Cloud Security Framework Audit Methods

Diana Salazar

Cloud Security Framework Audit Methods

GIAC (GSEC) Gold Certification

Author: Diana Salazar, salazd@protonmail.com
Advisor: Mohammed F. Haron
Accepted: 25 April 2016

Abstract

Increases in cloud computing capacity, as well as decreases in the cost of processing, are moving at a fast pace. These patterns make it incumbent upon organizations to keep pace with changes in technology that significantly influence security. Cloud security auditing depends upon the environment, and the rapid growth of cloud computing is an important new context in world economics. The small price of entry, bandwidth, and processing power capability means that individuals and organizations of all sizes have more capacity and agility to exercise shifts in computation and to disrupt industry in cyberspace than more traditional domains of business economics worldwide. An analysis of prevalent cloud security issues and the utilization of cloud audit methods can mitigate security concerns. This verification methodology indicates how to use frameworks to review cloud service providers (CSPs).

1. Introduction

> *The mantra of any good security engineer is: "Security is a not a product, but a process." It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.*
>
> — Bruce Schneier (1999)

Users have become more mobile, threats have evolved, and actors have become smarter. Users distribute information across multiple locations, many of which are not currently within the organization's infrastructure. With more reliance on clouds, data and applications are becoming more decentralized and distributed across numerous cloud service providers (CSPs). The organizational network is now just one possible location where users access applications and data. In a complex and interconnected world, no enterprise can think of its security as a stand-alone problem; this situation makes collective action nearly impossible (SANS, "Critical Security Controls for Effective," n.d.).

In the past two years, 90% of the world's data was created, increasing the proportion of all data that resides in the cloud to 66% (Brandtzæg, 2013). With the volume, velocity, and a variety of data increasing daily, within two years, 73% of all data ever created will be in cloud environments. For information technology (IT) departments, cloud security has become more important than intrusion detection. Managing cloud services and "shadow IT" is now a priority for many IT departments. The top two concerns are security and resources to handle these environments (Brandtzæg, 2013).

Current cloud computing trends indicate that the main drivers for organizations are moving from capital expenditures (CAPEX) to operational expenditures (OPEX) to bring about infrastructure savings and the delivery of strategic cloud capabilities. Initially, cloud computing was simply a platform used to transition to the next phase: the utilization of web application programming interfaces (API's) for every type of service (RightScale, 2015).

Diana Salazar, salazd@protonmail.com

By continuing to address barriers such as security, resources, and compliance for cloud adoption, organizations will be able to create new business and innovative solutions.

Data security requires a well-defined specification of the customer's and the cloud provider's responsibilities, with each having their own defined controls. The four usages identified in Figure 1 most commonly define cloud service models.

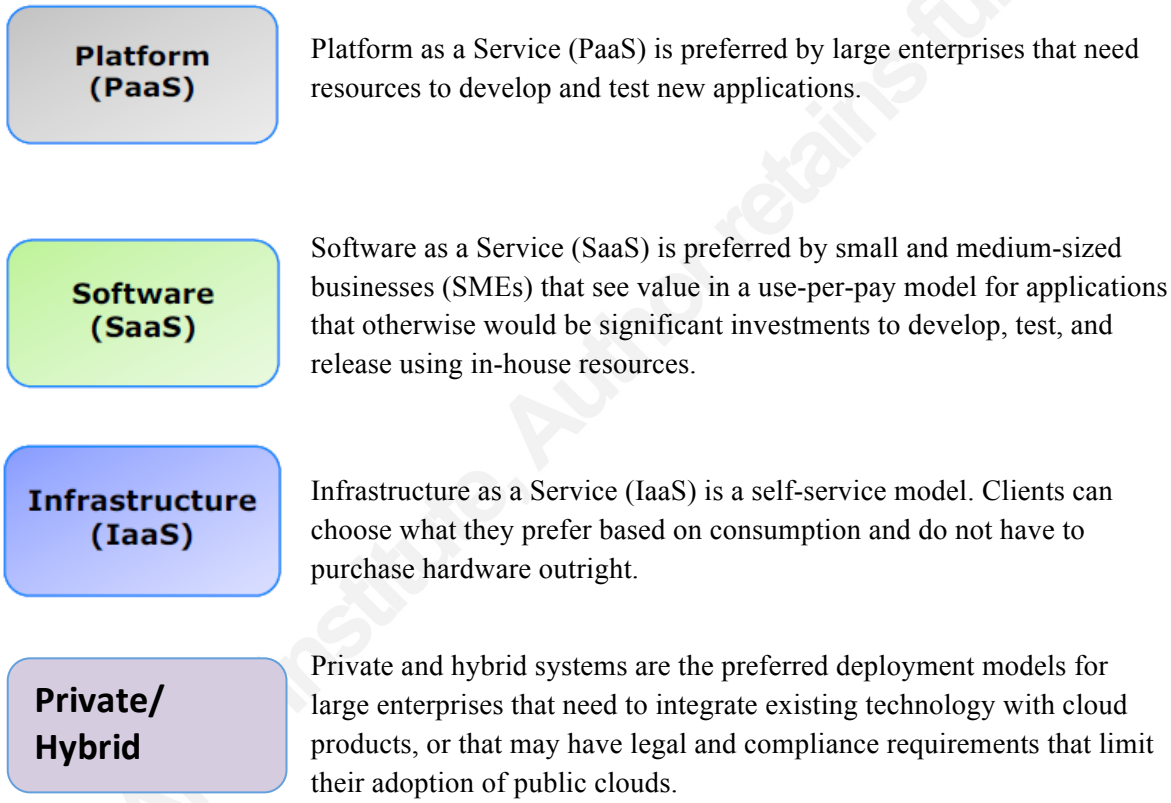

Figure 1. Four cloud service models.

