Post Event Report

CSA STAR Certification Summit 2016

5 May 2016 | **Improving Trust in Cloud**

cloud security alliance®

CSA STAR Certification Summit 2016
Improving Trust in Cloud

Event: CSA STAR Certification Summit 2016
Date: 5 May 2016

Attendees

Organisation	Country	Name	Title	
BSI	China	Maxim Wan	China STAR TM	
	Singapore	Amanda Nuar	Singapore Account Development Manager	
CEPREI	China	Liu Xiao Yin	Technology Director	
		Li Yao	Deputy Head, Technology Development	In-person
EGA	Thailand	Kitisak Jirawannakool	Information Security Specialist	
Gartner	Singapore	Sid Deshpande	Principal Research Analyst	
IDA	Singapore	Lee Hing Yan	Director of National Cloud Computing Office	
INS - Information Security	Canada	Gary Perkins	Executive Director/ Chief Information Security Officer	via Video Conference
Japan Information Security Audit Association (JASA)	Japan	Tadashi Nagamiya	Secretary General	
KPMG	Singapore	Daryl Pereira	Partner (SG)	
		Jim Fitzsimmons	Associate Director, Management Consulting, ASEAN	
		Mark Ames	Associate Director, Cybersecurity	
		Rajnish Kapur	Director, Information Protection & Business Resilience	In-person
Ribose	Hong Kong	Ronald Tse	Founder	
SGS	Taiwan	Sidney Ho	Global Cloud Certification Manager	
TUV Rheinland	Singapore	Carol Sim	Head of Systems	
		Heide Mateo	Chief Operating Officer	

Key Discussion Area

Topic (T) / Suggestion/Comment (S)	Raised by	Follow up action
T CSA's proposal to define a global framework for mutual/multiparty recognition of national and sector specific certification schemes.		
S All participants supported the idea and suggested that CSA is in unique position to achieve this goal being an independent global organisation and has also the flexibility that it might lack within the ISO community. The long term ambition of the work though should be the creation of an international standards that leverages the principles and mechanism defined within the CSA's effort.	All	To table in the next OCF meeting
T Feasibility of the proposal to create a repository of controls/requirements and a repository of assessment/audit evidences.		
S The idea of common repository of evidences and common repository of controls/requirements was generally well received and considered as usual way forward.	Ribose KPMG JASA	
While the repository of controls (based on CCM) and requirements doesn't create any potential negative side-effects, the repository of evidences could create problems since it might contain potentially confidentially information that organisations are not willing to publicly share.		To table in the next OCF meeting
S CSA proposal is to have the repository of evidences structured in 2 different areas.	CSA	
PUBLIC AREA: (i.e. the current STAR Registry) where organisation can voluntarily share the information they will comfortable to share with the general public.		
PRIVATE AREA: a repository under the full control of the organisation that own the evidences (i.e. the CSP). The access to the private area will be grated from CSP to the individual with the 'need to know', such auditors, regulators, customers.		
T Definition of the the concept of "acceptable evidence" and re-usability of the evidences collected from 3rd party auditor.		
S The definition and standardisation of the concept of an 'acceptable evidence' under different auditing approaches (e.g. ISO and ISAE 3000) is extremely challenging and not necessarily feasible.	KPMG Ribose BSI	To table in the next OCF meeting
While for the theoretical point of view it might be possible to agree on the specification that will describe an "acceptable evidence", in practice no auditor will be ready to issue a certification or attestation based on 'someone's else' assessment since there are liability implications.		
Even though the evidences collected by 'someone's cannot be fully re-used during an auditing process, certainly that can be taken as input and can be leveraged to substantially reduce the auditing time. From this point of view, the definition and standardisation of the concept of acceptable evidence would help.		

Topic (T) / Suggestion/Comment (S)	Raised by	Follow up action
(T) Currently CCM's structure is "flat". There's no indication of which controls should applied to organisation with different risk profiles. (S) It was proposed to adopt a structure similar to the one currently adopted within the Singapore standards MTCS. For instance, CCM controls could be structured in 3 levels corresponding low-moderate-high risk profile.	Ribose KPMG JASA CEPREI	FYI
(T) The current structure of the OCF framework implies that the 3 approaches offered a LEVEL 2, i.e. STAR Certification, STAR Attestation and C-STAR, have the same value. Based on the experience of Ribose that has undergone to the 3 different assessments, they do not have the same level of depth. For instance, STAR Attestation seems to be much more demanding. The audit time is much more. For instance, in the case of Ribose, on the same scope of assessment, they have 8 man/days of audit in the case of STAR Certification and 55 in the case of STAR Attestation. (S) The differences between STAR Certification - Attestation - C-STAR should be better highlighted in the structure of the OCF so to reflect the differences in terms of: 1) Scope/Coverage of Controls, 2) Maturity/Depth of the difference options offered at Level 2.	Ribose	To table in the next OCF meeting
(T) CCM mappings. (S) The current mappings between CCM and other standards should be supplemented with a reverse mapping in order to better demonstrate how a CCM control satisfy the requirement expressed in other standards. An example of such an approach is the work done by the Singapore Agency IDA that has done a mapping and reverse mapping of MTCS and CCM's controls, highlighting the gaps between the controls in the 2 standards. (S) This issue is known to CSA however the reverse mapping entails an amount of resource that is unavailable to CSA currently. Based on the input and support from the community, members and Government, CSA will prioritise a list of standards for which the reverse mapping will be executed.	Ribose CSA	To table in the next OCF meeting
(T) Driving assurance through CSP certification may not be sufficient to protect the end users. (S) In addition to CSP certification/audit, there is a need for CSPs to raise awareness on the customer-facing security issues as security incidents often occur due to the way customers use the vendor resources. It was proposed for this issue to be highlighted.	Gartner	FYI

Topic (T) / Suggestion/Comment (S)	Raised by	Follow up action
(T) Within the Chinese market there's confusion on the differences between STAR Certification and C-STAR. (S) CEPREI suggested to: 1) Put in place awareness comparing to better explain the differences between the STAR Certification and C-STAR, 2) STAR Entry certificate to reflect all the standards that are underlying C-STAR and not only making reference to the version of CCM.	CEPREI	To further discuss with CEPREI and the OCF WG
(T) CSA STAR Auditor Training. (S) To address the concern on consistency for the auditor training courses, there should be high level guidance for the exam question in place.	ALL, particularly KPMG	FYI – materials are vetted by DC now
(T) STARWatch. (S) The STARWatch is very much welcomed by the community since it facilitates the adoption of the CCM and CAIQ and it make them 'actionable'. Proposed changes for STARWatch: 1) Include supporting evidence on the website, 2) Include quantifiable data on the shared registry, 3) Explore including comparison between the suppliers on the registry.	ALL, particularly KPMG	To table in the next OCF meeting
(T) CSA STAR Website – to simplify for community to understand CSA STAR better. (S) Proposed potential model if CSA intends to revamp website, 2 different web experience: 1) CSP perspective, 2) End user perspective.	ALL, particularly KPMG	To table in the next OCF meeting

Conclusion

The next CSA STAR Certification Summit will be hosted in the EMEA Congress 2016 to be held in Madrid, Spain.
For further information about the event, please contact us at: csa-cb-summit@cloudsecurityalliance.org