Path to Maintaining Cloud Data, Security, & Privacy Compliance is outdated, already.

By Sunny Kalsi

March 16th 2017
Version 1.0.2

Washington, DC 20003

skalsi@alumni.harvard.edu : *email*
skalsi.com : *personal*
linkedin.com/in/skalsi : *professional*

(202) 90-KALSI : *tel*

** The opinions expressed here do not necessarily represent or reflect upon any organization the author currently works, or has worked, for.*

PREFACE:

Going to the Cloud is the by-product of the US Federal Government mandate going back to December 2010 when the White House directed all Federal Agencies to reduce their data center footprint[1] and go "Cloud First" (Kundra, 2010). It was egregiously expensive to maintain data centers for all US Departments. There was a data center sprawl that typically grew every year at escalating Capital Expenditure (CapEx). One reason is that the government wanted to reduce their CapEx and float their Operating Expenses (OpEx) strategically into the latest cloud based services & technology – e.g. Software-as-a-Service (SaaS). So, the Federal CIO, Vivek Kundra, sent the interagency memo[2] directing all CIO's to reduce their data center footprint and refocus.

This was around the time the Cloud was gaining steam worldwide but wasn't quite making it to the Federal Government due to security concerns. Cloud or Cloud based services for government usage was insecure and viewed with strong skepticism. Cloud in general wasn't in the natural lexicon for most IT Security professionals. Kundra's directive forced the government to understand the cloud security issues and build a path towards government adoption.

THE COMPLIANCE CHALLENGE:

Almost all Government Data, Security, and Privacy (DS&P) professionals had simple questions that weren't easy to answer then such as "How can we Certify and Authorize the Cloud in general?", "How can custom apps built in the Cloud get authorized?", and "Where are all the security minefields in this new direction?" There was uncertainty that needed attention.

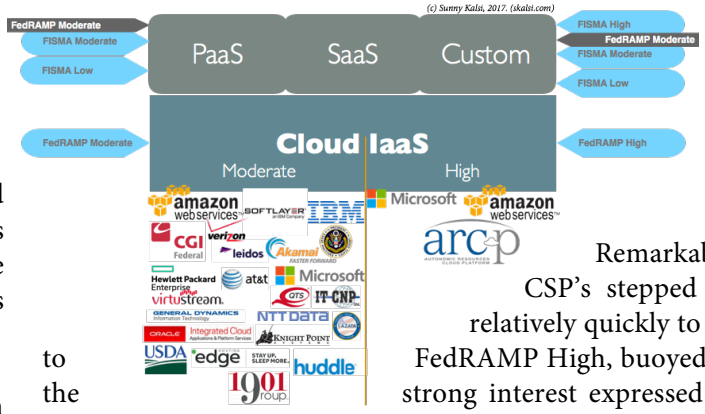
The government changed the compliance process from Certification & Authorization (C&A) to Accreditation & Authorization (A&A); a modernized process with focused attention on todays' security compliance needs that also fixed known gaps in the C&A process.

So, a strategy to Authorize the Cloud Service Providers (CSP), such as Amazon AWS, IBM SoftLayer, and Microsoft Azure, became necessary. Eventually a standard to certify the Cloud – aka Infrastructure-as-a-Service (IaaS) - was developed, called FedRAMP[3]. This initially granted an Authorization To Operate (ATO) to approved Cloud environments at the Moderate baseline; equivalent of a FISMA[4] Moderate Baseline Security level as defined by NIST[5]. FedRAMP and FISMA both use the NIST SP 800-53 security controls[6]. The Defense department (DoD) needed a Baseline appropriate for them, therefore they leveraged the FedRAMP Joint Authorization Board (JAB) and the ATO packages and created processes for each of their Security Impact Levels. Some Agencies needed a higher security baseline. But getting a CSP to FedRAMP High was going to be an arduous task with many "known unknowns" and "unknown unknowns"[7].

EFFECTS OF THE COMPLIANCE CHALLENGE:

Eventually several CSP's started getting their Cloud's authorized - Amazon's AWS, IBM's SoftLayer Federal Cloud, Microsoft Azure, and others. Cloud based applications, SaaS, & Platform-as-a-Service (PaaS), were also getting FedRAMP'd - such as Acquia Cloud and Salesforce GovCloud.