As shown in Figure 2, the cloud supplier (CSP) is always held responsible for the physical server, hardware, network units, and physical buildings. The same applies to procedures concerning the operation of hardware. In terms of administration and providing functionality to customers, the responsibility of the cloud supplier is is increased when moving from IaaS to PaaS to SaaS (National IT and Telcom Agency, 2011).

Diana Salazar, salazd@protonmail.com

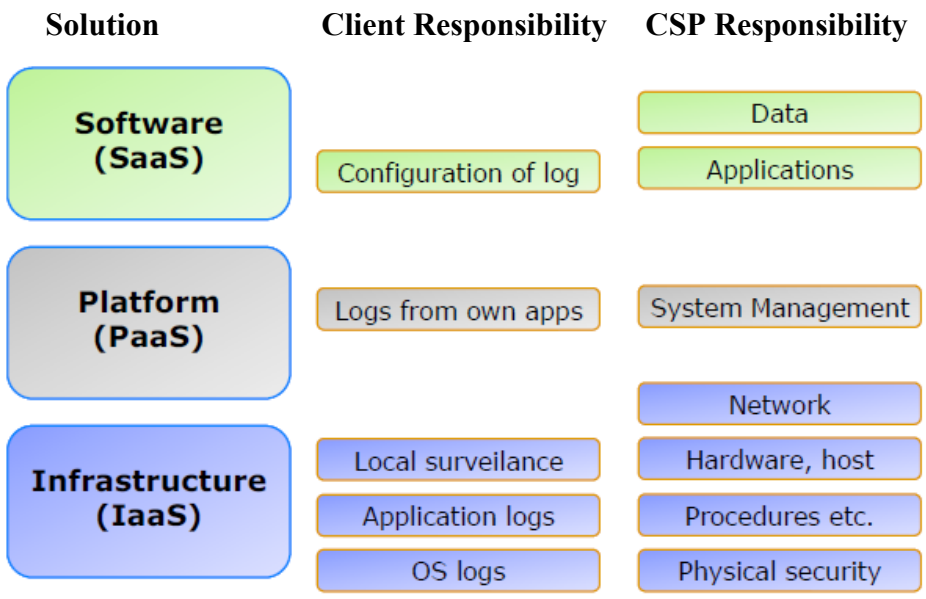

Figure 2. Cloud audit and assurance initiative (National IT and Telcom Agency, 2011).

The National Institute of Standards and Technology (NIST) provided an overview of the typical characteristics, service models, and deployment models of cloud computing (NIST, 2013).

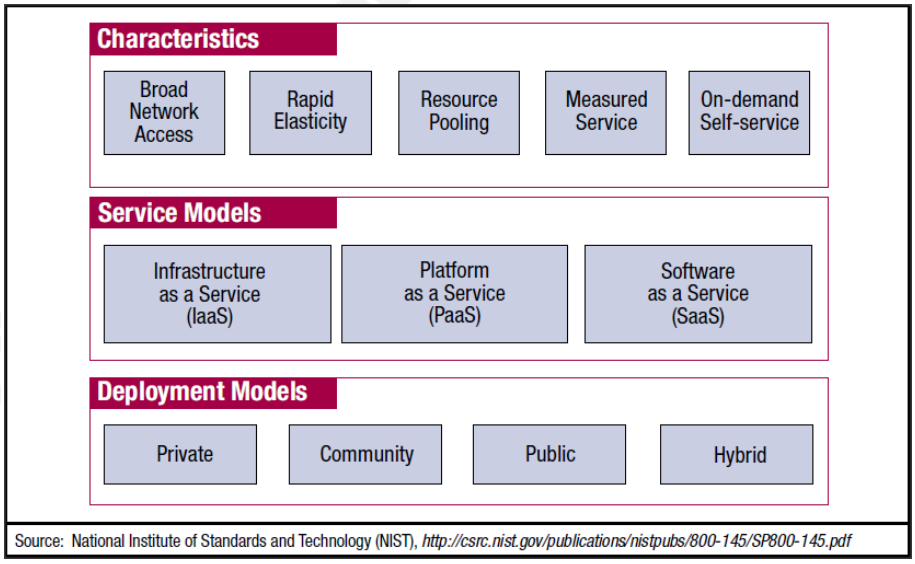

Figure 3. NIST visual model of cloud computing (NIST, 2013).

The deployment models shown in Figure 3 are described further as follows:

- Private: Comparable to buying, building, and managing the organization's infrastructure. Security concerns can be addressed

through a virtual private network (VPN) or by the physical location within the organization's firewall system. This model utilized by organizations where data or applications are required to conform to various regulatory standards (e.g., SOX, HIPAA, or GLBA) that may require data to be managed for privacy and regulations that govern the organization.

- Public: Provides pure cloud hosting with free services or those based on a pay-per-user license model. This cloud infrastructure provides for various types of clients. This model is also suitable for business requirements that make it necessary to manage load spikes, host SaaS applications, utilize short-term or instant infrastructure for SaaS applications, and to develop and manage applications for high user consumption that would otherwise require a significant investment in infrastructure from the businesses. The benefits of this model are that it reduces capital expenditure and reduces operational IT costs. Examples include the Amazon Elastic Compute Cloud (EC2), the IBM Cloud, and the Google Public Cloud.
- Hybrid: Businesses can take advantage of data hosting and security in a private cloud while also taking advantage of cost benefits by keeping shared data and applications in the public cloud. This model handles cloudbursts and load spikes, but requires a fallback option to support the load. This cloud model migrates the workload between public and private hosting without disturbing users. PaaS deployments provide their APIs for integration with internal organization applications or applications hosted on a private cloud while also maintaining security. Salesforce.com and Microsoft Azure are examples of this hybrid model.
- Community: This is a shared infrastructure model used by many organizations with the same policy and compliance considerations. This shared environment reduces costs compared to a private cloud.

