A new way to streamline and simplify cloud security compliance with STARWatch

Introduction

IT modernization has spawned growth in public cloud adoption by both small companies and large enterprises across the globe. Organizations of every type are reaping the benefits, as they shift infrastructure, applications and business services from the datacenter to the cloud. The greatest benefits anticipated by those who have embraced the cloud include huge cost saving in paying for only what you need, efficiencies in configuration management and greater agility in turning out innovative digitized services that drives business forward to experience substantial growth. Gartner sees cloud as a “dominate force of change [with] its impact felt in every major IT market”[1]. Moving to the cloud, however, is no easy feat for any company, especially those highly concerned with security of high-valued information and ensuring compliance to an ever-increasing number of regulatory and industry standards. Selecting the right cloud services can become an elaborate and sometimes complex series of business and technology decisions; with the potential security, legal, financial, and compliance impacts not necessarily clear to the cloud user.

Selecting a **Cloud Service Provider (CSP)** is not for the faint at heart. Once you have decided to migrate to cloud services, the process of evaluating a CSP is one of determining their trustworthiness and ability to provide capabilities needed; a process that can be quite daunting and very resource intensive. Being efficient in conducting an assessment against specific business objectives and compliance requirements across the variety solution providers is essential to ensuring the success of the project and greatest return on investment. Experts advise organizations to define their needs and conduct a thorough analysis of CSPs concerning those needs and factors before migrating to the cloud. In short, don’t contract a service until you have looked closely at what they can provide. Assessments call for a detailed, but non-prescriptive understanding of a CSPs ability to deliver in areas of reliability and capability, business health and process, administrative support, technical capabilities, security practices, compliance and more.

[1] Forecast Analysis: Public Cloud Services, Worldwide, 2Q16 Update, Gartner Analyst(s): Sid Nag | Fred Ng | David Edward Ackerman

Compliance is a Top Concern When Moving to the Cloud

Organizations face an ever increasing and changing list of statutory, regulatory, contractual and legal compliance obligations. This includes regulatory guidelines, rules and industry standards for both privacy and security (i.e., Sarbanes-Oxley, HIPAA, FISMA, PCI DSS, NERC, ISO27001, NIST SP800-53, COPPA,etc). Moreover, in recent years, policy makers in United States and European Union, as well as countries throughout Asia, introduced new laws, regulations and guidelines to further efforts to improve information security and combat cybercrime. For instance, the European Union enacted the General Data Protection Regulation (GDPR), and adopted the Network and Information Security (NIS) Directive imposing a new set of mandates specifying risk management and incident-reporting obligations for companies and digital services providers alike, holding both companies and business services more accountable in minimizing the impact of security incidents and privacy. Compliance with such introduces or reinforces new risk management, information security, data protection and incident reporting obligations for companies and digital services providers alike, making compliance amongst the first points of discussions by those looking to deploy a cloud service.

CSPs and their customers grapple with the complexities, cost and overlap in ensuring compliance on a continuous basis. Cloud computing often introduces complex supply chains, unclear network boundaries, as well as a system of shared security responsibilities, for which distribution may vary depending on which cloud service delivery models is considered (e.g. on SaaS the customers have the least level of security responsibilities). Having that in mind, there is vested interest from cloud service provider side to both achieve compliance and to put the cloud customers in the conditions to adhere to relevant standards, laws and regulations. From the customer side, although they may offload much of the burden and responsibility of implementing the operational controls to the cloud service providers, they are still legally accountable and financially liable in case something goes wrong. Insight and information early on helps both teams more effectively plan migration with compliance in mind to minimize potential liabilities that may impact business. With that said, compliance concerns not only the IT organization, but the board of directors, making it vital that IT, security and risk/audit teams within organizations understand how service providers enable compliance to specific regulations, controls, audit frameworks, and best practices they must adhere to.

Challenges in Evaluating CSP Compliance

Cloud service providers are challenged to instill customer confidence in their ability to meet key security criteria, compliance standards and or mandates -- especially across varying industries, regions/countries and standards. Unfortunately, creating the confidence often requires a great deal of research on part of the customer, and with full knowledge and a thorough understanding of specific standards (and their most up-to-date requirements) by both parties. Most CSPs do provide full transparency needed during an assessment. They readily communicate certifications, state standards and regulations that they can help their customers comply with and respond to detailed customer inquiries about key matters, but generally when asked as part of a vetting process. Although standards such as HIPAA and PCI require that CSPs be compliant as well, CSPs are encouraged to do more to provide prospective customers with the information they need to conduct a thorough analysis and respond to audits in terms of how they meet key standards. This information must be made more accessible to those who want to know.