Figure 1: FedRAMP & FISMA (Moderate & High)



Remarkably, CSP's stepped up relatively quickly to get to FedRAMP High, buoyed by the strong interest expressed by certain Agencies. Of course, billion dollar financial prospects make this an easier corporate decision and only those with deep pockets can compete. To date, only Amazon, Microsoft, and Arc-P's IaaS have received the FedRAMP High baseline authorization, just in the past six months. This is an enormous competitive advantage and sets the companies apart to monopolize contracts with the

[1] Data Center Consolidation: https://cio.gov/drivingvalue/data-center-consolidation/
[2] Kundra, Vivek: *25 Point Implementation Plan to Reform Federal Information Technology Management.* Whitehouse, https://obamawhitehouse.archives.gov/blog/2010/12/10/saving-money-government-it. Dec 9, 2010. Memo.
[3] Federal Risk and Authorization Management Program. http://fedramp.gov.
[4] Federal Information Security Management Act. http://csrc.nist.gov/groups/SMA/fisma/index.html.
[5] National Institute of Standards and Technology. https://nist.gov.
[6] NIST SP 800-53 publication. http://csrc.nist.gov/publications/PubsSPs.html.
[7] Rumsfeld, Donald. Known Knowns, Known Unknowns and Unknown Unknowns: A Retrospective. http://www.cbsnews.com/news/known-knowns-known-unknowns-and-unknown-unknowns-a-retrospective/. November 2006.

highly security conscious customers. However, FedRAMP High environments are far more expensive than Moderate ones. Therefore, any upcoming RFP's, or IDIQ's, for FedRAMP High CSP's will most likely include the requirement for Moderate ones. Balancing an IT System Portfolio between these environments in a Pay for Use setup is what was envisioned many years ago. Kundra's vision is slowly panning out.

THE COMPLIANCE COST:

All the FedRAMP applicants undergo a rigorous and expensive process to get authorized. The cost, after factoring in most variables, is borne by the FedRAMP applicant and can be up to $500,000 for a PaaS or SaaS in a FedRAMP'd IaaS and significantly more for IaaS. According to Matt Goodrich from FedRAMP, the median costs for a mid-range CSP obtaining FedRAMP Moderate authorization is $2.25M[8]. However, the costs between four sampled CSP's ranged between $0.5M to $4M. Add another $1M per year in Continuous Monitoring costs to maintain compliance. It's a major commitment but CSP's know the market opportunities are significant.

One of the key requirements of maintaining FedRAMP authorization is that all applicants need to demonstrate that their XaaS is logging all relevant data points for analysis and compliance. Examples include Cloud access logs, VSI security scans (e.g. Tenable NESSUS), System Logs, Security Violations & Incident Reports, Incident Responses, Monthly/Quarterly/Yearly audit reports, Roles and Responsibility matrices, Continuity of Operations (COOP) plans and tests, among many other NIST mandated controls. This will vary slightly by each Agency Information System Security Officer's (ISSO) office requirements.

THE PROBLEM:

Government ISSO's expect all CSP's to provide them with a Web based Dashboard to have visibility into the status of the Cloud environment. The dashboard is expected to show uptime, downtime, security events, mean time to recovery, statistics that shows whether any Service Level Agreements (SLA) have been breached, and more depending on the contract needs. Cloud IaaS providers will guarantee a certain SLA – say 99.9% uptime. Custom cloud applications that require their own FISMA authorization may be required to show 99.99% or higher uptime. However, these customer and/or delivery team dashboards can be weak or non-existent. Sophisticated software is typically used behind the scenes to monitor all activity, but it's not possible to monitor everything automatically for some CSP's. Monitoring servers is one thing, monitoring individual services, such as web services, Docker containers, and firewalls, for customer and internal view, requires more work.

Companies will show a manually generated scheduled report with all the relevant data to the government. Sometimes, a basic dashboard will be available in addition to the manual report, but there is much to be desired. Companies like IBM, Amazon, and Microsoft do have sophisticated tools available to perform the monitoring and advise the government as needed in emergencies, but not everyone is doing this well.

A ISSO's reliance on complete accuracy in the CSP's reporting becomes paramount. There is no simple way to review reports, logs, incident reports, without the possibility that a security event has been missed. Given the seriousness of foreign agent pilfering of government data, the ISSO's office is stuck between a rock and a hard place: Work with what you've got and do the best that can be done. They depend entirely on the CSP and/or the cloud application operations team to notify them of any serious incidents of any kinds. Not only is this far from ideal, ISSO offices must strategically plan to improve this to increase their security profile and make their lives easier.