Various organizations that require compliance or access to the same data can utilize a community cloud to manage applications and data. Examples are GovCloud on Amazon Web service (AWS) for the US government, FedRamp certified for unclassified information, and NYSE Euronext's Community Platform for Capital Markets, which is a financial-industry cloud.

2. Security Frameworks

The regulatory environment has become more complicated because organizations often find themselves required to comply with multiple regulations and industry mandates. As new threats emerge, regulations and standards continue to increase in number and complexity. Now, many laws carry penalties for data breaches and for not meeting timely notification of those affected. These areas of concern are addressed as the cloud environment continues to evolve with the utilization of encryption methods are incorporated as organizations define their strategy for cloud control.

The benefits of security frameworks are to protect vital processes and the systems that provide those operations. A security framework is a coordinated system of tools and behaviors in order to monitor data and transactions that are extended to where data utilization occurs, thereby providing end-to-end security (Vahradsky, 2012).

The leading frameworks and guidelines to meet regulatory requirements are as follows:

- Cybersecurity Framework that is based on the NIST framework that can be applied to any industry. The cybersecurity framework is employed to build an information security program. (NIST, 2013, 2014; SANS, 2016).
- Control Objectives for Information and Related Technology (COBIT) aligns IT with strategic business goals. This framework is commonly used to achieve compliance with Sarbanes-Oxley (ISACA, 2015).

Diana Salazar, salazd@protonmail.com

- International Organization for Standardization (ISO) is a broad information security framework applied to all types and sizes of organizations (ISO, 2015).
- The Payment Card Industry Data Security Standard (PCI DSS) is used by merchants for credit card processing (PCI-DSS, 2015; Ahmed, 2012).
- Health Information Trust Alliance (HIGHTRUST)/Health Information Technology for Economic and Clinical Health (HITECH) (CSF)/Health Information Portability and Accountability Act (HIPAA) applies to health providers and payers (HIPAA, 1996; US Department of Health and Human Services, 2009; HITRUST, 2015).
- Statement on Standards for Attestation Engagements 16 (SSAE 16) reports include the following: SOC 1, financial reporting; SOC 2, IT controls; and SOC 3, attestation (Hoehl, 2013; AICPA, 2011).
- GLBA/FFIEC/NCUA/FDIC provides security for financial services, banks, and credit unions (GLBA, 1999; FFEIC, 2015).
- Cloud Security Alliance (CSA) provides comprehensive guidance on how to establish a secure baseline for cloud operations. CSA maintains the Security, Trust & Assurance Registry (STAR) cloud provider registry (CSA, 2015).
- The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) is the national critical infrastructure framework for energy providers and utilities (NERC, 2013, 2015).
- Sarbanes-Oxley (SOX) includes publicly traded companies to meet Section 404 compliance (SOX, 2007).
- Sherwood Applied Business Security Architecture (SABSA) is used for information assurance architectures and risk management frameworks and integrates security and risk management into IT architecture methods and frameworks (SABSA, 2015).

Diana Salazar, salazd@protonmail.com

- The Unified Compliance Framework (UCF) utilizes a harmonized set of regulations and best practices to map IT controls. UCF incorporates SOX, PCI-DSS, GLBA, HIPAA, CMS, NERC-CIP, HITECH, CSF, COBIT, and ISO (UCF, 2015).
- The Privacy framework includes the rights and obligations of individuals and organizations to collect, use, retain, disclose, and dispose of personal information. Frameworks utilized are FTC's Privacy Framework and EU Privacy Directives.
- The Committee of Sponsoring Organizations (COSO) provides organizational performance and governance through effective internal control, enterprise risk management, and fraud deterrence. COSO is utilized to meet SOX compliance (COSO, 2015).
- The Organization for Economic Co-operation and Development (OECD)/ Asia-Pacific Economic Cooperation (APEC) Privacy Framework provides privacy protection through an approach grounded in risk management and requirements related to the flow of personal Cross-Border Privacy Rules (CBPR) (Privacy, 2012; OECD, 2013, FTC, 1999; European Commission, 2012; APEC, 2005; APEC-CBPR, 2011; Nymity, 2015).
- IT Assurance Framework (ITAF) provides IT audit standards that address assurance roles, responsibilities, knowledge, skills, diligence, conduct, and reporting requirements (ITAF, 2014).

The first step utilizing a framework is to determine what industry-specific compliance requirements apply to the business. Cross-reference tables are available for overlapping security controls to meet compliance requirements across the multiple frameworks that apply to an organization. Implementing a comprehensive framework prevents an adverse impact on the organization by enabling resilience and improved defenses.

Frameworks must be utilized in an appropriate context. Standards are a generic solution to an extremely individualized problem set. Cybersecurity connects directly to

business strategies and operations and must be tailored to the organization (Ruhse & Baturova, 2012). With the security unit or security role becoming a strategic business enabler, organizations can no longer afford to "check boxes" on compliance. The strategies, risks, goals, and operations of an organization should shape the cybersecurity program (Carstensen, Bernard, & Morgenthal, 2012). This program is even more critical with restricted resources and budgets because the organization needs to know where and how to scale its investments.

The new Cyber Security Framework continues to shift the mindset of security leaders towards a risk-based approach. This framework is a high-level construct designed to help "think" about problems by providing actionable guidance that enables a complete cybersecurity program to be developed in phases. By leveraging the Cyber Security Framework in addition to other leading frameworks (including maturity models), an organization can drive a security program forward to the desired state based on a set of controls and a roadmap that applies to the organization (NIST, 2014).

Specific standards require an organization to prescribe an entire suite of control objectives. To be certified, a cloud provider must materially comply with the complete set of controls and be continuously compliant.

