eForensics Magazine

DATABASE

VOL.3NO.04

ISG

Strategies and tactics for Information Security Governance

HOW DID WE GET INTO THIS MESS? IT HISTORY AND ARCHITECURE

COMMUNICATING RISK TO EXECUTIVE LEADERSHIP

HOW AND WHY INCLUDE DBAS IN INFORMATION SECURITY GOVERNANCE?

INFORMATION SECURITY GOVERNANCE AND WHY IT FAILS TO STOP APTS

PLUS

INTERVIEWS FOR THE SPECIAL QUESTIONS' COLUMN!

Issue 04/2014 (30) February ISSN 2300-6986

CLOUD SECURITY ALLIANCE AND GOVERNMENT CLOUD

by Mark Dunne

How to use the Cloud Security Alliance – Security, Trust & Assurance Registry (STAR) to your benefit while operating in the rapidly growing Government Cloud sector.

What you will learn:

- What the Cloud Security Alliance (STAR) is
- How to optimise Cloud Assurance with G-Cloud and (STAR)
- Some changes coming to G-Cloud
- The future of Cloud Assurance in the public sector

What you should know:

- Some basic principles of information security
- What an information security standard is
- The basic principles of cloud technology
- Security concerns related to cloud technology

In order to reduce cost, Governments globally are adapting cloud technology at a very fast pace. Like everything else in the IT industry, rapid take up of any technology brings with it concerns related to security. All organisations must protect their *crown jewels* in order to stay ahead of competition and maintain Confidentiality, Integrity, and Availability (CIA). In Government it's more than just that. Government departments must keep data safe, sometimes life depends on it. So can you imagine being in the shoes of a Government official when it comes to making a decision on the adoption of cloud technology. It must be like staring into the abyss!

Luckily there is industry help at hand with the use of standards such as FedRAMP (US Federal Government), G-Cloud Accreditation (UK). The US and UK are front runners when it comes to cloud adoption for public sector. What should you do however if you plan to sell your cloud solution into the public sector and you want to provide transparency and a certification scheme does not exist. The answer is to at least adopt the Cloud Security Alliance, Security, Trust & Assurance Registry (STAR). Let's find out why.

SO, WHO IS THE CLOUD SECURITY ALLIANCE?

The concept of the Cloud Security Alliance (CSA) was formalized in December 2008. It is a not-for-profit organization dedicated to provide education and promote best practices for providing security assurance within cloud computing. You can become a member of the CSA as an individual, as an affiliate (if not-for-profit), as a corporate or SMB. The CSA also partake in research in multiple disciplines related to cloud security worldwide. They also provide an Open Certification Framework (OCF), and as part of that framework is what they refer to as the Security, Trust & Assurance Registry (STAR).

MORE ON STAR

Launched at the end of 2011, what (STAR) essentially does is help end users make a decision on Cloud, and it achieves this with a publicly accessible registry that documents the security controls in the various cloud computing offerings.

Filling a gap in the market place for a system to help improve transparency and hence determine a level of trust in a particular cloud service. The 3 layers to (STAR) are self-assessment, 3rd party-based certification, and continuous monitoring based certification. It contains the results of assessments (based on CSA best practice) that organizations want to voluntarily publish in what's known as the CSA-STAR portal. The first organisations to gain Certification in (STAR) came in late 2013.

WHY THE CSA (STAR)

Well, earlier on I made the claim that the answer to provide transparency in public sector cloud Certification when none exists is the CSA (STAR). This is down to the fact that Certification schemes will follow this logic globally in the future and in fact some already do. It is best to put your right foot forward with an industry accepted open framework rather than do nothing at all. Particularly in the EU market place, where the EU Commission have established the European Cloud Computing strategy and part of that strategy is to produce a Cloud Standardisation Roadmap. While this is being developed, what are people currently doing to get by? Let us take a look at the UK market for example, and see how the (STAR) framework will and should play an important role in cloud public sector procurement.

UK G-CLOUD

As it stands, the UK public sector procurement for cloud is based around a system called G-Cloud. G-Cloud has been very successful in allowing UK public sector gain access to cloud services in a less cumbersome way that is friendlier to SMB's. The G-Cloud has a current accreditation scheme which focuses on the sensitivity of the information that is stored within the cloud solution and couples that with certain controls, actions and evidence that the cloud provider must provide in order to prove that the information is kept safe.

