior management full visibility to evaluate the effectiveness of both their management system and the roles and responsibilities of personnel within the organization.

- A flexible assessment that can be tailored through the Statement of Applicability. This guarantees the results and measurements of assessments are both relevant and necessary in helping organizations manage their business.

- A comprehensive business report that goes beyond a usual assessment report and gives a strategic and accurate overview of an organizations performance to enabling senior management to the identify action areas needed.

- A set of improvement targets to encourage an organization to move beyond compliance toward continued improvement.
Benefits of STAR Certification?

Operational Benefits

➤ Scalable to organizations of all sizes. Provides information that allows you to know where they are now and measure any improvements, internally benchmark their sites and potentially externally benchmark their supply chain to stimulate healthy competition.

➤ A visual representation of the status of a business and instantly highlights where the strengths, weaknesses, allowing clients to maximize resources, improve operational efficiencies and reduce costs

➤ Independent reassurance to prove to senior management where the risks, threats, opportunities lie within a business
## Benefits of STAR Certification?

**Guidance**

**Implementing the Cloud Security Principles**

Published 23 April 2014

---

### Table 1: Common approaches to implementing objectives

<table>
<thead>
<tr>
<th>Standard</th>
<th>Guidance on certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001:2005 or ISO/IEC 27001:2013</td>
<td>It is possible to be certified as compliant with ISO/IEC 27001:2005 or ISO/IEC 27001:2013. Since the scope of the certification can be specified by the organisation being certified, when using this mechanism to demonstrate implementation of one of more Cloud Security Principles it is recommended that the scope be verified as covering the right aspects. The individual performing this review should have the qualifications referenced in Table 1. ISO/IEC 27001 certification will not verify that the controls implemented by the service provider are effective. When relying on ISO/IEC 27001 certification, consumers should note that the United Kingdom Accreditation Service (UKAS) is the only national accreditation body recognised by government to assess organisations that provide certification services. ISO/IEC 27001 audits performed by bodies not recognised by UKAS may reduce the confidence that consumers can place in their quality.</td>
</tr>
<tr>
<td>Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0</td>
<td>CSA CCM v3.0 compliance is achieved through CSA’s <a href="#">STAR</a> scheme. Consumers are advised that the first level of STAR is ‘self-assessment’ - service providers referencing STAR at this level should be considered to fall into the ‘Service provider assertion’ category above. The remaining levels of STAR (‘certification’, ‘attestation’ or ‘continuous’) should be considered to fall in the ‘Independent validation of assertions’ category. As with ISO/IEC 27001:2005 or ISO/IEC 27001:2013 it is recommended that a qualified individual verify the scope and implementation of controls to ensure they support implementation of the Cloud Security Principles claimed. The individual performing this review should have the qualifications referenced in Table 1.</td>
</tr>
</tbody>
</table>
Certificate of Registration

CLOUD SECURITY MANAGEMENT SYSTEM - STAR CERTIFICATION 2013

This is to certify that:

Holds Certificate Number: STAR 12345
and operates an Information Security Management System which complies with the requirements of STAR Certification and has achieved Gold Certification for the following scope:

Information Security Management System

Applicability revision

In accordance with the Statement of

For and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally Registered: 13/06/2011  Latest Revision Date: 18/10/2012  Expiry Date: 13/06/2014

Page: 1 of 2

...making excellence a habit...
# STAR Certification: Entry

## STAR Certificate Registry Entry

The information below is provided as a companion to the CSA STAR Certificate.

### Client Name

**HP Enterprise Cloud Services for Government (ECS-G)**

### Client URL


### Client Description (200 words or less)

HP Enterprise Cloud Services for Government (ECS-G) is an ISO27001 certified Virtual Private Cloud (VPC) which is one of the first Cloud Services to gain the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) Certification within the UK. This service provides our Public Sector clients with desktop, infrastructure and networking without the high cost of owning and managing their own equipment or data centres. Designed and built for the enterprise, supporting high-end applications which can be quickly deployed in a secure, multi-tenant cloud environment, accessing the latest IT services without risk of developing such complex systems inhouse. VPC enables self-provisioning to match your business needs as they change and evolve. HP's proven hardware and software, together with its industry-leading services, form one of the best and most secure converged cloud platforms to base your future ICT strategy upon.

### Scope

Information Security Management System for ECS-G Central Operations and Support Services, Security Operations Centre, comprising managed security service, situational awareness, protective monitoring, and security incident management including the protection of customer data and company assets by the application of appropriate security controls.

This is in accordance with version 7.5.6 of the Regional EMEA Statement of Applicability, and version 7.7.6 of the Local Statement of Applicability. In association with ISO 27001 certificate IS 85756

### CCM Version Used

- 1.4
- 3.0

### Certificate Expiry Date

10/24/2016

### Certificate Country

United Kingdom

### Term of Certificate

3 years

### Certification Body

The British Standards Institution (BSI)

### Certificate Number

STAR 600174
STAR Attestation

OPEN CERTIFICATION FRAMEWORK

LEVEL 3
Continuous Monitoring-Based Certification

LEVEL 2
Third-Party Assessment-Based Certification

LEVEL 1
Self-Assessment

ASSURANCE

TRANSPARENCY
Star Attestation (through the type 2 SOC attestation examination) helps companies meet the assessment and reporting needs of the majority of users of cloud services, when the criteria for the engagement are supplemented by the criteria in the CSA Cloud Controls Matrix (CCM). This assessment:

- Is based on a mature attest standard
- Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change
- Does not require the use of any criteria that were not designed for, or readily accepted by cloud providers
- Provides for robust reporting on the service provider’s description of its system, and on the service provider’s controls, including a description of the service auditor’s tests of controls in a format very similar to the now obsolete SAS 70 reporting format, and current SSAE 16 (SOC 1) reporting, thereby facilitating market acceptance
Next steps

- Pilot CloudTrust Protocol (CTP)
- Integrate CTP in the Open Certification Framework (STAR Continuous)
- Integrate Privacy Level Agreement into the Open Certification Framework
- For more info on CSA Privacy Level Agreement results please check: [https://cloudsecurityalliance.org/research/pla/](https://cloudsecurityalliance.org/research/pla/)
In summary

- Transparency, assurance and accountability are the key elements to increase trust in cloud computing

- Security certifications could be good tool to increase trust, ONLY if:
  - Auditors are qualified and properly certified
  - The control framework used as underlying standard is relevant
  - The control framework is publicly available and it’s capability to address requirements can be verified.
  - The scheme support transparency (e.g. via publication of scope and SoA)
  - Different assurance need are supported (e.g. self certification – 3rd party assessment – continuous monitoring).

- Certifications need to be affordable for Small and Medium companies

- CSA Open Certification Framework and STAR Certification provides all the above.
Help Us Secure Cloud Computing

- www.cloudsecurityalliance.org
- dsavanovic@cloudsecurityalliance.org
- LinkedIn: www.linkedin.com/groups?gid=1864210
- STAR: https://cloudsecurityalliance.org/star/
- CloudWATCH: http://www.cloudwatchhub.eu/certification
- ENISA: https://resilience.enisa.europa.eu/cloud-computing-certification
SEE YOU @

CSA CEE SUMMIT 2015
CLOUD SECURITY ALLIANCE
SLOVENIA//LJUBLJANA//11 MAR

FULL DETAILS: www.csa-cee-summit.eu
THANK YOU!