2.1. Audit Methodology

The audit methodology utilizes an information-centric approach to review data, processes, and provide applications for clouds, hybrid, and on-premise environments employed by the organization.

The process to audit cloud vendors should be straightforward and performed by taking an inventory of data. It must determine the most important data to secure using a simple three or four level level classification: public, internal, confidential, and restricted. The audit must review information and data life cycles to determine which controls to apply to a specific step of a process or location where data resides or is in transit. It must identify where the data will live and then review data retention and the media that lies in it through the end of its data life in order to understand how and if the information will need to be encrypted throughout the life cycle.

The audit methodology includes a review of the use of cloud-based applications and unsanctioned information-sharing apps, which is known as "shadow IT." A majority of companies are leaving themselves exposed to a suite of legal, reputational, and financial risks associated with the use of unsanctioned information-sharing apps. This "shadow IT" cloud area poses a variety of unacceptable cyber risks, including: inadvertent exposure of sensitive data, possible theft of intellectual property, regulatory compliance failures, the inability to adequately identify relevant data for e-discovery, service outages, and the inadequate application of document retention.

What to do about cracking down on shadow IT apps and the risks they pose requires a bit of "tough love" from in-house legal and technology departments. A large number of applications provide little value with a lot of risks; the organization should take steps to block the use of those applications. IT and legal departments should collaborate to identify a small group of useful and sturdy cloud-based applications to sanction for employee use and put controls in place around them ("Shadow IT," 2016).

The audit methodology should review the qualifications of the cloud service provider to thoroughly vet cloud vendors. Every cloud service provider should meet basic criteria. The benefits must outweigh the enormous risks of safeguarding information assets and complying with standards set by a host of educational, industrial, and governmental precedents.

While cloud computing provides areas for advancements, it also creates new security challenges. Cloud service providers should demonstrate that they provide adequate hiring, oversight, and access controls to enforce delegation. CSPs should also be able to account for their data, even while stored in a public cloud. This accountability should ensure that the CSP is ready, willing, and able to be audited. They should also be prepared to reveal the locations of data centers and to commit to privacy requirements specified by the needs of their clients. It is critical to make sure that there is complete data segregation and the ability for a full restoration in the event of a disaster. While difficult to do, there should be some support for investigations and the portability of data. Depending on its sensitivity, data in transit should utilize encryption, and the cloud service provider should explain this fully. There should be a discussion between the

vendor and the client about physical security measures as well as who has access to the server room and the servers themselves. This access is essential to maintaining transparencies in audits, which is discussed later in this paper.

As well as this, there should be a viable data recovery system in place. Many vendors use different methods for data recovery. While some may employ high retention cloud backups, some may or may not offer a file-based restoration. There should be an explanation of any disastrous events that could cause a massive loss of client data. Backup encryption keys should also be included. The customer should understand the archival process as well as the process of monitoring and reviewing security risks and the stability of the cloud that is in place. Certain legal requirements must be followed and ongoing risks assessments enacted to manage the likelihood of information leaks. Data privacy must be integrated into risk assessments and a security policy must be in place that is based solely on cloud information. There must be measures in place to encrypt personal data and restrict access as well as a policy outlining the use of information; this should come under the umbrella of a corporate security policy. Data should be integrated into continuity plans that are conducted through regular testing of such security measures and maintained through a data loss prevention (DLP) system.

If a breach should occur, there should be an immediate response. If applicable, an incident response remediation provider should be located in addition to a forensic investigation team to track the source of the breach. The cloud service provider may or may not offer insurance coverage for a data privacy breach, as this could come as an add-on service or just not offered at all. However, there should be a reliable monitoring system in place to track and log all breaches or incidents of this nature. This security control boosts the reputability of the CSP, which is necessary for the market in which this service is growing.

Included in the cloud service should be all hardware registration numbers, including manufacturer information, serial numbers, product registration, and anything physical related to the setup of the cloud that is imperative to the needs of the client for using the service. Symantec (2014) stated, “This complexity of trust requirements drives

the need for a ubiquitous, highly reliable method to secure… data as it moves to, from and around the cloud" (p. 4).

While not often provided in litigation, a client should always question a service provider in what they can and cannot or do and/or do not supply to their customers. As the nature of the market of CSPs continues to change, the demand for better and more secure systems has risen. The need for a more streamlined and understandable process that is more transparent than confusing on the part of the client is also required. The market is evolving quickly, and certifications that will make for a well-established company can help integrate new customers into an already existing business model—a daunting task for a business new to using a CSP over an in-house provider. This business model keeps costs low while giving clients the best services.

Finally, the audit methodology must determine if the cloud provider has certifications, what type they are, and how current. The CSP must interact with the supplier to request the information needed for review. Certifications should be recent: preferably within the last 1.5 years. The client must ensure that there is the ability to audit, perform a physical review, and receive reports or logs about controls for organizational data. Audit templates must be used in order to understand the service controls in place, and reviews of cloud providers must be performed at least yearly to ensure that controls are still in place. Finally, the frequency of reporting for access control, change control, security logging, and configuration information must be determined.

Security is a shared responsibility between two organizations and security iinformation must be regularly updated. The two organizations must determine the control responsibilities of the CSP and the client organization. The controls that both organizations agreed to, along with the reporting of those controls on a periodic basis, must be reviewed with the cloud provider (Senft, Gallegos, & Davis, 2013).

2.2. Audit Checklist

When conducting an audit of a cloud service provider, utilize the investigative model outlined in Table 1 (Deloitte, 2010; Heiser, 2015; Lehigh, 2016).

Table 1.