HOW TO MAXIMISE ON CLOUD ASSURANCE FOR THE PUBLIC SECTOR

Using the principles of the G-Cloud accreditation plus the Cloud Security Alliance (STAR) Certification can provide a very high level of assurance. The following section will demonstrate how both G-Cloud and (STAR) can be used together for an incredible level of assurance:

Table 1. *How G-Cloud and CSA can be used together*

G-Cloud Accreditation	CSA (STAR)
Risk Assessment, RMADS, Residual Risk Statement, Risk Register	Cloud Controls Matrix (CCM)

As part of the G-Cloud accreditation, the Pan Government Accreditor (PGA) must review and approve the Risk Management and Accreditation Documentation Set. This is referred to as (RMADS) in the market place. Part of this process is to conduct a risk assessment that is based on the HMG IS1 risk assessment standard. A good approach to take when working with cloud technology is to ensure that the controls in the Cloud Controls Matrix are considered for risk treatment in relation the cloud technology assets.

The idea behind the Cloud Controls Matrix (CCM) is to provide fundamental principles to guide cloud vendors and to help customers of those vendors in assessing the security risk related to using the cloud service. The idea is to provide internal control direction, structure and clarity related to information security in the cloud sector. In practice it works well alongside another document from the CSA GRC stack called the Consensus Assessments Initiative Questionnaire (CAIQ). The (CCM) also maps very well to other industry standards including ISO 27001. So in summary, while conducting the risk assessment and completing RMADS, it would be very beneficial to also use the (CAIQ) and also the (CCM) to build an overall more robust view of risk in relation to the cloud technology. In terms of certification, customers have a choice going forward from March 2014 on what version of the (CCM) to use. I recommend using version 3 or transition to this version as soon as possible, as the version 1.4 is only valid for 12 months.

Table 2. *How G-Cloud and CSA can be used together*

G-Cloud Accreditation	CSA (STAR)
Risk Assessment, RMADs, Residual Risk Statement, Risk Register	Cloud Controls Matrix (CCM)
ISO 27001 Certificate	ISO 27001 Certificate

One commonality between the G-Cloud accreditation process for (Business Impact Levels) IL1/2 and above is that ISO 27001 certification is central to the process. Not only is certification necessary on both parts, but the certification must also be conducted by a government recognised certification body, in the UK this is referred to as a UKAS accredited certification body and in the US ANAB is the accreditation body. For more detail on this I recommend that you visit the SaaSAssurance blog page, where we have a post called 'The importance of UKAS accreditation'. During the audit process, do not hesitate asking the certification body to provide an auditor with a background and understanding of cloud technology as this will enhance the quality of the audit experience.

Table 3. *How G-Cloud and CSA can be used together*

G-Cloud Accreditation	CSA (STAR)
Risk Assessment, RMADs, Residual Risk Statement, Risk Register	Cloud Controls Matrix (CCM)
ISO 27001 Certificate	ISO 27001 Certificate
ISO 27001 Certificate (suitably scoped)	ISO 27001 Certificate (fit for purpose)

Staying with the topic of ISO 27001. G-Cloud accreditation IL1/2 (Business Impact Level profiles 11x/22x) relies on what is referred to as a *suitably scoped* ISO/IEC 27001 certificate. What this ensures is that no shortcuts are taken and the assets being protected in the Information Security Management System (ISMS) include all applicable assets related to the cloud service for instance.

The Certification assessment for (STAR), use a similar method and refer to this as having an ISMS with scope, processes and objectives that are "*Fit for Purpose*". This is a very common sense approach to ensuring a high quality (ISMS). For more information on ISO/IEC 27001 scope and risk assessment, visit the SaaSAssurance YouTube channel where we provide basic digital media.

Table 4. *How G-Cloud and CSA can be used together*

G-Cloud Accreditation	CSA (STAR)
Risk Assessment, RMADs, Residual Risk Statement, Risk Register	Cloud Controls Matrix (CCM)
ISO 27001 Certificate	ISO 27001 Certificate
ISO 27001 Certificate (suitably scoped)	ISO 27001 Certificate (fit for purpose)
Information Assurance (IA) compliance	Management Capability Score

As part of the G-Cloud accreditation process there are some Information Assurance (IA) activities to be performed and it considers evidence relating to the Data Protection Act, Location of assets, management of personal information, dealing with subcontractors and also details on the technical solution itself. As technical solutions relating to cloud technology vary considerably, there is no real way to predict exactly how the technical solution is assessed, and yet again the Cloud Controls Matrix (CCM) is the perfect resource to assist with this as it defines what controls fall under SaaS, PaaS, IaaS service models. I recommend visiting the NIST 'definition of cloud computing' if you require more information on the cloud service models. Similarly, to really bolster the quality of the certification, the Cloud Security Alliance as part of their certification measures the (CCM) domains and will then provide a 'Management Capability' score. Each domain will be scored on five management principles. These levels will then designated as either 'No', 'Bronze', 'Silver' or 'Gold', where I can assure you that the Gold level is a true level of excellence. Some months back HP have achieved the Silver award and were one of the first cloud service providers to do so.