REPORTING:

During audits or security reviews, the security specialists from the Government get together to analyze the report submitted by the CSP, or cloud application team. Questions are asked by the Government and answered by the system or cloud owners and any risks and issues are dealt with. But when there are a large number of devices to audit in the entire Cloud, e.g. Network nodes, Firewall, Load Balancers, Backup servers, along with Server scans, Application scans, validation of dual-site redundancies or an Active-Active or Active-Passive system setup, it is difficult for reporting to be completely accurate. If a specific service is not being monitored explicitly, a security event may never be noticed. The government, cloud or cloud application team may not necessarily realize that the environment was hacked.

[8] Goodrich, Matt: *How much does it cost to go through FedRAMP?* https://www.fedramp.gov/how-much-does-it-cost-to-go-through-fedramp/. September 8, 2016.

Challenge is that you have the Cloud IaaS customer portal, virtual or bare metal servers, firewalls, network setups, several data centers, down to individual applications and services on each device to monitor.

It is possible that one bad actor, internal or external, could inflict, or infect, damage. Not knowing about 1% of the systems' activity footprint could be just where the hack occurred. The lengths these organizations go through to get FedRAMP Authorized means they're extremely careful and always report incidents when it's known. At the FISMA level, where Systems are being certified in the cloud not the cloud itself, there is an additional risk due to application complexity and the system hardening level, e.g. DISA STIG[9] or CIS Benchmarks[10].

Over the past two years alone the number of FedRAMP applications for Cloud based systems has skyrocketed. Additionally, FISMA A&A for Cloud based systems has increased.

With so many Cloud I/P/SaaS systems coming into play, the Government will discover that what they are doing is in fact documenting more and validating less rigorously. Any budget cuts could mean less Security personnel to perform audits not to mention that there aren't that many Security professionals to go around. The gap widens as more systems come on board. Security professionals can't catch up. Keep in mind, many of the Security professionals aren't hackers, network admins, or coders in their former lives. They are professionals who are experts in maintaining DS&P compliance and generally understand Systems, some far more than others. Sometimes Agencies engage independent White hat security professionals to probe for weaknesses and document security non-compliance without any advance warning to the Cloud provider or Cloud system owner.

Even if the risk raised above is ruled minimal, the government does need to ask itself what its target cloud security compliance architecture should be. What is the ideal setup for the Compliance process as well as maintaining compliance that is standardized across the Fed or by Agency? The answer, as you will see soon, is complicated.

SOLUTION A: *CLOUD COMPLIANCE API (ccAPI)*

ccAPI: Similar to the Data Center consolidation initiative ordered by the White House back in 2010, a mandate requiring all Cloud IaaS providers and Cloud based S/P/XaaS systems to tie all their systems into a Government contracted compliance system, e.g. ccAPI, would be the first start. ccAPI would essentially be an API that would be the means by which all Cloud XaaS environments could stream, or schedule upload, the data required to maintain FedRAMP or FISMA compliance on a periodic basis based on the requirements of that Agency.

Let's examine two scenarios - one a CSP and the other a Cloud based application where this would be useful.

Use Case one: The Agency is on the hook to make sure the CSP is FedRAMP compliant. This can overwhelm ISSO offices because the amount of work involved is significant. Then why do some Agencies authorize a FedRAMP to a CSP instead of waiting for the FedRAMP JAB to do it?

Here is an example why: CSP provider "C" has entered the Federal Government space and their Cloud IaaS has received an ATO from the FedRAMP JAB. At pre-approved intervals throughout the year the government receives comprehensive reports from "C" to show compliance across all appropriate security controls. At this point any Agency can use "C" without having to go through an ATO process of their own. Sometimes Cloud contracts are awarded to CSP's who aren't authorized yet but have submitted their application to the FedRAMP JAB. In this case, Agencies may opt to issue their own ATO after an expensive and lengthy assessment. When "C" receives an ATO from an Agency instead, i.e. an Agency FedRAMP ATO, then any other government entity that wants to leverage that ATO would have to review and in some cases, add new conditions and requirements the CSP has to conform to, prior to granting one of their own ATO's unless the FedRAMP JAB declares "C" to be FedRAMP Authorized.