Today organizations are often left to engage in what can amount to a complicated, lengthy vetting process when evaluating CSPs and investigating claims and controls implementations that map to specific compliance requirements. Much of the effort in assessing providers for suitability in compliance can be quite manual. Although manually, and with persistence, you may be able to gather necessary insight and answer key questions over time, a purely manual assessment method may prove inefficient when assessing multiple CSPs. Arriving at a decision may be long to come and overburden resources. Depending upon how responsive service providers are, it can be difficult to fully determine how prescribed mandates are met, how they meet key requirements and to what degree they have controls in place. Although leading providers have teams in place dedicated to answering customer questions, engaging a CSP directly before a commitment is made may require multiple discussions, well documented spreadsheets listing all pertinent requirements across varying standards, and time to respond.

Time is a factor, as not every CSP is forth coming and willing to spend the time with organizations during the pre-contract stage. Even more so, vetting the services of different cloud providers can be a long and arduous process, as you repeat the effort of combing through various documents, online resources, contracts, service level agreements, lengthy spreadsheets and checklists. Below is a list of common challenges one may encounter when assessing CSPs for compliance. Remember, CSPs are eager to understand their clients' business and underlying operational processes to best plan service activation, not so much the other way around. It is important to seek detailed information on cloud service technologies, compliance and audit preparation as part of the CSP selection process using the most efficient information gathering methods and tools.

LIST 1: Challenges in assessing cloud service suitability and sustainability:

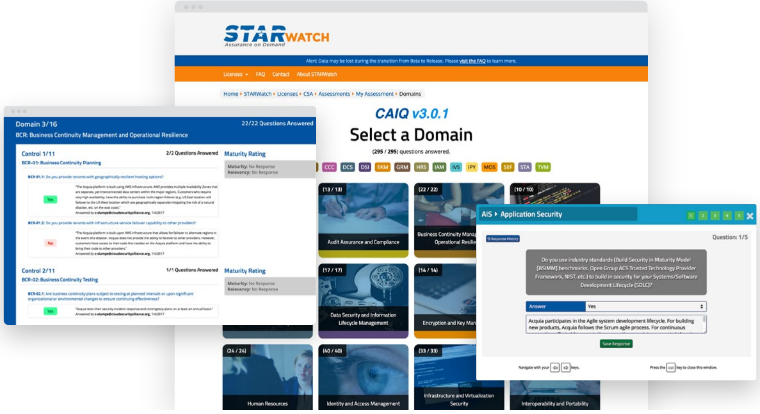
- Gathering specific information from multiple sources takes time - lots of time
- Information outlining how cloud services are secured is not readily available without request
- Proving specific requirements can be an exercise requiring in depth technical expertise
- Ensuring compliance against standards in varying countries and for different industries
- Getting a full picture of compliance across multiple CSPs for multiple areas of the company
- Employing a consistent method of information gathering and evaluation of security requirements.
- Maintaining accountability and enforcing an adequate level of due diligence during the cloud service lifecycle while dealing with in even increasing number vendors.

It is important to note that assessing the security capabilities of cloud service providers is not a one-time task, but a continuous and ongoing activity that follows the cloud service lifecycle from service selection and procurement through implementation and operation, and periodically per regular schedule until termination of service. Increasingly a key part of overall vendor management, continuous assessments of CSPs has become, and without a doubt, amongst the most critical and resource-consuming tasks performed by cloud customers seeking excellence in service implementation and assurance of accountability within their organizations and that of the CSPs of choice.

Cloud Security Alliance: Simplifying Compliance Assessments

There are steps one can take to simplify the cloud service assessment process. Cloud Security Alliance (CSA) offers tools that streamline the process and enable prospective buyers to make more informed procurement decisions when contemplating cloud migration. CSA is the world's leading organization dedicated to defining and raising awareness of best practices that help ensure a secure cloud computing environment. CSA's cloud security provider certification program, the **CSA Security, Trust & Assurance Registry (STAR)**, provides transparency and validation of the security posture of today's most used cloud offerings. CSA enables CSPs to easily publish information that provides customers with insight into the security maturity and compliance status of their offerings. Buyers can then easily see information across multiple providers in a single instance from complimentary registry that documents the security controls provided by popular cloud computing offerings. The STAR initiative is integral into providing an assessment foundation for anybody considering using cloud services. It further supports self-assessment, 3rd party auditing and continuous monitoring.

Additionally, **CSA STARWatch**, a Compliance and Assurance as a Service (CAaaS) application, helps organizations better visualize and manage compliance of CSA STAR database and requirements. Using CSA's proprietary Cloud Control Matrix (CCM), STARWatch eliminates the need for complex and lengthy spreadsheets, used in gathering information and assessing compliance across a variety of standards. CCM enables users to depict customized relationships between various industry-accepted standards, regulations, and control frameworks including ISO 27001/27002, ISACA COBIT, PCI DSS, NIST 800-53, AICPA TSC and NERC CIP, for stronger compliance assessments, monitoring and management. This provides guidance that improves internal control and facilitates the achievements of attestations and certifications for CSPs and their customers. CSA tools facilitate accuracy in information collection regarding security practices, requirements and standards and enables close monitoring of the status of compliance by CSPs and companies leveraging their services.