SOME CHANGES ON THE WAY

It's safe to say that combining the current requirements of the G-Cloud accreditation with the CSA (STAR) certification provides an outstanding level of assurance in the UK market place. However as 'the cloud' matures and continues to gain industry acceptance where the pros and cons are fully understood, changes to Government accreditation systems are sure to evolve. In 2014, a new classification system called the Government Security Classification Policy replaces the Government Protective Marking Scheme, which has an effect on places in the document where I refer to business impact level 2 (IL2). Although this is not as a result of cloud technology, it is sure to have ramifications to the cloud technology sector while this new policy is gradually introduced. A good time to be an information security consultant in the UK, as this will keep the industry somewhat busy. Other encouraging changes come from the current UK CTO, Liam Maxwell. Strong on backing innovation and change and driving this change through the UK GDS, Mr Maxwell has recently spoke out on a blog post that it is not the remit of Government to create cloud standards…

"Given our commitment to making Government business more accessible to SMEs, now would be the wrong time for a government body to develop new standards and certification schemes specifically for cloud services for government. We expect standards to emerge as markets mature – led by the industry, not by government. Governments should be cautious about intervening in the development of standards unless there is clear evidence that markets are not meeting user need. "

This is encouraging news for the industry as a whole and in the EU Commission, where the European Telecommunications Standards Institute (ETSI) is tasked with developing certification schemes. So if you are waiting for your Government to provide guidance on Cloud Technology assurance, adopting the CSA (STAR) as a first step will undoubtedly stand you in good stead for when the industry has caught up. In the meantime it will help provide a differentiator to your cloud services.

Some would then argue that the next logical step is to place the accreditation process itself to an independent assessor and for Governments to come together to help work out what is contained in that assessment. This has the benefit of standardization throughout the market place, and it can take the burden of certification itself away from Government agencies, where given the growth of the sector they are sure to be overrun with work. In the US federal government they have done this successfully with the FedRAMP standard, where the accreditation is done by 3rd party assessors. I spoke some months back in Berlin at a European Cloud Event 'Cloud4Europe' where I made reference to several accreditation initiatives worldwide including FedRAMP and encouraged the EU commission to make an effort to adopt the best of what is out there. I also encouraged the take-up of ISO/IEC 27001 and CSA (STAR) in the meantime as a 'safe bet', as the Government sector can't afford to sit back and do nothing. On top of my practical advice on providing assurance, I would also encourage you to visit the 'Good practice guide for securely deploying governmental clouds' from ENISA. All links to resources referenced are below.

LINKS TO RESOURCES USED IN THIS ARTICLE

- CSA, Cloud Controls Matrix version 3 (CCM): *https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx*
- CSA, Consensus Assessments Initiative Questionnaire (CAIQ): *https://downloads.cloudsecurityalliance.org/initiatives/cai/CSA-CAI-Question-Set-v1-1.xlsx*
- SaaSAssurance blog with reference to ISO 27001 Certification: *http://www.saasassurance.com/blog.html*
- NIST, definition of cloud computing: *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*
- ENISA, good practice guide for securely deploying governmental clouds: *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/at_download/fullReport*

ABOUT THE AUTHOR

Mark Dunne is CEO of SaaSAssurance. SaaSAssurance provide digital and easy to use solutions for implementing an Information Security Management System (ISMS) compliant with the international standard ISO/IEC 27001. Mark has a background in cloud architecture and specialises in applying information security frameworks to complex cloud environments. Mark acts as Program Manager for SaaSAssurance collaborating with informations security consultancy firms worldwide providing them with a scalable business model where they can transition to annual re-occurring revenue, hence build a consultancy business that is efficient with less travel requirements based around a digital solution. To get in touch: Email: Mark.Dunne@SaaSAssurance.com | Twitter: @2SaaS