Use Case two: Similar to example one, except instead of a CSP being evaluated, the individual application in the cloud is assumed to have already received an ATO and needs to maintain their FedRAMP or FISMA ATO status. This means different data points are kept for compliance purposes depending on the type of application environment

[9] DISA STIG: *Security Technical Implementation Guide*. http://iase.disa.mil/stigs/Pages/index.aspx. Defense Information Systems Agency.

[10] CIS Benchmarks: https://benchmarks.cisecurity.org. Center for Internet Security.

it is; i.e. what the OS type is, what the container type is (e.g. Docker, Linux containers), what network devices are being utilized (firewall, load balancers, server type, configuration {active-active vs active-passive}), backup type & frequency, application server type, application transaction logs, application security logs, etc.

Solution: The government should issue an Indefinite Delivery Indefinite Quantity (IDIQ) for the ccAPI. All new cloud based systems, and perhaps even non-cloud, should tie their systems into the API for data collection and reporting. All relevant cloud, server, network, firewall, system, application, and other logs must be exported to the ccAPI in an asynchronous or synchronous way. Even network packet data shouldn't be off limits for consideration. The ccAPI will need to be powerful enough to crunch the eventual daily barrage of data, running predictive analytics, and business rules against them, as part of the security analysis and overall Security Health Check Dashboard.

Each agency should have their own dashboard, that would feed into the overall Federal CIO's, so that at any point the US Department's ISSO can report on the security posture of their new cloud and new cloud based applications. The intent of the analytics is to assess security risk but to also predict whether any sophisticated security attack is occurring over a period of time across various cloud applications. At the Federal CIO level, it would be observing the security posture at the highest level across all Agencies.

Thus, Predictive Analytics must be an essential tool and shield to protect and improve the Federal Civilian security posture. Homeland Security, Defense, and Intelligence groups would probably not want to be a part of that IDIQ – but they should do something similar for their own institutions.

The benefit of having the ccAPI would become apparent not long after implementation. The ability to see whether the systems are actual doing what their FISMA or FedRAMP documentation says will become clearer. All procedural security controls, i.e. those related to COOP tests, security training requirements, and others items that require a human to do something manual would continue to get reported the usual way.

Initially, it may be easier to focus on FISMA authorized cloud systems through the ccAPI. Over time, all the various Cloud IaaS environments should tap into the ccAPI to make compliance audit's easier for all ISSO offices. Putting a CSP's hat on, asking Cloud environments to report all their transactional data via ccAPI may be impossible due to the cost prohibitive implication to the CSP's; but it shouldn't be ignored.

There is another option, but it will be a First-of-a-Kind (FOAK) project that should be built as a prototype. It may fail several times before finally succeeding. It is based on the Blockchain[11].

SOLUTION B: *BLOCKCHAIN CLOUD COMPLIANCE SYSTEM (BCCS)*

Blockchain[12] is the technology that drives Bitcoin[13]. It has the attention of the leading technology firms and government agencies. Hundreds of millions of dollars is being invested to pursue blockchain and its uses in industry. Use cases include financial, health records[14], regulatory compliance, and several other areas.

A synopsis of blockchain: it is an open source and decentralized system of validating any transaction, a hash of the actual data, through the use of several trusted independent and autonomous server nodes, called "miners". A transaction could be a payment, a new asset, or a new health record. The options are endless. When the digital transaction occurs, all the miners are notified and they are tasked to solve a cryptographic puzzle the hashed-up transaction presents itself as. Through a mathematical process, each miners' conclusion is analyzed; the transaction is either verified or it's not. If it's verified, the transaction is inserted to the blockchain ledger as another block in the chain of blocks and collectively becomes the distributed blockchain database. This is then replicated across all the blockchain nodes for every instance of the blockchain that is being utilized. Data is immutable and is never lost. This decentralized system of trust is critical to the effectiveness of a blockchain system. Should any bad actor falsify an entry,

[11] Blockchain@MIT: http://blockchain.mit.edu.
[12] Gupta, Vinay: *A brief history of blockchain*. https://hbr.org/2017/02/a-brief-history-of-blockchain. February 28, 2017. Harvard Business Review.
[13] Forde, Brian: What is bitcoin and the blockchain? https://medium.com/mit-media-lab-digital-currency-initiative/what-is-bitcoin-and-the-blockchain-2a61b1bd6427#.kjr10ybpm. June 30, 2016. Massachusetts Institute of Technology.
[14] Halamka, J.D.; Lippman, Andrew; Ekblaw, Ariel: *The potential for blockchain to transform Electronic Health Records*. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records. March 3, 2017. Harvard Business Review.

the other independent miners would not accept the adjusted transaction and thus not allow that change to be entered into the blockchain ledger. This is a mathematical process that no person is involved in.