CSP Audit Investigative Model

Area	Details
Governance	Review organizational strategy and risk appetite, roles and responsibilities, insurance, and governance tasks (Phillips, 2012).
	Monitor usage of cloud services through vendor provided dashboards or logging information available to the client.
	Address issues promptly based on governance requirements and defined roles/responsibilities.
Data Management	Perform a data flow and privacy assessment by reviewing the data throughout its life cycle. Is it vulnerable at any point?
	Ask for an overview of the dedicated, single-tenant and shared (multi-tenant) cloud services provided by the CSP.
	Review data transfer to the CSP.
	Data segregation: Review shared environments for data segregation, logical separation, and security in a multi-tenancy environment or utilize separate servers.
	Data recovery: Review if the CSP can do a complete restoration in the event of a disaster or if they have data replication capabilities available for an alternate data location. Review where that alternate location is in addition to its recoverability capabilities.
Data Environment	Where are the data centers located? Can the CSP can commit to specific privacy requirements?
	Review the applications and operating systems utilized. Use a data life cycle approach regarding what is stored and where.
	Provide a description of how often are infrastructure components are updated, such as hardware and software.
Cyber Threat	What are patch and vulnerability management program practices? How does CSP ensure these program practices do not create a security risk for client infrastructure?
	What is the vulnerability remediation process?
	Review security monitoring processes utilized by the CSP.
	Are there established application-level reviews, a defined Software Development Life Cycle process, and change notification and release management?
	Does the CSP follow Open Web Application Security Project (OWASP) and SANS top guidelines for secure application development?
	Will third party application utilization as part of the CSP services be discussed?

Area	Details
Infrastructure	Is there restricted and monitored access to assets all of the time?
	How is an employee or third party access to client data controlled?
	Are staff background checks employed? How extensive are these background record reviews and are they reoccurring?
	Vulnerability management: Patch vulnerabilities in virtual machine templates and offline virtual machines.
	Network management. Secure network traffic between distributed cloud components.
	Detection for defense against attacks originating from within the cloud environment.
	Review the perimeter for exposure to distributed denial-of-service attacks against public-facing cloud interfaces.
	System security: Review where there may be vulnerable end-user systems interacting with cloud-based applications.
	Discuss how the CSP handles secure intra-host communications among multiple virtual machines.
	Who controls encryption keys? How are the encryption keys monitored? What is their storage and backup locations? Review encryption certifications and determine what they apply to, and test them.
	How does change control occur for the cloud provider infrastructure, such as system patching, firewalls, intrusion detection, anti-malware, virtual environment management, and hardware equipment?
	Describe the ability of the CSP to troubleshoot performance issues due to continuous environment changes.
	Review demonstrations and frequency of application and penetration scans as part of the certification controls, as well as continuous monitoring and scans when changes occur to the code used for SaaS applications.
	Application security: Review the controls to monitor circumvention of application access controls by the cloud provider staff.
	Define the maximum available cloud resources.
Logs and Audit Trails	How long are logs and audit trails kept?
	How does the CSP provide for tamper proofing of logs and audit trails?
	Is there dedicated storage for logs and audit trails?
	Can the CSP provide timely forensic investigations; e.g., eDiscovery and system analysis?

Diana Salazar, salazd@protonmail.com

Area	Details
Availability	The client should review Service Level Agreement (SLA) uptime tolerance levels and check for "additional subtractions" disclaimers for the stated level.
	Review storage options, storage area network/network attached storage device (SAN/NAS), and connections to cloud client services.
	Does the CSP have resiliency (e.g., cluster systems, redundancy, and failover capabilities) and tests these abilities after changes or system updates?
	Does the CSP test restores, and what actions require additional fees?
	Where is the location of the backups (e.g., on-site, off-site, replicated to another location)?
	What file and directory versioning is available?
	Does the CSP have an incident response plan and can the CSP describe it?
	What measures are employed to guard against threat and errors, use of multiple CSPs and denial of service (DoS) protection?
	When do peaks in demand occur, and does the CSP have the capacity to handle such maximum load?
	What service level guarantee does the CSP offer under Disaster Recovery/Business Continuity conditions?
Identity and Access Management	Provide information regarding authentication, restriction of access, or implementation of segregation of duties (SOD) for cloud provider staff.
	Provide a description of the physical security measures in place within the CSP data centers, including server areas and access to host/network systems.
	Review the types of access available: single-sign-on (SSO), authentication using the client identity management software, or two-factor authentication.
	Does the client have administrative privileges and controls, and over which system components, software, and/or client users?
Encryption	Understand the environment for the service boundary, including the connection points to and from the data with encryption utilized for data in transit, data at rest, and the type of encryption.
	Ensure that the CSP provides SSL from an established Certificate Authority (CA) and the SSL CA has its practices audited annually by a trusted third party auditor; e.g., Symantec Webtrust audit or AICPA Webtrust Audit requirements.
	SSL should provide a minimum of 128-bit, 256-bit optimum, encryption based on the 2048-bit global root. Determine the type of encryption.
	Is there any encryption utilized for data at rest? For data in storage, how are encryption keys stored? For data backups that are data encrypted in transit or at rest? How are keys managed?
Privacy	How are digital identities and credentials protected in cloud applications?
	What client data is stored and used, and what is its disposal process?
	Under what conditions might third parties (including government agencies) have access to confidential data?
	Is there a guarantee that third party access to shared logs and resources will not reveal critical, sensitive information?