STARWATCH
Assurance on Demand
Licenses
FAQ
Contact
About STARWatch
Home › STARWatch › Licenses › CSA › Assessments › My Assessment › Domains
CCC
DCS
DSI
EKM
GRM
HRS
IAM
IVS
IPY
MOS
SEF
STA
TVM
(13 / 13)
Audit Assurance and Compliance
(22 / 22)
Business Continuity Management and Operational Resilience
(10 / 10)
(17 / 17)
Data Security and Information Lifecycle Management
(14 / 14)
Encryption and Key Management
(24 / 24)
Human Resources
(40 / 40)
Identity and Access Management
(33 / 33)
Infrastructure and Virtualization Security
Interoperability and Portability
Response History
Save Response
1
2
3
4
5

Alert: Data may be lost during the transition from Beta to Release. Please visit the FAQ to learn more.

CAIQ v3.0.1

Select a Domain

(295 / 295) questions answered.

Domain 3/16 — 22/22 Questions Answered

BCR: Business Continuity Management and Operational Resilience

Control 1/11 — 2/2 Questions Answered — Maturity Rating

BCR-01: Business Continuity Planning

Maturity: No Response
Relevancy: No Response

BCR-01.1: Do you provide tenants with geographically resilient hosting options?

Yes — "The Acquia platform is built using AWS infrastructure. AWS provides multiple Availability Zones that are separate, yet interconnected data centers within the major regions. Customers who require very high availability, have the ability to purchase multi-region failover (e.g. US-East location will failover to the US-West location which are geographically separate) mitigating the risk of a natural disaster, etc. on the east coast."
Answered by c-slumpe@cloudsecurityalliance.org, 1/4/2017

BCR-01.2: Do you provide tenants with infrastructure service failover capability to other providers?

No — "The Acquia platform is built upon AWS infrastructure that allows for failover to alternate regions in the event of a disaster. Acquia does not provide the ability to failover to other providers. However, customers have access to their code that resides on the Acquia platform and have the ability to bring their code to other providers."
Answered by c-slumpe@cloudsecurityalliance.org, 1/4/2017

Control 2/11 — 1/1 Questions Answered — Maturity Rating

BCR-02: Business Continuity Testing

Maturity: No Response
Relevancy: No Response

BCR-02.1: Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?

Yes — "Acquia tests their security incident response and contingency plans on at least an annual basis."
Answered by c-slumpe@cloudsecurityalliance.org, 1/4/2017

AIS › Application Security

Question: 1/5

Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?

Answer: Yes

Acquia participates in the Agile system development lifecycle. For building new products, Acquia follows the Scrum agile process. For continuous

Navigate with your ⇦ ⇨ keys.

Press the esc key to close this window.

CSA STARWatch is unique in its ability to effectively standardize security and operational risk management and make key information on security and compliance available in a robust cloud service for use throughout your organization. Whether an enterprise, or solution provider for enterprises or smaller companies, with CSA businesses can normalize security expectations across their organization and between all cloud vendors and service consumer, ensuring common cloud taxonomy, terminology, and security measures are implemented for all cloud services. More than 200 CSPs, auditors and brokers leverage the STARWatch to provide customers with rapid responses to their compliance questions, to assure a common baseline for security compliance and to drive efficiencies is with integration of cloud services.

With CSA STARWatch customers can:

- Easily create and maintain unlimited assessments through an intuitive user interface.
- Leverage a standard language (CCM) so to improve and facilitate the communication between cloud customer and provider on security controls and requirements.
- Have a clear reference between CCM controls and the corresponding controls in other industry standards.
- Assign maturity and relevance scoring to specific controls objectives.
- Log and track user changes to Consensus Assessments Initiative Questionnaire (CAIQ) domain questions.
- Import existing STAR registry assessments from over 200 major cloud service providers.
- Assign responsibilities to address assessment questions to the right subject matter expert within the organization.

About the Cloud Security Alliance

Cloud Security Alliance brings together those behind leading cloud and security technologies, governments, and individuals experts, practitioners, and associations, for cloud security-specific research, education, certification and events. CSA’s activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provides a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

Reference Resources

“Gartner Forecast Analysis: Public Cloud Services, Worldwide, 2Q16 Update”, Gartner Sid Nag | Fred Ng | David Edward Ackerman
“Growth of the Cloud Computing Industry“, WWW Metrics
“How do I choose and cloud service provider”, Microsoft Azure
“What is a cloud service provider” Tech Target
“Four Big Cloud Providers Respond to Four Big Cloud Computing Questions” , Tech Target
“Directives on Security and Network Information Systems“, European Commission
“Cybersecurity: 2015’s top legal developments and what they mean for key sectors”, DLA PIPER Publications
Performing a cloud readiness assessment: Technology, process, people, Tech Target, Crystal Bedell