The bitcoin implementation is public but for enterprises, the blockchain technology must be repurposed. Miners are essentially computational resources. The more powerful, the quicker it can process the millions of transactions. Using the Department of the Interior (DOI, doi.gov) as an example, there could be a miner within every one of the nine Bureaus. In the proposed BCCS, a Cloud Security Compliance blockchain could encompass the entire FISMA or FedRAMP compliance workflow. Rules and logic can be built to execute against every transaction. Access Controls by user or role can enable visibility into any given transaction type. Overall, the blockchain's transactional visibility is up to the discretion of the Agency. The NIST's Cybersecurity functional areas can all be represented in a blockchain, i.e. Identify, Protect, Detect, Respond, and Recover. The data is almost impossible to hack[15] and alter due to the decentralized approach. Even if a miner is hacked and is forced to falsify a transaction, the other miners would crypto-deduce it as an invalid transaction.

Analytics and custom COTS, as mentioned for ccAPI, can be executing in parallel for further insight into the compliance data. ISSO offices would be ecstatic if they had the ability to see the status of any given system from a compliance perspective. They know that what they see is also what the vendor sees. The data is exactly the same. This could revolutionize how they do business and reduce the security risk of all the systems under their purview.

To give a simple example, one challenge that all Security Compliance professionals can attest to is when they're working on a FISMA package, for example, the interaction between the Government and the Cloud application compliance team can get confusing. Copies of working artifacts go back and forth via email, Box, Google Drive, SmartCloud, SharePoint, and so on. The versions get routinely out of sync and by the time the government has reviewed an artifact, they may realize they're already several versions behind. This causes angst and delays occur. It shouldn't be so difficult nowadays but it still happens.

CONCLUSION:

If the White House Federal CIO initiates this transformation, or if a heavy hitting Department takes the initiative, a target compliance cloud architecture and process is achievable. The General Services Administration (GSA) may be an interesting option, perhaps via their 18F[16] outfit that built and manages cloud.gov on Amazon AWS. This could also be initiated by the Department of Defense (DoD) or quite possibly by little-known players in innovation, for example the Consumer Finance Protection Bureau (CFPB, cfpb.gov), assuming the current administration doesn't scrap it. DOI is another possibility – they're big on open source technology and are open to Cloud based innovation. In fact, it was DOI that pioneered the push to a Cloud based Web Content Management System (CMS) Platform-as-a-Service (PaaS) to serve the entire Agency & Bureaus that IBM (ibm.com) built and still runs for them[17]. It was so contractually innovative that other Agencies have been greatly intrigued and may follow suit.

Cloud security compliance is difficult to achieve and tedious to maintain. Some Federal Agencies that have embraced Cloud have discovered that the learning curve is steep. Compliance hasn't change tremendously but the complexity in the security risk determination has definitely gotten harder. The challenge is that as depicted in Figure 1: FedRAMP & FISMA (Moderate & High), FISMA authorization is dependent on a Cloud environment that is FedRAMP'd. A FISMA Security Plan (SP) is dependent on some details only present in the FedRAMP SP. However, the FedRAMP SP is a highly sensitive and secure artifact and CSP's guard it zealously, giving permission to review only in certain circumstances. The CSP will never give access to the SP to any outsider. Only the CSP and the Government has a copy. That means that the Cloud FISMA SP will inherit controls from the FedRAMP by proxy. ISSO offices' not familiar with this practice will find that their work will double and the authorization process will become challenging.

ccAPI may alleviate this, but BCCS may be the paradigm shift that Compliance management needs. Incorporating both FedRAMP & FISMA into the blockchain will change everything.

[15] Berke, Allison: *How safe are blockchains? It depends.* https://hbr.org/2017/03/how-safe-are-blockchains-it-depends. March 7, 2017. Harvard Business Review.
[16] GSA 18F: Government digital services group. https://18f.gsa.gov.
[17] Fullerton, Tim; Gillick, Larry; Kalsi, Sunny: *Interior's new Web platform.* U.S. Department of the Interior. https://livestream.com/usinterior/events/3647477. December 16, 2014.