Diana Salazar, salazd@protonmail.com

Area	Details
Regulatory Compliance	What are the compliance requirements of the vendor or third party?
	The provider should demonstrate compliance with regulatory requirements; e.g., PCI, HIPAA, FedRamp, CSA, SSAE16 (SOC1-financial, SOC2-IT controls, SOC3-attestation), and ISO. For example: Audit and assurance information is made available on Amazon's website, under the portal AWS Security Centre: http://aws.amazon.com/security/. To obtain configuration information, use Amazon Cloudwatch: http://aws.amazon.com/cloudwatch
	AWS SSAE16 SOC 3 report
	The provider should demonstrate financial viability requirements; e.g., the SOC1 report.
	Review vendor's commitment to their and any third party utilized service to remain in such compliance.
	Discuss the CPS's commitment to maintaining the described level of security compliance and the interval of conformity updates.
Legal	Ensure that there is an engagement agreement: The right to audit and physically inspect; timely removal of data and its destruction; change control notifications; intellectual property; cloud staff hiring requirements; and training, confidentiality, backups, outsourced services to other vendors, certifications, and their maintenance renewal intervals. Ensure provider guarantees storage of the organization's data in a particular location based on the contractual agreement.
	What notification arrangements are in place for the cloud provider to notify the customer organization in the event of a suspected breach?
	What forensic investigation tools and cloud provider staff training are in place for logging and preserving evidence of an alleged violation?
	Agreed upon recourse needs to in place for security incidents, data breach, or failure to meet SLA's.
	Records management: Review the life cycle in terms of preservation, retention, eDiscovery, and disposal policies based on organization requirements.
	Review rights to data by ensuring that the client organization is the data owner for all data and applications, including replicated copies, with the right to delete all customer information if instructed with assurance documentation and promptly as agreed to by the client and CSP.
	Update the cloud contract over time to reflect operating changes.
	Specify if there are any additional fees for termination of services, delivery, or erasure of data.

Sources: Deloitte (2010); Heiser (2015); Lehigh (2016); O'Hanley & Tiller (2013).

By auditing and implementing frameworks, the majority of breaches and risks are reduced through the utilization of cloud provider environments (Halpert, 2011). While most data attacks on traditional servers are criticized due to the lack of entry and exit points in comparison to a cloud service provider, the most recent and massive data

breaches have occurred within traditional on-site IT environments. When cloud service providers take the necessary, preventative and cautionary measures to ensure data safety, they drive up demand for access to their cloud. The more secure a cloud service provider is reputed to be, the more customers will flock to it. Cloud service providers face tougher minimum standards than in-house IT and data centers simply because they are independently audited and must therefore adhere to a broad range of standards. Security between the client and the CSP must be handled with the utmost seriousness to accurately evaluate the level of security needed and for the CSP to provide security assurance for its clients.

Some customers may employ a host of CSPs, creating a multi-vendor cloud environment. This trend in IT is because many businesses want to

> build out hybrid IT portfolios that include a combination of on-premises computing and multiple cloud providers with a range of price points, service levels, and support agreements. As organizations' needs change, they'll also want the ability to shift cloud providers. (Overby, 2015, para. 5)

Given the rapid rate of change the cloud-computing market is experiencing, each company must evaluate the need for the multi-vendor cloud computing systems in place. Customers should base their decision on the need to take extra precautions to ensure the security of their data as well as the amount of data storage and the skills required to use various cloud platforms. According to Overby (2015):

> In the past, IT teams developed finely tuned processes around homogeneous resources to harden the environments and lower the risk of failure. That silo methodology is expensive—with redundant skill requirements, dashboards, toolsets, APIs and scripts to deploy, manage and automate solution stacks. Repeating this legacy approach with hybrid cloud resources will erode the very benefits organizations are trying to reap: agility, flexibility and cost reduction. (para. 11)

While there is much to consider with multi-vendor platforms, the market for CSPs is vast and ever-changing. Using research to determine the proper knowledge of a client's needs helps guide the customer to make the best decision and reduce the strain on a CSP. Cloud

computing is not a one-size-fits-all solution. Each organization has its requirements and mission. A transition to cloud computing requires research, planning, execution, and regular review of successful implementation (Cascarino, 2012).

Though there are many regulations in place for a CSP to adhere to, transparency is an increasingly common challenge within the realm of CSPs. While transparency maintains a healthy environment for a vendor to analyze security risks and to enact countermeasures against such hazards, there can be a lack of data transparency that interferes with this process.

Transparency is critical in the course of an IT audit because security-relevant data is harder to obtain from CSPs, as they control most of the data. Encryption can provide a safeguard for data, but pitfalls such as double encryption and even the lack of encryption when left up to clients and not to the service providers can create a less secure environment for data. Traditional IT infrastructure also maintains that encryption can be quite difficult and that encryption faces many concerns. Traditionally, to prevent data loss due to theft from hackers, a client would encrypt their data in-house before sending it to a cloud storage system. Therein lies the fault: Should this data, stored in the cloud, be encrypted again, it would cause the problem of double encryption. While this is not optimum from a security standpoint, accessing double encrypted information can be a nightmare. Additionally, if one part of the cloud becomes compromised through a breach or a hack, the entire cloud could be jeopardized. Therefore, most data is currently encrypted outside the cloud and sent to the cloud already encrypted to be at rest. A new type of encryption, homomorphic in nature, allows for searching encrypted data without decrypting the data itself. This homomorphic encryption could solve the "encrypted data at rest" issue for platforms of data storage and traditional and cloud storage.

With the advent of bigger and even multi-vendor cloud systems comes a whole host of problems with auditing. A security audit can "provide a clear and recognizable trail of resource access for various organizations" (Ryoo, Reizvi, Aiken, & Kissell, 2015, para. 3). Typically, there are two types of audits. The employees of a company can do an internal audit focused to a deeper degree. This internal audit provides for optimal risk and management assessments and improves organizational processes. External audits occur

from an outside source and usually follow strict regulations, both governmental and industry-specific. This external review requires the cloud service to pass regulations and meet laws that are in place for CSPs. Usually, both are used throughout traditional and non-traditional IT services.

Businesses currently considering cloud services will ask potential providers about their cloud security audit strategy. If the answer is weak, those prospective customers will consider moving on to another CSP. After all, while the allure of the cloud is to alleviate IT management burdens, it does little good if businesses cannot manage operational risks, and those operational risks cannot be managed without continuous data and exploration into the black hole of cloud security (Bruton, 2013).

While auditing is necessary to keep up the balance in the system provided by the CSP, the broad spectrum of bigger and larger clouds creates a problem of volume to audit. This vast cloud environment increases the complexities of the system, making for needed time and resources to be able to run a check of these massive systems. Because of the complexity, this creates a need for auditors to be more aware of subtle differences in cloud-specific audits. If there is standardization in place, this can vastly trim down the time and effort required to inspect these massive systems. This standardization makes the process go much smoother for auditors and clients alike. Figure 4 presents the standards applicable to cloud security auditing.

Table 2. Standards applicable to cloud security auditing.

Standard	Type	Strength	Sponsoring organization
Service Organization Control (SOC) 2	Audit for outsourced services	Technology neutral	American Institute of CPAs
ISO 27001 and 27002	Traditional security audit	Technology neutral	ISO
NIST 800-53 rev. 4	Federal government audit	Technology neutral	National Institute of Standards and Technology
Cloud Security Alliance (CSA)	Cloud-specific audit	Dedicated to cloud security auditing	CSA
Payment Card Industry (PCI) Data Security Standard (DSS)	PCI Qualified Security Assessor cloud supplement	Cloud specific and provides guidance	PCI DSS

Figure 4. Standards applicable to cloud security auditing (Ryoo et al., 2015).

According to Ryoo et al. (2015), "An audit's quality depends heavily on the auditor's cloud computing experience and knowledge" (para. 41). This audit experience could cause a major problem if an auditor is more familiar with in-house systems as opposed to constantly evolving cloud systems. Though cloud systems are becoming

increasingly popular, there is a higher demand for more secure services and a more straightforward auditing process. These secure services needs create greater demand for more quality auditors, and as systems grow with the advent of multi-vendor systems, there will be a need for audit standardization of cloud-computing services.

2.3. Global Regulation

An organization should identify laws, regulations, and standards that apply to its business for each county or jurisdiction it operates within. Regulations may fall behind as people continue to move toward bring your own devices (BYOD) and bring your own cloud (BYOC); therefore, organizations need to use a continuous process to assess their framework for cross-border data protection, information sharing, data movement, and greater interoperability among legal and privacy bodies. There should be a review of technology challenges (including application, profiling, digital education, and web tracking), removing data for the right to be forgotten requirements, and increased transparency on what data organizations are collecting and the required controls, with a comprehensive use of frameworks.

3. Conclusion

There is no easy solution to securing an organization's assets, infrastructure, and data critical to operations. The framework process and appropriate maturity model per control take time, effort, and planning. Combining policy, technology implemented with cybersecurity configurations, and incorporating audit practices provides an effective environment to mitigate the risk of attacks on systems throughout an organization's technological ecosystem.

To see what is right and not do it is a lack of courage.
— Confucius (551 - 479 BC)

Diana Salazar, salazd@protonmail.com

4. References

Ahmed, A. (2012). Meeting PCI DSS when using a cloud service provider. *ISACA*, *5*, 24-30.

American Institute of Certified Public Accountants. (2011). *Statement on standards for attestation engagements (SSAE) No. 16*. Retrieved from http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs_service_orgs.pdf

APEC cross border privacy rules (CBPR) system. (2011). Retrieved from http://www.cbprs.org/default.aspx

Asia-Pacific Economic Cooperation (APEC) Framework. (2005). Retrieved from https://cbprs.blob.core.windows.net/files/APEC%20Privacy%20Framework.pdfps

Brandtzæg, P. B. (2013). *Big data, for better or worse: 90% of world's data generated over last two years*. Retrieved from http://www.sciencedaily.com/releases/2013/05/130522085217.htm

Bruton, S. (2013, April). *Why every cloud provider needs a robust security audit strategy*. Retrieved http://searchtelecom.techtarget.com/tip/Why-every-cloud-provider-needs-a-robust-security-audit-strategy

Carstensen, J., Bernard, G., & Morgenthal, J. P. (2012). *Cloud computing: Assessing the risks*. United Kingdom: IT Governance Publishing.

Cascarino, R. E. (2012). *Auditors guide to IT auditing*. Hoboken, NJ: John Wiley and Sons, Inc.

Cloud Security Alliance (CSA). (2015). *Cloud controls matrix, assessments, certification*. Retrieved from https://cloudsecurityalliance.org/

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2015). Retrieved from http://www.coso.org/

Deloitte. (2010). *Cloud computing risk intelligence map*. Retrieved from http://www.isaca.org/Groups/Professional-English/governance-of-enterprise-it/GroupDocuments/Deloitte%20Risk%20Map%20for%20Cloud%20Computing.pdf

Diana Salazar, salazd@protonmail.com

European Commission. (2012). *Data protection rules*. Retrieved from http://ec.europa.eu/justice/data-protection/

Federal Financial Institutions Examination Council (FFIEC). (2015). *Cybersecurity assessment tool*. (2015). Retrieved from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf

Federal Trade Commission (FTC). (1999). *Financial institutions and customer information: complying with the safeguards rule.* Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

FTC. (2012). *Protecting consumer privacy in an era of rapid change*. (2012). Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

Gramm-Leach-Bliley Act (GLBA). (1999). *Examination procedures to evaluate compliance with the guidelines to safeguard customer information*. Retrieved from http://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-35a.pdf

Halpert, B. (2011). *Auditing cloud computing: A security and privacy guide*. Hoboken, NJ: John Wiley and Sons, Inc.

Health Information Trust Alliance (HITRUST). (2015). *Common security framework (CSF)*. Retrieved from https://hitrustalliance.net/hitrust-csf/

Health Insurance Portability and Accountability Act (HIPAA). (1996). Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

Heiser, J. (2015, September 22). *Clouds are secure: Are you using them securely?* Retrieved from https://www.gartner.com/doc/reprints?id=1-2OEYJKW&ct=150930&st=sb

Hoehl, M. (2013). *Understanding what service organizations are trying to SSAE*. Retrieved from https://www.sans.org/reading-room/whitepapers/auditing/understanding-service-organizations-ssae-34475

Diana Salazar, salazd@protonmail.com

Information Systems Audit and Control Association (ISACA). (2014). *Information technology assurance framework (ITAF)*. Retrieved from http://www.isaca.org/knowledge-center/itaf-is-assurance-audit-/pages/default.aspx?cid=1003567&appeal=pr

ISACA. (2015). *COBIT framework - Governance and management of IT*. Retrieved from http://www.isaca.org/cobit/pages/default.aspx

International Organization for Standardization (ISO). (2015). *ISO/IEC 27001 - Information security management*. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

National Credit Union Association. (2006). *IT security compliance guide for National Credit Union Association (NCUA) rules*. Retrieved from http://www.ncua.gov/Resources/Documents/LCU2006-07ENC.pdf

National Institute of Standards and Technology (NIST). (2013, April 30). *Security and privacy controls for federal information systems and organizations*. Special Publication 800-53 Revision 4. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST. (2014). *Framework for improving critical infrastructure cybersecurity.* Retrieved from: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

National IT and Telcom Agency. (2011, March). *Cloud audit and assurance initiative*. Retrieved https://digitaliser.dk/resource/1029260/artefact/Cloud Audit and Assurance EN_cagr.pdf

North American Electric Reliability Corporation (NERC). (2013). *CIP standard mapping to the critical security controls* (Draft). Retrieved from https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf

NERC. (2015). *Critical infrastructure protection (CIP)*. Retrieved from http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Nymity. (2015). *Nymity privacy management accountability framework*. Retrieved from https://www.nymity.com/data-privacy-resources/data-privacy-research/privacy-program-framework.aspx

Diana Salazar, salazd@protonmail.com

O'Hanley, R., & Tiller, J. S. (2013). *Information security management handbook*. Boca Raton, FL: CRC Press Taylor & Francis Group.

Organization for Economic Co-operation and Development (OECD). (2013). *The OECD privacy framework*. Retrieved from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Overby, S. (2015). *How to manage a multi-vendor cloud environment*. Retrieved from http://www.cio.com/article/3005317/cloud-computing/how-to-manage-a-multi-vendor-cloud-environment.html

Payment Card Industry (PCI) Security Standards Counsel. (2015). *Data security standards (DSS)*. (2015). Retrieved from https://www.pcisecuritystandards.org/pci_security/

Phillips, B. (2012). *IT governance for CEOs and member of the board*. Middletown, DE: CreateSpace Independent Publishing Platform.

RightScale. (2015). *State of the cloud report*. Retrieved from http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf

Ruhse, K., & Baturova, M. (2012). Cloud computing as an integral part of a modern IT strategy examples and project case studies. *ISACA, 3*, 1-4.

Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2015). *Cloud security auditing: Challenges and emerging approaches*. Retrieved from http://www.infoq.com/articles/cloud-security-auditing-challenges-and-emerging-approaches

SANS. (n.d.). *The Critical security controls for effective cyber defense* (Version 5.0). Retrieved https://www.sans.org/media/critical-security-controls/CSC-5.pdf

SANS. (2016). *CIS critical security controls: Guidelines*. Retrieved from https://www.sans.org/critical-security-controls/guidelines

Schneier, B. (1999, December 15). *Security is not a product; it's a process*. Retrieved from https://www.schneier.com/crypto-gram/archives/1999/1215.html#1

Senft, S., Gallegos, F., & Davis, A. (2013). *Information technology control and audit.* Boca Raton, FL: CRC Press Taylor & Francis Group.

Diana Salazar, salazd@protonmail.com

Shadow IT: The looming cybersecurity threat you probably aren't addressing. (2016, March 20). *The Global Legal Post*. Retrieved http://m.globallegalpost.com/corporate-counsel/shadow-it-the-looming-cybersecurity-threat-you-probably-arent-addressing-73311612/

Sherwood Applied Business Security Architecture (SABSA). (2015). *Security framework, architectures, risk & governance*. (2015). Retrieved from http://www.sabsa.org/

Symantec. (2014). *White paper choosing a cloud hosting provider with confidence*, (4 pps.). Retrieved from https://www.symantec.com/content/en/us/enterprise/white_papers/b-choosing-a-cloud-hosting-provider-with-confidence_WP.pdf

Unified compliance framework (UCF). (2015). Retrieved from https://www.unifiedcompliance.com/

US Government Publishing Office. (2012). *Privacy of consumer financial information*. Retrieved from http://www.gpo.gov/fdsys/granule/CFR-2012-title12-vol5/CFR-2012-title12-vol5-part332

US Department of Health and Human Services. (2009). *Health information technology for economic and clinical health (HITECH): Health information privacy*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

US Office of the Comptroller of Currency. (2011). *Privacy of consumer financial information & GLBA*. (2011). Retrieved from http://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/pcfi.pdf

US Securities and Exchange Commission. (2007). *Sarbanes-Oxley (SOX) Section 404: A guide for small business*. (2007). Retrieved from https://www.sec.gov/info/smallbus/404guide/intro.shtml

Vahradsky, D. (2012). Cloud risk: 10 principals and a framework for assessment. *ISACA, 5,* 1-12.

Last Updated: March 20th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
SANS Jeddah March 2019	OnlineSA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced