3-2021

Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud

Vyshnavi Sailakshmi
vyshnavi.sailakshmi@gmail.com

Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud

by

Vyshnavi Sailakshmi

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

May, 2021

Starred Paper Committee:
Abdullah Abu Hussein, Chairperson
Nimantha P. Manamperi
Changsoo Sohn

Abstract

This research paper aims to identify the gaps in information related to mapping the cloud security alliance top 20 critical controls against cloud security services provided by the major cloud providers. This paper will be reviewing the security controls against the cloud security applications and services provided by major cloud providers. Most organizations are adopting the cloud for their business-critical applications. Organizations need to be compliant with various frameworks relevant to their industries. Along with cloud security controls, organizations also need to perform an audit that measures the organization's security policies to maintain compliance. Although a vast amount of information on cloud security is available, we still hear about cloud systems attacks. This paper focuses on providing baseline information on cloud security controls published by Cloud Security Alliance (Cloud Security Alliance, 2019) and map them to cloud services. Information technology professionals need to review the cloud security measures in AWS, Google Cloud, Azure against Cloud Security Alliance top 20 controls, which will help the cloud user make an informed decision. This paper assists as a decision support document for the cloud user who wants to understand the role of security controls in a cloud environment and address the cloud security risks. Cloud users, cloud architects, and cloud consumers will understand how various cloud providers offer tools that assist in maintaining the security controls. This research paper provides the base layer information and aims to help future research in cloud security controls.

Acknowledgment

I would like to express my sincere gratitude to my supervisors and committee members, Dr. Abu Hussein, Abdullah; Dr. Manamperi, Nimantha P.; and Dr. Sohn, Changsoo for providing their invaluable guidance, comments, and suggestions throughout the research paper.

Table of Contents

Chapter Page

Chapter Page

List of Tables

Table Page

Chapter I: Introduction

Introduction

Cloud technology is gaining popularity, and organizations are adopting them rapidly due to multiple benefits. Enterprise resource planning applications are using hybrid architecture for their critical business processes. The cloud security alliance published the top 20 essential controls to assist the enterprises, which are most vital and cover significant security risks in the cloud (Cloud Security Alliance, 2019).

Along with cloud security controls, organizations also need to perform an audit that measures the organization's security policies to maintain compliance. Although a vast amount of information on cloud security is available, we still hear about cloud systems attacks. This paper focuses on providing baseline information on cloud security controls ranked top 20 by Cloud Security Alliance and mapped them to cloud services (Cloud Security Alliance, 2019).

Problem Statement

Although there are many efforts by researchers from academia and industry to educate organizations planning to move to the cloud about the necessary cloud security controls, we still hear about various attacks and how they are targeting organizations' cloud environments resulting in data breaches. Cloud data breaches could be attributed to the fact that these organizations still lack the know-how to apply these controls properly. This paper aims to address cloud data breaches by mapping Cloud Security Alliance (CSA) top 20 cloud security controls against AWS, GCP, and Azure cloud providers.

Nature and Significance of the Problem

According to a report published by the Ponemon Institute (2015), an average number of 1.7 successful attacks per company each week. This number shows an increase in attacks from the 1.3 successful attacks per company each week observed in 2012. While analyzing the security breaches, the Ponemon Institute (2015) discovered that 7% of the worst security breaches were partly caused by senior management giving insufficient priority to security which was down 12% from a year ago.

Security is a continuous effort to keep the system in a secure state according to government guidelines and other industry-based compliance requirements. Many small and medium scale organizations are moving to the cloud to reduce their cost expenditure on information technology requirements. These are the primary targets for security breaches. Small business organizations have a limited budget to prioritize security and to reap a maximum return on investment. Furthermore, small businesses need to identify critical security controls and tools to monitor and prevent security breaches. The goal of this paper is to help with identifying the essential security controls and how each major cloud service provider can provide them (Gartner Research, 2020).

There is a wealth of cloud information available for the general public to access. But limited information is available when a user tries to review the top three cloud providers Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure, based on Gartner Research, 2020 Cloud Assessment (Gartner Research, 2020), against the Cloud Security Alliance top 20 critical controls (Cloud Security Alliance, 2019).

Organizations perform audits that measure controls defined by their security policies, which are believed to assess the system's security. Critical concerns are security deployments, software updates patching, policy changes, new tools, and changing cyber threat landscape. Measuring the effectiveness and return on investment from the security mechanisms requires actionable security metrics. Auditors now include the cloud systems and cloud security controls in the audit scope. This work is part of the process to ensure cloud systems are compliant. Periodic review of security control results in either pass or fail. If a control fails during an audit, it requires remediation. This continuous process ensures organizations are secure. If control is misconfigured, its effectiveness to prevent an attack also decreases. Smaller organizations are preferring to transfer the risk by selecting a service from the cloud provider. This requires the cloud users to understand cloud security controls and the service offered by the cloud providers.

The Objective of the Research

This study reviews the cloud security services in Amazon Web Services (AWS), Microsoft Azure, and Google Cloud against cloud security alliance top 20 security controls. Review of cloud security controls according to the cloud security alliance. Comparison of cloud security services in AWS, AZURE, Google Cloud against CSA (Cloud Security Alliance, 2019) top 20 controls.

The study is not biased towards any product or organization but only offers a review of the three popular cloud service providers. This review will show how cloud security controls effectively mitigate 80% of known security risks in the cloud. The security controls can only reduce the known security risks and should be able to consolidate the risks addressed in security policies.

Limitations of the Research

This research paper aims to supplement the information available for the cloud user on security controls while focusing on services and applications provided by the major cloud providers. Due to the limitations, we review these controls on a high level and analyze the primary function of the control. Some additional security features are from paid cloud-managed security providers. Due to limitations, we are not going to specify if they are not available from the cloud service provider. The research is limited to cloud security alliance (Cloud Security Alliance, 2019) top 20 security controls only.

Summary

This section will discuss the importance of security controls and cloud audits and the lack of information to compare cloud security controls against cloud providers. Research objectivities and Nature, and significance of the problem were explained in detail and various research limitations related to the research area and the information constraints we presented to the reader. The next chapter will include the background and literature review related to security and comparison methodology.

Definition of Terms

The terms in security and information technology or technical so to provide accurate and precise verbiage regarding these technical jargons I have taken the definitions from the SANS institute website (SANS, 2017).

- Access Control: Access Control ensures that resources are only granted to those users who are entitled to them.

- Access Control List (ACL): A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.
- Access Control Service: A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.
- Access Management: Access Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.
- Activity Monitors: Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system and blocking that activity when possible.
- Advanced Encryption Standard (AES). An encryption standard being developed by NIST. It intended to specify an unclassified, publicly disclosed, symmetric encryption algorithm.
- Algorithm. A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that a computer can implement.
- Asymmetric Cryptography: Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair different steps of the algorithm.
- Auditing: Auditing is the information gathering and analysis of assets to ensure policy compliance and security from vulnerabilities.

- Authentication: Authentication is the process of confirming the correctness of the claimed identity.
- Authenticity: Authenticity is the validity and conformance of the original information.
- Authorization: Authorization is the approval, permission, or empowerment for someone or something to do something.
- Autonomous System: One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An independent system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).
- Availability: Availability is the need to ensure that the system's business purpose can be met and that it is accessible to those who need to use it.
- Bandwidth: Commonly used to mean a communication channel's capacity to pass data through the track in a given amount of time and usually expressed in bits per second.
- Botnet: A botnet is a large number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial-of-service attack.
- Brute Force: A cryptanalysis technique or other kind of attack method involving an extra procedure that tries all possibilities, one-by-one.
- Buffer Overflow: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since system memory is created to contain a finite amount of data, the extra information -

which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

- Business Continuity Plan (BCP): A Business Continuity Plan is a plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency.
- Business Impact Analysis (BIA): A Business Impact Analysis determines what levels of impact to a system are tolerable.
- Certificate-Based Authentication: Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.
- Client: A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.
- Cold/Warm/Hot Disaster Recovery Site:
  - Hot site. It contains fully redundant hardware and software, telecommunications, telephone and, utility connectivity to continue all primary site operations. Failover occurs within minutes or hours following a disaster. Daily data synchronization usually occurs between the prior and hot sites resulting in minimum or no data loss. Offsite data backup tapes might be obtained and delivered to the hot spot to help restore operations. Backup tapes should be regularly tested to detect data corruption, malicious code, and environmental damage. A hot spot is the most expensive option.

  - Warm site. It contains partially redundant hardware and software, with telecommunications, telephone, and utility connectivity to continue some, but not all, primary site operations. Failover occurs within hours or a day following a disaster. Daily or weekly data synchronization usually occurs between the prior and warm sites resulting in minimum data loss. Offsite data backup tapes must be obtained and delivered to the warm site to restore operations. A warm site is the second most expensive option.
  - Cold site. Hardware is ordered, shipped, and installed, and software is loaded. Basic telecommunications, telephone, and utility connectivity might need turning on to continue some, but not all, primary site operations. Relocation occurs within weeks or longer, depending on hardware arrival time, following a disaster. No data synchronization occurs between the primary and cold sites and could result in significant data loss. Offsite data backup tapes must be obtained and delivered to the cold site to restore operations. A cold site is the least expensive option.

- Confidentiality: Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
- Configuration Management: Establish a known baseline condition and manage it
- Countermeasure: Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders from gaining further access to a computer network. Other countermeasures are patches, access control lists, and malware filters.

- Defense In-Depth: Defense In-Depth is the approach of using multiple layers of security to guard against the failure of a single security component.
- Demilitarized Zone (DMZ): In computer security, in general, a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZs provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet that is used for servers accessible from the outside is referred to as a DMZ.
- Denial of Service: The prevention of authorized access to a system resource or the delaying of system operations and functions.
- Dictionary Attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.
- Due Care: Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.
- Due Diligence: Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse and additionally deploy a means to detect them if they occur.

- Encryption: Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used.
- Firewall: A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.
- Integrity: Integrity is the need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete.
- Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet.
- Internet Protocol Security (IPsec): A developing standard for security at the network or packet processing layer of network communication.
- Internet Standard: A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support and is recognizably useful in some or all parts of the Internet.
- Intrusion Detection: A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

- IP Address: A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.
- Least Privilege: Least Privilege is the principle of allowing users or applications the least number of permissions necessary to perform their intended function.
- Malicious Code: Software (e.g., Trojan horse) that appears to perform a useful or desirable function but gains unauthorized access to system resources or tricks a user into executing other malicious logic.
- Malware: A generic term for several different types of malicious code. National Institute of Standards and Technology
- (NIST): National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science in developing and using these standards.
- Patching: Patching is the process of updating software to a different version.
- Payload: Payload is the actual application data a packet contains.
- Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
- Penetration Testing: Penetration testing is used to test the external perimeter security of a network or facility.
- Permutation: Permutation keeps the same letters but changes the position within a text to scramble the message.

- Port: A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.
- Port Scan: A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number the laptop provides. Port scanning, a favorite compute cracker idea of where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
- Protocol: A formal specification for communicating; an IP address the unique set of rules that endpoints in a telecommunication connection use when they speak. Protocols exist at several levels in a telecommunication connection.
- Protocol Stacks (OSI): A set of network protocol layers that work together.
- Proxy Server: A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from external intrusion.
- Public Key: The publicly disclosed component of a pair of cryptographic keys used for asymmetric cryptography.
- Public Key Encryption: The popular synonym for "asymmetric cryptography."

- Public Key Infrastructure (PKI): A PKI (critical public infrastructure) enables users of an unsecured public network such as the Internet to exchange data and money securely and privately through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
- Ransomware: A type of malware that is a form of extortion. It works by encrypting a victim's hard drive, denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.
- Reconnaissance: Reconnaissance is the phase of an attack where an attacker finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.
- Risk: Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.
- Risk Assessment: A Risk Assessment is a process by which risks are identified and the impact of those risks determined.
- Risk-Averse: Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail to avoid risks associated with e-mail may be considered "Risk Averse."
- Role-Based Access Control: Role-based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.
- Root: Root is the name of the administrator account in Unix systems.

- Secure Sockets Layer (SSL): A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.
- Security Policy: A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
- Social Engineering: A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.
- Software: Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.
- System-Specific Policy: A System-specific policy is a policy written for a specific system or device.
- TCP/IP: A synonym for "Internet Protocol Suite," The Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the primary communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).
- Threat Assessment: A threat assessment is the identification of types of threats that an organization might be exposed to.
- User: A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

- Virtual Private Network (VPN): A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, suppose a corporation has LANs at several different sites, each connected to the Internet by a firewall. In that case, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a real dedicated network because the virtual network shares the cost of system resources with other users of the virtual grid.
- Vishing: A form of phishing attack which takes place over VoIP. In this attack, the attacker uses VoIP systems to call any phone number with no toll-charge expense. The attacker often falsifies their caller-ID to deceive victims into believing they are receiving a phone call from a legitimate or trustworthy source such as a bank, retail outlet, law enforcement, or charity. The victims do not need to be using VoIP themselves in order to hack over their phone system by a vishing attack. (See phishing.)
- Vulnerability: Vulnerability an asset or security protection that would allow a threat to cause harm. It may be a flaw in coding, a mistake in configuration, a limitation of scope or capability, an error in architecture, design, or logic, or a clever abuse of sound systems and their functions.

- Whitelist: A security mechanism prohibits the execution of any program that is not on a pre-approved list of software. The whitelist is often a list of the file name, path, file size, and hash value of the approved software. Any code that is not on the list, whether benign or malicious, will not execute on the protected system. (See blacklist.)
- Wi-Fi: A means to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, including speed, frequency, authentication, and encryption.
- Worm: A form of malware that focuses on replication and distribution. A worm is a self-contained malicious program that attempts to duplicate itself and spread it to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encounters
- Zombie: A term related to the malicious concept of a botnet. The term zombie can refer to the system that is host to the malware agent of the botnet or to the malware agent itself. If the former, the zombie is the system that is blinding performing tasks based on instructions from an external and remote hacker. If the latter, the zombie is the tool that is performing malicious actions such as DoS flooding, SPAM transmission, eavesdropping on VoIP calls or falsifying DNS resolutions as one member of a botnet. (SANS, 2017)

Chapter II: Background and Review of Literature

Introduction

The second chapter discusses the background and literature related to the problem, discussing the significance of security metrics and measures and Cloud Security Alliance (CSA) top 20 security controls. The methods of security measures and different implementation methodologies. The literature review includes the various security measures, and metric performance shows they are designed and implemented. Information on cloud computing technology the multiple risks it adds to the security policies.

Background Related to the Problem

David Komendat, VP and CSO for Boeing, stated:

> Security Leaders now also need to be a business leader you have to look at your peers and leadership, and all of those folks have metrics that they use every day to run and manage your business you need indicators of the health of what you're doing and so if you're running a security organization and you don't have some metrics package, then you don't know how effective your organization is at accomplishing its mission. (cited in Brandel, 2011)

One of the significant security problems is adopting or implementing security measures that can accurately identify the status of security in the system and detect breaches. Data breaches have been happening even with more emphasis on security, and now, when companies are moving to the cloud, this adds more challenges to already existing difficulty in monitoring security. Data is moved from an on-premises location to the cloud environment, and this process increases the risk, which needs a secure method. The increase in risk results in multiple security

controls, without which it is challenging to plan security systems engineering. This paper also aims to examine different requirements for cloud security and compare various cloud providers to ensure that they satisfy the critical security controls mentioned in CSA's top 20 security controls.

Literature Related to the Problem

Cloud security is the number one challenge, creating hurdles for many organizations adopting cloud into their information systems. This is consistently ranked as a top security challenge due to a lack of clarity regarding cloud computing security issues. To reduce the severity of this challenge, we use various cloud definitions and references to address. The majority of organizations are willing to inform their users about the breach but conceal the details unless government organizations require this. To understand the scale of the attacks, we look into cloud data breaches in health care.

In this paper, we will shed light on data breaches that happened in the United States since 2009. We chose healthcare as our concentration as it is a goldmine of patient's sensitive health information, known as PHI (Protected Health Information). PHI consists of data like Patients first and last name, date of birth, address, phone number, email address, bank details, credit/debit card information. It is considered a very alluring "one-stop-shop" by the attacker.

As per Health Information Technology for Economic and Clinical Health (HITECH) Act all the health information breaches affecting more than 500 individuals have to be reported to the Department of Health and Human Services. We found a list of healthcare providers breached from 2009 to 2016. A total of 1802 healthcare providers (including hospitals, private doctors,

clinics) reported breaches in their facilities which affected 171 million individuals, out of which 163 providers were breached multiple times (Adler, 2020).

We now would briefly discuss incidents in the most significant data breaches and provide a high-level report that covers the breaches' reasons for all the providers. As many organizations would not reveal information about their data breaches, we will report all that we could find. AHMC Healthcare Inc. and affiliated Hospitals was the second most significant breach of the year. Two unencrypted laptops were stolen with 729,000 patients' information, including patients' names, Medicare/insurance identification numbers, diagnosis/ procedure codes, and insurance/patient payment records and SSNs (Winton, 2013).

Texas Health, Fort Worth, Texas, contracted with Shred-it International Inc. to safely dispose of their confidential patient information. However, residents found microfilm pieces containing 277,000 patients' information in a park and two other public areas. The provider informed that microfilms need special equipment to read them, so it is a little secure than paper (McCann, 2013).

Digital Archive Management, a vendor for El Centro Regional Medical Center, lost 189,000 patients' records. The vendor misplaced the x-rays provided by ERMC to digitize and preserve. The misplaced data contains patients' x-rays, paper jackets containing the films, written interpretations, patient names, dates of birth, addresses, medical record numbers, ECRMC account numbers, physicians' names, diagnoses, radiology procedures, radiology interpretations, health insurance numbers, and in some cases SSNs (DataBreaches.net, 2011).

RCR Technology Corporation, hired by Indiana Family and Social Services Administration, was responsible for exposing 187,000 patients' information because of a

programming error. Because of the mistake, they emailed many clients with information about other clients' demographic data, types of benefits received, monthly benefit amount, employer information, financial data, bank balances, and other assets, medical information such as providers, disability benefits, and medical condition, and specific information about the client's household members like name, gender, and date of birth (McCann, 2013).

Community Health Systems Professional Services Corporation reported a network attack originating from China twice in the same year. As a result, the non-medical information of 4.5 million individuals was stolen. The network was hacked because a test server that was not supposed to be connected to the internet was connected and had VPN credentials stored in its memory. Using those credentials, hackers could access the provider's servers and steal the data (Knippa, 2014).

Xerox State Healthcare, LLC failed to return computer equipment and paper files to Texas Health and Human Services Commission (THHSC) after their contract has ended, resulting in 2 million patient records exposed, including personal identifiers, Medicaid numbers, and Protected Health Information (Xerox, 2014).

The most significant healthcare breach happened in 2015 when 78.8 million records from Anthem, Inc. were exposed to the second-largest health insurance provider, including personal information such as names, dates of birth, addresses, and email addresses, along with Social Security numbers, medical IDs. A database administrator discovered that his credentials were being used to run a query he did not initiate (Ragan, 2015).

Premera Blue Cross was the second-largest breach with 11 million records. Investigators report that this could be a phishing attack where a site was made with a spelling "prennera,"

which looked like Premera and gathered users' credentials to succeed in breaching the databases (Krebs, 2015).

The year 2015 was the year of health care breaches. The next victim was Excellus Health Plan, Inc. The details of the breach were not revealed. However, it was reported that hackers were in their network undetected for two years. The security breach resulted in a loss of 10 million patient records (Kern, 2015).

University of California, Los Angeles Health stands in the fourth position with 4.5 million records stolen. The breach was noticed when a suspicious network activity was discovered. No other information was released about the method of hacking (UCLA, 2015).

Medical Informatics Engineering detected an unusual load on their company's network monitoring systems and discovered that hackers had access to their servers. They immediately responded by shutting down the affected server and notified their 3.9 million customers (Adler, 2015).

In 2016, Banner Health was hacked from the POS credit card machines, which later expanded to stealing medical information. They lost 3.7 million individuals' information, including names, birth dates, addresses, physicians' names, dates of service, claims data, and possibly health insurance information and Social Security numbers (Modern Healthcare, 2016).

New York-based Newkirk Products, Inc. discovered that there is unauthorized access to one of their servers. It resulted in the exposure of 3.5 million customers. They responded immediately by shutting down that server. The exposed data included member names, mailing addresses, type of plan, member and group ID numbers, names of dependents enrolled in the

program, primary care providers, and in some cases, dates of birth, premium invoice information, and Medicaid ID numbers (Snell, 2016).

21st Century Oncology reported that they were investigating an unauthorized third-party intrusion into their network. This incident impacted 2.2 million customers. They claim that there is no evidence that the patient's information has been misused and provided a year's worth of free credit check (DataBreaches.net, 2011).

Like the top three attacks above, Valley Anesthesiology Consultants, Inc. reported that they were investigating an unauthorized third-party intrusion into their network. This incident impacted 882,000 customers impacted by this incident. The forensic team they hired to examine could not determine if patient information was accessed but could not rule out the intrusion (Valley Anesthesiology, 2016). The County of Los Angeles Departments of Health and Mental Health was a victim of the phishing attack. One hundred eight employees were tricked into giving their usernames and passwords through a legitimate-looking email. This impacted 749,000 patients. The scammer was caught and charged with unauthorized computer access and identity theft (McGee, 2016).

The European Network and Information Security Agency (ENISA) (2012) defined cloud computing as "an on-demand service model for IT provision, often based on virtualization and distributed computing technologies" (p. 4). They defined the cloud as an abstracted resource that is available instantly and highly scalable and can be self-provisioned.

The National Institute of Standards and Technology (NIST) (2011) termed cloud definition as:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST, 2011)

NIST (2011) listed five essential qualities of cloud computing, resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service. It also listed software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)) and four deployment models (private, community, public, and hybrid), which broadly define cloud computing models. NIST also published a cloud computing reference architecture. The definitions and architecture references provide us with a basic foundation upon which helps to analyze the security issues. In this paper, a review of security control measures in Amazon Web Services (AWS), Azure, Google Cloud will be analyzed for security controls and benchmarking them against CIS's top 20 security controls.

> Security metrics which include the product evaluation criteria identification, Information Assurance (IA) strength quantification, risk assessment/analysis methodology development, and other techniques to provide a metric which utilizes a simplicity in implementation and operation. Rating security goodness, purchasing a given countermeasure, operating, or retiring a given system component. To date, computer science has frustrated these activities by providing neither generally accepted nor reliable measures for rating IT security or requisite security assurance. "Furthermore, inconsistent terminology has complicated the development of IT metrics, often confusing single

> measurements with accepted metrics, such as rating, ranking, quantifying, or scoring measurements. (Vaughn, Henning, & Siraj, 2003, p. 1)

Metrics for Organizational Security were in demand to assess the state of security under the taxonomy of metrics. At the 36th Hawaii International Conference on System Sciences (HICSS'03), a workshop was conducted for classifying the metrics insecurity. Some of the outcomes of the workshop were discussed (Vaughn et al., 2003. A single metric will not be enough for security as it is complicated needed multiple security measures. Software and design of architecture influence the establishment of metrics. Periodic penetration testing is required to identify vulnerabilities. Processes, procedures, tools, and people all interact to produce assurance in systems (Vaughn et al., 2003).

Literature Review on Cloud Data Breaches

Attacks on cloud services rapidly increased in 2019, matching the growth of the cloud adoption of the organization, according to the report published by the *2020 Trustwave Global Security Report* (Trustwave, 2020). The report highlighted cyber-criminals prominently target that cloud services. The report also mentioned that the ransomware attacks had surpassed the payment card data breaches. This is higher than the told payment card data breaches.

One of the significant finding from the report is that the number of spam email attacks targeting the organizations reduced from 45.3% in 2018 to 28.3% in 2019. This indicates the effectiveness of security controls and security operations organizations have implemented to mitigate Spam email attacks (Trustwave, 2020). The report included information from security logs that have logged over trillion security events, including compromised events, data breaches, and security incident investigations—showing the changes in Tactics, Techniques, and

Procedures (TTP) of attackers. Due to a spike in ransomware attacks and increased spending to harden security, organizations have reported increased operational expenditure and business impact, which resulted in substantial monetary loss (Trustwave, 2020).

A report by Microsoft (2020b) entitled *Microsoft Digital Defense Report* stated that organizations that are highly dependent on the cloud face increased attacks from cyber-criminals. The report stated that the attacks on Microsoft's cloud-based accounts have increased by 300% since 2016. Cyber-criminals are using attack techniques like using compromised cloud infrastructure to launch fishing attacks. The compromised infrastructure provides more cybercriminals to make phishing campaigns under trusted brands like Microsoft. This has caused a significant impact on the brand reputation of popular cloud providers (Microsoft, 2020b).

Increased Distributed Denial of Service (DDoS) attacks as cyber-criminals are using the increased data traffic and internet usage due to Covid-19. Most of the organization's users are working from home and use digital conference solutions. These attacks disrupt the organization's network traffic and bring down the websites, primarily used as a smokescreen to blend in with traffic. Attackers launch a more sophisticated and focused attack while the network professionals are busy with the DDoS attack, which acts as a misdirection (Microsoft, 2020b).

Data leakage and data loss have also increased with increased VPN usage and personal devices used for work. Many organizations are using multiple cloud vendors who require cross-cloud security controls to mitigate the risk of attack from another cloud provider's compromised instance (Microsoft, 2020b).

According to Sanhotra (2020) in his report, *The State of Cloud Security 2020*, 75% of the organizations which host data in the public cloud have faced a security incident in 2019. Seventy

percent of faced attacks like ransomware and malware attacks in 2019. Four percent of organizations were concerned about data loss and data leakage. Ninety-six percent of the organizations have concerns with their current effectiveness of cloud security. Multi-cloud organizations have faced more security incidents than those using a single platform. The report infers that European organizations faced reduced attacks compared to other regions due to increased guidelines of the General Data Protection Regulation (GDPR) (Sanhotra, 2020).

Despite the number of attacks, only one in four organizations have mentioned the lack of cybersecurity professionals' technical security expertise as a top concern. Most organizations underappreciate the requirement of excellent technical expertise to harden the security postures of the organization. Sixty-six percent of the organizations leave the backdoor open, which the attackers exploit. Sixty-six percent of the attacks were due to security gaps caused by misconfiguration. Thirty-three percent of the attacks were due to stolen credentials where the cyber-criminals used compromised credentials to get into cloud provider accounts. Loss of sensitive data has impacted brand reputation and resulted in legal cases against the organizations resulting in vast amounts of compensation and regulatory fines (Sanhotra, 2020).

Aqua Security has installed a honeypot in the public cloud environment and recorded one year's worth of cyber-criminal attacks. The honeypot revealed an interesting finding that most hackers have targeted had cloud infrastructure to install crypto-mining malware instead of the usual target of sensitive data. Aqua Security's Security captured more than 16,000 attacks from June 2019 to June 2020, where the peak of attacks was during the start of the year 2020, which was a 250% spike than the previous year (Aquasec, 2021).

The mode of operation (modus operandum) of the cyber-criminals is to acquire the honeypot's control to deploy the malicious code. Attackers used a container image that contains the malicious code, which was downloaded to compromised instances and deployed. Analysis of the container images revealed that 95% of the malicious images were focused on crypto-mining and the remaining 5% concentrate on targeted DDoS attacks. Aqua has also mentioned that their analysis shows that cyber-attacks have patterns that indicated organized cybercrime organizations are increasing their compromised cyberinfrastructure for future episodes (Aquasec, 2021).

Organized cybercrime groups have increased the number of attacks and sophistication, raising the complexity of the attacks. Multiple intrusion patterns and complex malware have increased the difficulty of detecting and resolving security incidents. The patterns also identify the increased usage of supply chain attacks that exploit unpatched software and systems' vulnerabilities. Many of the attacks were carried out by placing malware containers that look like regular containers and are also hard to detect with static containers analysis and evading signature-based security systems (Aquasec, 2021).

Aquasec (2021) also mentioned in their report that the malware is becoming more complex, targeting desktops, and using multistage payload deployment. Some malwares even used 64-bit encoding to hide their malicious code and also techniques to disable their competing malware (Aquasec, 2021).

Literature Review on Methodology

Selecting the right cloud provider requires a lot of due diligence. Cloud users want to measure the security strength of cloud computing services which requires a model. Shaikh and

Sasijumar (2015) want to use the trust model to evaluate various components of cloud security. The trust model looks like an upside-down tree structure where multiple aspects of the cloud lead to a trust value (Shaikh & Sasikumar, 2015).

The parameters included in the paper are broken into nine major components: Identity management, Authentication, Authorization, Data Protection, Confidentiality, Communication, Isolation, Virtualization, Compliance. The trust model assigns a weightage for each of the parameters according to its strength. The total sum calculates the cloud security. Shaikh and Sasikumar (2015) based this approach by breaking the parameter into sub-parameters, which are further divided into smaller parameters. The assigned values to each of the parameters, sub-parameter, and subcomponents values contribute to overall security strength. They further stated that making the trust model dynamic by taking the inputs from users' comments, feedback, specific attacks, and frequency is considered to update the trust model.

For the cloud environment, the trust model is used in the framework, including a cloud service manager, Trust model, Service log, and Web Research, which provide the weightage for the cloud trusting model.

The trust model's final part talks about implementation and testing the three parts: implantation of test, environment, and test validation. The results will be reviewed and analyzed for adequacy. I prefer this model because it works with new entrants or startup environments of the cloud—an organization willing to take a risk on a new organization without any brand reputation. The cloud user will be a more extensive organization trying to save cost. The cloud provider is a new startup building its core product. This model considers various parameters, but the results may vary as weights and sub parameters are dependent on the cloud user.

Furthermore, this model requires staff expertise to evaluate and test a highly time-consuming and costly process.

Halabi and Bellaiche (2017) presented a quantification process to measure the cloud security, which the cloud service providers can use to perform self-evaluation. Their report included various cloud computing security aspects like Cloud confidentiality, Integrity, availability, accountability, and compliance. Cloud security services are also included, like authentication and authorization.

Halabi and Bellaiche (2017) mainly discussed using the evaluation matrix using implementation metrics, effectiveness metrics, impact metrics. The evaluation matrix is designed specifically for a cloud service provider to self-evaluate, so most of the weights associated with starting with a nominal baseline of values will be updated by the cloud service provider. This process requires periodic testing and fine-tuning for self-evaluation.

A paper entitled *A Security Framework for Secure Cloud Computing Environments* by Jouini and Rabai (2019) provided a methodology to solve security problems using a quantitative security risk model named multi-dimensional mean failure cost (M2FC). The model formula was designed based on a hierarchical linear system that consists of stakeholders, security requirements, and two perspectives. The framework introduced security issues into the cloud computing environment and analyzes the relation between security issues and their solution. The framework consisted of four main security steps: mapping security issues to problems, mapping security threat dimensions to systems requirements, and mapping threats to dimension elements and mitigation (Jouini & Rabai, 2019).

A paper by Luna, Taha, Trapero, and Suri (2015) entitled *Quantitative Reasoning About Cloud Security Using Service Level Agreements* focused on the security level agreement in the cloud for the quantitative assessment of cloud security SLA (SecSLA). This quantitative assessment consists of quantitative policy trees (QPT) and quantitative hierarchy process (QHP). The approach focuses on mapping the security requirements and security SLA work by assigning the quantitative weightage. The weights are adjusted based on refining the requirements, which helps in maximizing the Security SLA of the cloud services (Luna et al., 2015).

The above papers' methodology reviews used different quantitative approaches to define a solution for unique security problems faced in-crowd. My analysis of these papers demonstrates that the research results are academically focused, and methodology can be implemented in very few areas. The corporate cloud service provider has access to experienced staff and resources to refine and maintain cloud security. The individual cloud consumer who uses the cloud for personal projects and small businesses will not perform these analysis procedures. Moreover, it shows a need for a simple process that increases the security awareness of new and individual cloud consumers who operate on low volume. This paper will follow a straightforward methodology to map security controls to cloud services that have high readability for the average novice cloud user and focus on increasing the cloud user's security awareness.

Summary

In this chapter, the reason for the need for security metrics the background information needed for the readers to understand the consequences and importance was discussed. Literature review regarding the security metrics and how they assist in decision making. NIST's definition of cloud computing and various actors involved in the cloud was briefly discussed. In the next

chapter, we will look into the actual methodology of how the three cloud service providers' security measures will be analyzed will be addressed.

Chapter III: Methodology

Introduction

Based on the literature, we can conclude that hacking was a significant cause of data breaches. The methodology followed in this paper is simple and includes two steps. We leverage the Cloud Security Alliance's top 20 security controls, which are focused on preventing 80% of the risk (Cloud Security Alliance, 2019). We list the top 20 controls and research the corresponding application or service provided by AWS, Azure, and Google Cloud.

Design of the Study

The data gathered is directly from the sources which are available on the cloud providers' website documents. The process starts with selecting a security control and reviewing what the control focuses on to identify if the cloud provider natively provides that service to the cloud user. For this study, we are not considering the applications provided by third-party vendors. This is because although there can be configuration and API support, this will also introduce third-party risk and one more attack vector. Due to this third-party risk, we are only considering native applications and services. The final table will include all the findings in a tabular form where "X" indicates the security control is present and "- "indicates the service is natively not available.

Hardware and Software Environment

For this research, a general computer system that is connected to the Internet will be used as we are going to implement and work on the cloud. For analysis and visual representation, Excel, Visio will be used. Microsoft Office Suite is used for documentation of the research paper.

The important part is to set up IT controls that are fully automated where the system automatically performs the necessary checks, which will assure that applications are secured in the cloud environment. The controls primarily differ based on the business purpose to securely transfer the data between the cloud consumer and cloud provider. There are some basic principles that guide us in this purpose.

Control Principles

1. Controls need to ensure all the transactions were processed and completed from start to end.
2. Control needs to ensure the correct data is processed within applications.
3. Control needs to verify under authenticate the right users have access to the appropriate system under applications.
4. Controls that need to verify the authorization of these authenticated users and the rights they have on these objects
5. Controls that validate the integrity of data coming from the source to application and the data that is sent from the application to the downstream data consumers
6. Controls that log the transactions and processes that occurred during these activities to ensure that there is enough data to audit for complaints and also in the event of an incident

Although there are different cloud security models, the level of controls depends on various security and service level agreements made between the organization and the cloud service provider. These agreements also providing detail on the responsibilities of each party in the cloud environment bought the cloud service provider, and the consumer can use these

controls to build if focused security model and customize it to address the risk applicable to the organization.

Control Domains

The Cloud Security Alliance (CSA) cloud control matrix (2017) divides these controls into multiple domains: Cloud User, Cloud Application, Cloud Integration, Cloud Data and Cloud Processes.

Cloud user is the first domain, and there are multiple use cases for the cloud user with various user access requirements that focus on the authentication and authorization of other cloud applications. This domain provides controls aimed at cloud user access control management, cloud authentication, and cloud authorization.

A cloud application is the second domain. There can be multiple applications within the cloud environment. These applications need to be secured within the cloud at the same time, need to ensure they are able to communicate with other applications and also the upstream and downstream systems. This domain focuses on controls that are aimed to secure the applications within the cloud.

Cloud integrations are the third domain that focuses on controls that are required to securely integrate the cloud provider applications from compromise to the cloud and also other applications that are present in different locations. This can be geographically dispersed on-premises locations also can be other cloud providers that the cloud consumer uses.

Cloud data is the fourth domain, which focuses on securing and regulating the critical data and predict the data. These controls need to ensure the data which is stored in the cloud is

securely stored according to the compliance requirements and also the organization's standards as the data in the cloud is the prime target for malicious actors.

Cloud processes this is the fifth domain. These controls are primarily focused on supporting the highly critical processes under applications usage is in the cloud. These controls ensure that the processes are in line with the risk management and also able to mitigate the risks.

Control Responsibility Framework Reference

The primary pillars of this research paper contain the review of 20 controls which are identified by the cloud security alliance as the top 20 critical controls a cloud consumer needs to evaluate before migrating these applications and services into the cloud environment to provide an A-frame of reference for the reader we briefly describe the main sections for each control that is included. So, each control will include the domain that the control is assigned to and a unique control ID which segregates the control and provides an identification, description of the control itself, and how it should be addressed. The object that this control tries to address various threats and risks this control helps us to mitigate and additional information that can provide key insights

Depending on the cloud responsibility model, some of these controls can be assigned to the cloud provider, and some can be assigned to the cloud consumer sometimes, these responsibilities are a shared model, so once we determine the responsibilities of the cloud consumer, they should draft the cloud responsibility document on reviewing the controls and add weather to implement the control cost of control and the team that will be owning the control for the organization. Data will be provided in the following table format for each control.

Table 1

The Sample Table Format for Each Control

	AWS	AZURE	GCP
Control Present (X)	X	X	-
Tool Name	AWS IAM	Azure IAM	Not Available

Summary

We have reviewed the methodology implemented in this paper. The cloud security controls will be mapped against the cloud services in a table for convenient review of services. This methodology shows what other cloud services are offering for the same control.

Chapter IV: Implementation

Introduction

In this chapter we will review the top 20 cloud security controls explaining in brief, each control. Reviewing the controls against services of cloud providers. We will mention that below in detail and name the control in the related table.

Control ID: USR01 - Secure Authentication

The first control secure authentication is part of the domain cloud users. This control is focused on cloud users. The cloud users were accessing the cloud environment in order to gain access to the applications under the system. Users need to authenticate the user identity to gain access and must ensure that there are secure encryption protocols in order to securely authenticate the user. These secure tunnels use multifactor authentication to mitigate the risk and also to achieve the controls' objective. Building this control within the cloud will fall under the responsibility of the cloud consumer, which is dependent on their secure service model.

Cloud consumers can review various authentication and authorization tools provided by the cloud service provider to authenticate the identity of the users and also to securely set up the authentication protocol that is up to the industry standard. This can be secured by encrypting the login process using encryption, which prevents session hijacking man in the middle attack, which is a common attack while collecting the users do a cloud service. This control should also use a single sign-on centralized authentication system like SAML 2.0. Also, a two-step verification like multifactor authentication whenever there is additional risk and should trigger challenges at the user, based on the risk profile. The user interface also needs to have secure

processing mechanisms and needs to be constantly updated to mitigate interface vulnerabilities like ensuring a particular browser best login like Chrome, Explorer under version number.

Cloud user control mitigates access to unauthorized users, which is a primary threat. This is critical as most prominent attacks are executed using stolen credentials, session hijacking, dictionary-based attacks, Social engineering.

AWS provides the cloud user with secure authentication options along with AWS Command-line interface and Multifactor authentication for cloud applications AWS has AWS Cognito, which provides secure authentication to cloud users (Amazon Web Services, n.d.).

Azure provides Azure Active Directory, which has both single sign-on and multifactor authentication capability. This Azure active directory can integrate with Microsoft products and is capable of the technology stack (Microsoft, 2020a).

Google Cloud platform has enterprise grade Identity platform, which is used for secure access to the application and Google Cloud (Google Cloud, n.d.).

Table 2

USR01 - Secure Authentication

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Cognito	Azure Active Directory	Identity Platform

Control ID: USR02 - User Accounts Management

The cloud user accounts management control also comes under the cloud user domain. Many of these applications which are present in the cloud are accessed by multiple users from multiple teams within the organization. Most of these users might be located in different

geographical locations and can be working in different time zones. These user accounts can be abused, and malicious attackers can gain access to the applications through these accounts, so to manage the user account process, we need to have a control that can monitor the user accounts. This is critical because there are various changes in the user account lifecycle. An account is created for the corporate user when user joins an organization during onboarding, and sometimes this user can change his role within the organization and also can leave the organization, during which, if not properly monitored, these orphan accounts can be a critical vulnerability.

This control ensures that there are sufficient user access management mechanisms and processes that is compliant with user lifecycle. Starts with "User-ID" creation by provisioning an account for access where the employee joins the organization and revokes the access by de-provisioning when the employee leaves the organization.

To ensure this, the control focus on access reviews and periodical account audits, which will strengthen the effectiveness of the cloud control. This controls the primary objective to ensure that the accounts are not abused by the malicious actors to gain access to the enterprise data. The mechanisms that would help this control to be effective by creating a user access management, access authorization process with periodical access reviews and accurate access revocation.

AWS provides the cloud user with AWS IAM and Access Management, which provides the cloud customers with user access control management. This provides granular control of user access like providing temporary credentials, password reset (Amazon Web Services, n.d.).

Azure provides Azure Active Directory, External Identities, provides organizations with capabilities to manage users including external users, customers, partners. This helps organizations to have control over user accounts management (Azure, 2020).

Google provides cloud customers with the Cloud Identity tool, which provides capabilities to manage user identities, devices, and applications (Google Cloud, n.d.).

Table 3

USR02 – User Accounts Management

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS IAM and Access Management	Azure Active Directory External Identities	Cloud Identity

Control ID: USR03 - Role-Based Access Control

This role-based access control management is focused on managing user roles and privileges. These controls can be used across different users in an enterprise where the count of users is in thousands. and this kind of control also provides fine-grained access control and user access allocation process for both technical and non-technical activities. Role-Based Access Control also ensures that segregation of duties is implemented in a safe and secure manner in order to prevent any unauthorized intentional or unintentional use of data and applications.

The fine-grained access control and shows that the user roles or the system roles have the minimum permissions required to complete the task by that particular user in order to avoid Toxic combinations. All these recent roles should be periodically reviewed and updated according to the job duties and responsibilities to ensure additional permissions were not

included in the role. Regardless the responsibility will always be with the cloud customer while providing the authorizations for the user.

AWS provides the cloud user with secure authentication options along with AWS Command-line interface and Multifactor authentication for cloud applications. AWS has AWS Cognito, which provides secure authentication to cloud users (Amazon Web Services, n.d.).

Azure provides Azure Active Directory, which has both single sign-on and multifactor authentication capability. This Azure active directory can integrate with Microsoft products and is capable of the aligning with technology stack (Azure, 2020).

Google Cloud platform has enterprise grade Identity platform, which is used for secure access to the application and Google Cloud (Google Cloud, n.d.).

Table 4

USR03 – Role-Based Access Control

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Cognito	Azure Active Directory	Identity Platform

Control ID: USR04 - Emergency Access

This control comes under the domain of cloud users and is widely used in risk management operations of an organization. In an organization, during the day-to-day operations risk team will encounter multiple incidents and events and failures. These incidents are failure events at a higher risk for an organization, which can have a huge impact on operations and business.

During emergencies and the incidents, the users need to have access to the production level systems with elevated privileges in order to identify the root cause of the issue and resolve issue. Solution needs to be implemented within a short span of time to avoid for loss or risk of impact on business. The request for emergency access should have a process defined. Process should capture why the emergency access is requested the duration of time the access. This request will be available for the user and approvals required to grant the user the emergency access. These events need to be logged and audited in order to present to the compliance team that's sufficient measures are probably available to accurately maintain the control. During this process if any exceptions are made and performed that are not in line with the standard operating procedure already information sector standards they should also be reviewed and added to the emergency access process. Management reviews the emergency access reports periodically to ensure that there is not any abuse or deviation from the standard provisions provided with the emergency access.

Most organizations use Firecall ID. Fire call ID is an emergency id that can be assigned to any user temporarily with the ability to resolve the issue and implement changes. Firecall IDs have a span of 24 hours or a lesser short time frame like three or four hours depending on the criticality the ID exposes. There should be stringent monitoring of privilege Firecall IDs as these ID's have higher privileges and most sought after by the malicious attackers. This control mitigates that risk which emerges while granting access to emergency authorizations and approvals for our activities. It also ensures that this emergency access is terminated once its requirement is completed with the operations team.

AWS provides the cloud user with secure authentication options along with Emergency access capabilities through Firecall IDs (Amazon Web Services, n.d.).

Azure provides Azure Active Directory, which provides emergency access for cloud customers (Azure, 2020).

Google Cloud platform has enterprise-grade Identity platform, which is used for secure access to the application and Google Cloud (Google Cloud, n.d.).

Table 5

USR04 – Emergency Access

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Cognito	Azure Active Directory	Identity Platform

Control ID: USR05 - Segregation of Duties

This control ID is also under the domain of cloud users focusing on the Separation of duties. Separation of duties is one of the cloud control principles where prevent a toxic combination happening with newer access and authentication systems implementation. A toxic combination is where a person has authorization to perform multiple tasks within an organization which can allow abuse or malicious acts and increases the risk of abuse from inside. It also tries to prevent the fraud that can take place when internal employee turns rogue and intentionally sabotage applications. To prevent this organizations, use separation of duties metrics, which identifies different permissions that a user has and eliminates the toxic combination. This toxic combination is used by both access management reviews and internal and external auditors to verify that organization is implementing the separation of duties principle and least privilege.

There are some applications which automatically detect separation of duties violation within an application or organization. The responsibility of maintaining separation of duties falls under the application owner and also the access control personal.

AWS provides the cloud users with fine-grained access control capabilities where customers can create users' roles that are aligned with the Separation of duties principle (Amazon Web Services (n.d.).

Azure provides Azure Active Directory, which has the ability to define roles that are segregated and are based on the Separation of duties. This Azure active directory can integrate with Microsoft products and is capable of the technology stack (Azure, 2020).

Google Cloud platform has enterprise grade identity platform, which is used for separation of duties and defining roles, and maintaining roles, so that separation of duties principle is maintained (Google Cloud, n.d.).

Table 6

USR05 – Segregation of Duties

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Cognito	Azure Active Directory	Identity Platform

Control ID: USR06 - Secure User Provisioning and De-provisioning

This control also falls under the cloud domain Cloud users. The user account should be thoroughly reviewed to ensure that there is always an actual user assigned to the account. The user account life cycle starts with human resources during onboarding, starting with the employer ID number. This employee ID number will be the primary key that will link to all

applications until bound with the user account details. The user account provisioning should follow entitlements based on the rule the user performs within an application. The user access account lifecycle should also have options for de-provisioning the user from applications across multiple access layers. Periodic user access review is required to ensure that the user account lifecycle is managed effectively.

There should be a defined process for privileged account management to ensure there is no abuse of unmanaged accounts to elevate permissions to critical application access.

AWS provides the cloud user with AWS IAM and Access Management, which provides the cloud customers with secure user provisioning and de-provisioning, which provides granular control of user access, providing temporary credentials, provides access analysis (Amazon Web Services, n.d.).

Azure provides Azure Active Directory External Identities provides organizations with capabilities to manage users and including external users, customers, partners. This helps organizations to have control over user accounts management (Azure, 2020).

Google provides cloud customers with the Cloud Identity tool, which provides capabilities to manage user identities, devices, and applications (Google Cloud, n.d.).

Table 7

USR06 – Secure User Provisioning and De-Provisioning

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS IAM and Access Management	Azure Active Directory External Identities	Cloud Identity

Control ID: USR07 - ERP Account Security

Security of enterprise accounts is highly critical especially when you're migrating these applications to the cloud environment there should be a detailed procedure for login process, which makes it harder for an attacker to gain access to the ERP system using valid credentials. Additionally, there are many mechanisms that restrict the usage like session management mechanisms, application access standards. Organizations also need to ensure a complex password policy is assigned along with multifactor authentication. Process involves analyzing the user entity behavior based on user login location, time zone, IP address and also to ensure single sign-on is used across applications. For logging and security there need to be certain access restrictions based on the critical systems and specific networks maintaining and managing the session tokens in a random dynamic encrypted environment. The responsibility of this control lies with the cloud consumer completely, to specify the accounts required to manage the cloud environment by reviewing the roles and entitlements required.

AWS provides the cloud user with Account security by providing AWS Account Security Features, which provides users with AWS credentials, AWS MFA (Multi Factor Authentication), Access Keys, Key Pairs, X.509 Certificates (Amazon Web Services, n.d.).

Azure provides Azure Security Center, which provides cloud customers with tools and resources to secure the accounts and also monitor the accounts (Azure, 2020).

Google provides cloud customers with the Cloud Identity tool, which provides capabilities to manage user identities, devices, and applications. Cloud Identity provides the account security features (Google Cloud, n.d.).

Table 8

USR07 – ERP Account Security

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Account Security	Azure Security Center	Cloud Identity

Control ID: APP01 - Secure Landscape

The control ID cloud secure landscape focuses on the requirements needed to secure the cloud environment. Due to complexity in the multi-tier cloud environment, many of these applications are deployed based on different layers like the development layer, testing layer, production layer, on-premises network, and cloud environment.

Securing landscape focuses on secure settings, Separating the interfaces and access layers. These secure practices could define the integrity of security in production environments. This control focuses on mechanisms that prevent unauthorized access risk and ensure entitlements are clearly defined. Restrict users from accessing the operating system by controlling system access. This control also ensures that a similar level of security has been configured across all environments to prevent unauthorized escalation of entitlements and privileges in the cloud system regardless of the contract the responsibility of managing this control duty of cloud customer.

AWS provides the cloud user with account security by providing AWS Account Security Features, which provides users with AWS credentials, AWS MFA, Access Keys, Key Pairs, X.509 Certificates (Amazon Web Services, n.d.).

Azure provides Azure Security Center, which provides cloud customers with tools and resources to secure the accounts and also monitor the accounts (Azure, 2020).

Google provides cloud customers with the Cloud Identity tool, which provides capabilities to manage user identities, devices, and applications. Cloud Identity provides the account security features (Google Cloud, n.d.).

Table 9

APP01 – Secure Landscape

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Account Security	Azure Security Center	Cloud Identity

Control ID: APP02 - Baseline Secure Configurations

The control baseline secure configuration is also under the domain of cloud users. Configuration is one of the main risks. Incorrectly configured cloud systems can expose different attack vectors for the hackers, so to prevent this from happening, this control focuses on observing different layers of secure configurations. The cloud customer decides the secret configuration that is required for each control that makes this cloud system secure. These baseline security configurations need to be thoroughly reviewed and documented for the application owners and auditors to review them. Secure configurations also assist in early detection of unauthorized access. For the security administrators the main objective is to assign an application layer secure configuration which coincides with industries baseline.

AWS provides the cloud user with baseline security configurations by providing AWS Account Security Features, which provides users with AWS credentials, AWS MFA, Access Keys, Key Pairs, X.509 Certificates (Amazon Web Services, n.d.).

Azure provides Azure Security Center, which provides cloud customers with tools and resources to secure the accounts and also monitor the accounts (Azure, 2020).

Google provides cloud customers with the Cloud Identity tool, which provides capabilities to manage user identities, devices, and applications. Cloud Identity provides the account security features (Google Cloud, n.d.).

Table 10

APP02 – Baseline Secure Configurations

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Account Security	Azure Security Center	Cloud Identity

Control ID: APP03 - Security Vulnerabilities

The control security vulnerability is also under the domain of cloud users which focuses on the enterprise control processes, which assist the organization to detect secret vulnerabilities and risks that impact the applications. These vulnerabilities need to be documented with an impact risk and priority so that the mitigation activities for these vulnerabilities are in top priority of the organization. Cloud customers will perform management tasks using security tools that actively monitor, scan, and test the applications. Documentation should also have an incident management team who are focused on incident response and incident remediation efficiently. It is possible to maintain this control with a vulnerability assessment process and administrators

who remediate the vulnerabilities in a timely manner. The main difference in this comes with software as a service model where the responsibility falls under cloud service provider.

AWS provides the cloud user with Amazon Inspector application to scan for vulnerabilities in the cloud environment and cloud instances. This provides the user the capability to scan the cloud assets for vulnerability (Amazon Web Services, n.d.).

Azure provides cloud users with Azure defender, which is helpful in scanning and providing vulnerability assessment for cloud instances (Azure, 2020).

Google provide a security vulnerability tool automatic vulnerability scanning. This has both pros and cons where google service might be more large enterprise focused (Google Cloud, n.d.).

Table 11

APP03 – Security Vulnerabilities

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	Aws Amazon Inspector	Azure Defender Vulnerability Assessment	Automatic Vulnerability Scanning

Control ID: APP04 - Secure Communications

These secure control communications focus on the cloud users and how they connect into the cloud based on the protocols. Defining the channels that the protocols use and services for security. Most of these application access channels need to be encrypted to protect the organization from unauthorized access to sensitive data. Communications need to be secured based on the prevalent industry standards security frameworks. The cloud customer is always responsible for who is accessing the cloud system and implementing the secure communication

is the responsibility of the cloud user. This process ensures all the upstream and downstream applications transfer data securely using the protocols. This control prevents many attacks like the man in the middle attack, sniping data extraction and session hijacking

AWS provides the cloud user with Amazon secure configuration tools, which adds VPN and encryption to enable secure data communications (Amazon Web Services, n.d.).

Azure provides cloud users with an Azure security center, which is helpful in providing secure communications (Azure, 2020).

Google provides secure communication by providing transfer layer security and encrypted connection options to Google Cloud systems (Google Cloud, n.d.).

Table 12

APP04 – Secure Communications

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Amazon Security	Azure Security Center	Google Security

Control ID: APP05 - Change Management Controls

This control focuses on the change management process that the organization is using to implement the changes within the cloud environment. As the cloud is highly scalable and dynamic, the change management process would be defined with proper controls and approvals processes. This will ensure that there is least disruption to the organizational, operational activities. This control also ensures prevention of misconfiguration in cloud systems. Change management process requires the users to define all the activities that are performed, which are then being reviewed by the change management team and approved only when satisfied.

Amazon offers AWS Systems Manager-Change Manager tool for Change Management in the cloud (American Web Services, n.d.).

Azure provides cloud users with Azure Change Tracking & Inventory, which helps users with cloud change management (Azure, 2020).

Google provides GAPPS Change Management which is a change management tool for users using Google Cloud platform (Google Cloud, n.d.).

Table 13

APP05 – Change Management Controls

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Systems Manager Change Manager	Azure Change Tracking and Inventory	GAPPS Change Management

Control ID: APP06 - Secure Extensions

This control focus on securing the extensions of the application as many of these applications are expanded to support multiple organizational vendors and processes which might introduce additional risk for the organization. Organizations need to ensure the extensions which grant the vendors access to the systems. They should focus on the authentication of authorized users' permissions and also prevent injection attacks into the code to ensure that the new software patching the vulnerability does not add unauthorized code. This will provide unauthorized users the ability to add additional privileges so whenever there's a new code implementation being pushed into the production environment, the code should be reviewed by application security team to run static and dynamic code review and also the local source code review to prevent the introduction of novel vulnerabilities. This control ensures that any new

code introduced by the vendors is certainly reviewed so that it does not become a high-risk vulnerability for the organization.

AWS provides AWS Lambda Extensions, which helps users with connecting and securing extensions between different cloud and hybrid systems (American Web Services, n.d.).

Azure provides cloud users with Azure Virtual Machine Extension, which helps users with connecting and securing extensions between different cloud and hybrid systems (Azure, 2020).

Google provides Google Cloud extensions. This is an extension tool to support extensions (Google Cloud, n.d.).

Table 14

APP06 – Secure Extensions

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Lambda Extensions	Azure Virtual Machine Extension	Google Cloud Extensions

Control ID: INT01 - Secure Integrations and APIs

This secure integration and APIs control is focused on the integration of applications with external applications and data locations. A cloud system contains multiple interfaces and connections that connect to different applications and solutions and also different environments. If these applications are not securely integrated with the organization, this may allow unauthorized users to abuse and results in a data breach. This control primarily focuses on addressing the risks with the interfaces within the organization. Businesses need to document all the interfaces and the data contracts, the technical details of the collection's types, protocols,

authorizations, and the encryption details of these interfaces. This control also ensures that the organization avoids interfaces that are insecurely configured and also prevent broad and blind trust relationship.

Organizations use the least privilege principle to determine the access that the technical users need to perform their duties and also the interfaces they need to access. The control focuses on encrypting all the interfaces which use critical data and also ensures that there are no interfaces that are connecting the cloud system with a lower security application.

The secrets which are used to configure these interfaces, like API keys, password certificates, need to have a life cycle that is constantly changed as per the organization policy. As this is the responsibility of cloud customer

AWS provides AWS API and API Gateways to connect services with the cloud using APIs. This provides a secure API connection between different cloud and hybrid systems (American Web Services, n.d.).

Azure provides Azure API and API Gateways to connect services with the cloud using APIs. This provides a secure API connection between different cloud and hybrid systems (Azure, 2020).

Google provides Google API and API Gateways to connect services with the cloud using APIs. This provides a secure API connection between different cloud and hybrid systems (Google Cloud, n.d.).

Table 15

INT01 – Secure Integrations and APIs

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS API	Azure API	Google Cloud API

Control ID: DAT01 - Continuous Monitoring

At any point in time, there are multiple activities and operations that have constantly been running and occurring in the cloud systems. This may be the data coming into the system from different connections that are requested by users. System activity monitoring includes the performance of secure networks in detecting of privileged escalations system changes and various other risks. Primary tools that assist in maintaining control are the audit logs and reports of system logs, where all the events and transactions of these security logs will assist us in detecting unauthorized activity and also provide evidence for unauthorized changes that occur in the cloud system.

The audit logs implemented should be configured to capture critical transactions, potential unauthorized access abuse of secure configurations, data access egress, and ingress of data across the network.

AWS provides AWS Lambda Extensions, which helps users with connecting and securing extensions between different cloud and hybrid systems (American Web Services, n.d.).

Azure provides cloud users with Azure Virtual Machine Extension, which helps users with connecting and securing extensions between different cloud and hybrid systems (Azure, 2020).

Google provides Google Cloud extension tool which support integration with different third-party vendor applications (Google Cloud, n.d.).

Table 16

DAT01– Continuous Monitoring

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Lambda Extensions	Azure Virtual Machine Extension	Google Cloud Extensions

Control ID: DAT02 - Data Separation

Data is a highly important asset of enterprise applications. This data is primarily stored in the databases, and this database is the source for multiple users and applications which access the data. This control, which falls under the domain cloud data, ensures that data is stored separately in the cloud systems. This can be mentioned as the separation of production-level data and non-production-level data.

The data in these cloud systems need to be classified on priority, and the sensitivity and some data have additional regulations like personally identifiable information, which is why most financial organizations and healthcare organizations use this control. This control ensures that the production data is not available in a non-production level environment and non-production level data is not available in a production-level environment, so the databases that show this information in the cloud should be properly configured to maintain this distinction of data, and also the cloud customers should ensure that the separation of duties principle is followed for the users, so that no user has data access to both production level and non-production level data.

AWS does not have any tool to assist cloud customers with data separation in the cloud (American Web Services, n.d.).

Azure does not have any tool to assist cloud customers with data separation in the cloud (Azure, 2020).

Google does not have any tool to assist cloud customers with data separation in the cloud (Google Cloud, n.d.).

Table 17

DAT02– Data Separation

	AWS	AZURE	GCP
Control Present (X)	-	-	-
Tool Name	No Tool in AWS	No Tool in Azure	No Tool in Google

Control ID: DAT03 - Data Encryption

This control focuses on how the data is stored in a business system, both on-premises and cloud. The critical data must be encrypted at all stages. Both are addressed in transit and also during processing to avoid unauthorized access. This control also implements mechanisms like the need to have a different key for different data.

The control requests organization to document its data governance policies of what kind of data should be encrypted what data should not be encrypted based on the business use cases. The control recommends organization that the data should be encrypted in all stages. The user interface that accesses this data also needs to create a secure connection—introducing proper algorithmic ciphers, like usage of soft token and hard token certificates. Also need to ensure

proper policies are placed on reviewing the access life cycle by revoking, provisioning the access keys and certificates.

AWS provides multiple encryption tools for AWS Cloud HSM, AWS Key Management Service, AWS Encryption SDK, Amazon DynamoDB Encryption client AWS Secrets Manager (American Web Services, n.d.).

Azure client-side encryption, Server-side encryption, Azure Disk Encryption, Azure Storage Service Encryption (Azure, 2020).

Google client-side encryption, Server-side encryption Customer, supplied encryption keys, Customer Managed encryption keys (Google Cloud, n.d.).

Table 18

DAT03– Data Encryption

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Cloud HSM, AWS Key Management Service, AWS Encryption SDK, Amazon DynamoDB Encryption client AWS Secrets Manager	Client-side encryption, Server-side encryption, Azure Disk Encryption, Azure Storage Service Encryption	Client-side encryption, Server-side encryption Customer supplied encryption keys, Customer Managed encryption keys

Control ID: BUS01 - Inventory of Business Assets, Data, and Processes

This control focus on the primary applications that support the organization. The processes and applications are built on a much more complex layer like application servers' databases. These interfaces host numerous components which are populated in this cloud enterprise. To manage all business assets, there should be a process that takes care of managing and administrating these applications. Most of the organization generally use one component that is called CMDB configuration management database. This tool supports the organization goal of

managing inventories and business assets. Data that is stored and processed by the vendor solutions and products. All the technical components and applications on the servers that host these applications infrastructure like physical servers, virtual servers, physical database, virtual database, applications that execute this data, stored data, and classified data. This provides the organization an actual view of business assets and how they're managing them and also assist in the change management process.

AWS provides AWS Systems Manager Inventory, which helps cloud customers to inventory their cloud assets (American Web Services, n.d.).

Azure provides cloud customers with Security Control: Inventory and Asset Management (Azure, 2020).

Google provides cloud customers with cloud asset Inventory (Google Cloud, n.d.).

Table 19

BUS01– Inventory of Business Assets, Data, and Processes

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Systems Manager Inventory	Security Control: Inventory and Asset Management	Cloud Asset Inventory

Control ID: BUS02 - Business Process Controls

The business process control focuses on the critical operational process within the organization. This ensures that no unauthorized entity has access to business-critical applications, which can lead to an incident of a data breach, including fraud and corporate espionage organizations with the help of this control, implement business-level controls that prevent unauthorized activity and can also identify fraud and determine how this authorized

access has spread across applications it can also help in identifying the critical data and detect the access to this critical data. Some of this control's features focus on user access to these critical processes and how it is available to the applications.

AWS does not have any tool to assist cloud customers with data separation in the cloud (American Web Services, n.d.).

Azure does not have any tool to assist cloud customers with data separation in the cloud (Azure, 2020).

Google does not have any tool to assist cloud customers with data separation in the cloud (Google Cloud, n.d.).

Table 20

BUS02 - Business Process Controls

	AWS	AZURE	GCP
Control Present (X)	_	_	_
Tool Name	No Tool in AWS	No Tool in Azure	No Tool in Google Cloud

Control ID: BUS03 - Continuous Compliance

This control ensures that all the applications that the organization uses are in compliance with the industry requirements and various frameworks. Organizations are commonly subjected to regulations like Sarbanes-Oxley Act.

General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS). There are multiple regulations that the organization is subjected to. If the controls fail, it will lead to being non-compliant. This would result in hefty fines and a huge business impact.

This control ensures that the organization practices to identify relevant complaints regulations and identify which control should be implemented to achieve an audit approved, compliance accepted control. This requires rigorous monitoring and auditing of both internal and external applications that the organization connects, and also there should be a mechanism that focuses on regularly identifying these complaints violations and notifying the application or the asset owners to resolve these issues and making them compliant again.

AWS Config Rules provides cloud customers with continuous compliance in AWS (American Web Services, n.d.).

Azure Policy Provides users with continuous compliance of Azure cloud assets (Azure, 2020).

Google Compliance Center provides cloud customers with continuous compliance with Google Cloud assets (Google Cloud, n.d.).

Table 21

BUS03 - Continuous Compliance

	AWS	AZURE	GCP
Control Present (X)	X	X	X
Tool Name	AWS Config Rules	Azure Policy	Google Compliance Center

Table 22

Review of Top 20 Cloud Security Controls against AWS-Azure-Google

Control	AWS	Azure	Google
USR01- Secure Authentication	X	X	X
USR02 – User Accounts Management	X	X	X
USR03 – Role-Based Access Control	X	X	X
USR04 – Emergency Access	X	X	X
USR05 – Segregation of Duties	X	X	X
USR06 – Secure User Provisioning/Deprovisioning	X	X	X
USR07- ERP Accounts Security	X	X	X
APP01-Secure Landscape	X	X	X
APP02 – Secure Baseline Configurations	X	X	X
APP03- Security Vulnerabilities	X	X	X
APP04- Secure Communications	X	X	X
APP05- Change Management Controls	X	X	X
APP06- Secure ERP Extensions	X	X	X
INT01-Secure Integrations and Application Programming Interfaces (APIs)	X	X	X
DAT01- Continuous ERP Monitoring	X	X	X
DAT02- Data Separation	_	_	_
DAT03- Data Encryption	X	X	X
BUS01-Inventory of Business Assets, Data, and Processes	X	X	X
BUS02- Business Process Controls	_	_	_
BUS03- Continuous Compliance	X	X	X

Table 23

Security Tools Review of Top 20 Cloud Security Controls against AWS-Azure-Google

Control	AWS	Azure	Google
USR01- Secure Authentication	AWS Cognito	Azure Active Directory	Identity Platform
USR02 – User Accounts Management	AWS IAM and Access Management	Azure Active Directory External Identities	Cloud Identity
USR03 – Role-Based Access Control	AWS Cognito	Azure Active Directory	Identity Platform
USR04 – Emergency Access	AWS Cognito	Azure Active Directory	Identity Platform
USR05 – Segregation of Duties	AWS Cognito	Azure Active Directory	Identity Platform
USR06 – Secure User Provisioning/Deprovisioning	AWS IAM and Access Management	Azure Active Directory External Identities	Cloud Identity
USR07- ERP Accounts Security	AWS Account Security	Azure Security Center	Cloud Identity
APP01-Secure Landscape	AWS Account Security	Azure Security Center	Cloud Identity
APP02 – Secure Baseline Configurations	AWS Account Security	Azure Security Center	Cloud Identity
APP03- Security Vulnerabilities	AWS Amazon Inspector	Azure Defender Vulnerability assessment	Automatic Vulnerability Scanning
APP04- Secure Communications	AWS Amazon Security	Azure Security Center	Google Security
APP05- Change Management Controls	AWS Systems Manager Change Manager	Azure Change Tracking & Inventory	GAPPS Change Management
APP06- Secure ERP Extensions	AWS Lambda Extensions	Azure Virtual Machine Extension	Google Cloud Extensions
INT01-Secure Integrations and Application Programming Interfaces (APIs)	AWS API	Azure API	Google Cloud API
DAT01- Continuous ERP Monitoring	AWS Lambda Extensions	Azure Virtual Machine Extension	Google Cloud Extensions

Table 23 Continued

Control	AWS	Azure	Google
DAT02- Data Separation	No Tool in AWS	No Tool in Azure	No Tool in Google Cloud
DAT03- Data Encryption	AWS Cloud HSM, AWS Key Management Service, AWS Encryption SDK, Amazon DynamoDB Encryption client AWS Secrets Manager	client-side encryption, Server-side encryption, Azure Disk Encryption, Azure Storage Service Encryption	client-side encryption, Server-side encryption Customer supplied encryption keys, Customer Managed encryption keys
BUS01-Inventory of Business Assets, Data, and Processes	AWS Systems Manager Inventory	Security Control: Inventory and Asset Management	Cloud Asset Inventory
BUS02- Business Process Controls	No Tool in AWS	No Tool in Azure	No Tool in Google Cloud
BUS03- Continuous Compliance	AWS Config Rules	Azure Policy	Google Compliance Center

Chapter V: Conclusion

Cloud service providers are adding new services to attract more cloud users. After mapping the cloud services with security controls, we can observe all three providers have services that support cloud security controls. After reviewing the documentation for the services, this paper provides a high-level overview for the cloud user on the security controls. They can review cloud security controls and what corresponding services that can implement those controls.

One observation that I would like to make in relation to this paper is although there are multiple services and cloud providers, the major challenge would be the configuration of security controls accordingly. Most of these services have extensive documentation and a learning curve, due to which it is easy to misconfigure the security controls, which can lead to a cloud security breach.

Future work should focus on cloud security with a single control in focus and analyze the security controls in-depth in the cloud to ensure if the actual tool or application works as intended or mentioned by the cloud service provider. The challenges of customization and configuration of security controls. Cost of each security control to implement in the cloud.

I would suggest the user use this paper as baseline information of security controls and review the cloud services documentation for further research.

References

Adler, S. (2015). *Data breach sparks medical informatics engineering lawsuit*. http://www.hipaajournal.com/data-breach-medical-informatics-engineering-lawsuit-8054/

Alder, S. (2020). *2020 saw a major increase in healthcare hacking incidents and insider breaches*. https://www.hipaajournal.com/2020-saw-major-increase-in-healthcare-hacking-incidents-and-insider-breaches/

Amazon Web Services. (n.d.). *AWS documentation*. https://docs.aws.amazon.com/index.html

Aquasec. (2021). *Cloud native threat report: Attacks in the wild on container infrastructure*. https://info.aquasec.com/cloud-native-threats

Azure. (2020). *Microsoft azure documentation*. https://docs.microsoft.com/en-us/azure/?product=featured

Brandel, M. (2011). *Lessons in security leadership: David Komendat*. https://www.csoonline.com/article/2129299/lessons-in-security-leadership--david-komendat.html

Cloud Security Alliance. (2017). *Cloud controls matrix*. https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview

Cloud Security Alliance. (2019). *Top 20 critical controls for cloud ERP customers*. https://cloudsecurityalliance.org/artifacts/top-20-critical-controls-for-cloud-erp-customers/

DataBreaches.net. (2011). *HHC press release on backup tapes stolen from GRM van*. https://www.databreaches.net/hhc-press-release-on-backup-tapes-stolen-from-grm-van/

European Network and Information Security Agency (ENISA). (2012). *Cloud computing: Benefits, risks, and recommendations for information security*. https://cloud-computing-benefits-risks-and-recommendations-for-information-security (europa.eu)

Gartner Research. (2020). *Gartner Research, 2020 magic quadrant for cloud infrastructure and platform services*. https://www.Gartner Research, 2020.com/en/documents/3989743/magic-quadrant-for-cloud-infrastructure-and-platform-ser

Google Cloud. (n.d.). *Google Cloud platform documentation*. https://cloud.google.com/docs/

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of cloud service providers. *Journal of Information Security and Applications, 33*, 55-65. http://dx.doi.org/10.1016/j.jisa.2017.01.007

Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. *Cloud Security: Concepts, Methodologies, Tools, and Applications*, pp. 249-263. IGI Global. https://doi.org/10.4018/978-1-5225-8176-5.ch011

Kern. C. (2015). *Excellus data breach undetected for nearly two years*. https://www.healthitoutcomes.com/doc/excellus-data-breach-undetected-nearly-two-years-0001

Knippa, P. (2014). *What healthcare can learn from CHS data breach*. http://www.informationweek.com/healthcare/security-and-privacy/what-healthcare-canlearn-from-chs-data-breach/a/d-id/1317696

Krebs, C. (2015). *Premera Blue Cross breach exposes financial, medical records*. https://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/

Luna, J., Taha, A., Trapero, R., & Suri, N. (2015). Quantitative reasoning about cloud security using service level agreements. *IEEE Transactions on Cloud Computing, 5*(3), 457-471.

McCann, E. (2013). *Programming error causes Indiana data breach*. http://www.healthcareitnews.com/news/programming-error-causes-indiana-data-breach

McGee, M. K. (2016). *L.A. County: Major breach stemmed from phishing attack*. http://www.bankinfosecurity.com/la-county-major-breach-stemmed-from-phishing-attack-a-9595

Microsoft. (2020a). *Azure active directory documentation*. https://docs.microsoft.com/en-us/azure/active-directory/

Microsoft. (2020b). *Microsoft digital defense report*. https://www.microsoft.com/en-us/security/business/security-intelligence-report

Modern Healthcare. (2016). *Banner Health cyberattack impacts 3.7 million people*. http://www.modernhealthcare.com/article/20160803/NEWS/160809954

National Institute of Standards and Technology (NIST). (2011). *The NIST definition of cloud computing*. (NIST Publication 800-145). https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

Ponemon Institute. (2015). 2014: *A year of mega breaches*. http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

Ragan, S. (2015). *How does a breach like Anthem happen?* http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html

Sanhotra, R. (2020). *The state of cloud security 2020*. https://news.sophos.com/en-us/2020/08/07/the-state-of-cloud-security-2020/

SANS Institute. (2017). *SANS glossary of terms used in security and intrusion detection*. http://www.sans.org/resources/glossary.php

Shaikh, R., & Sasikumar, M. (2015). Trust model for measuring security strength of cloud computing service. *Procedia Computer Science, 45,* 380-389.

Snell, E. (2016). *Health data security not compromised in Newkirk data breach*. http://healthitsecurity.com/news/health-data-security-not-compromised-in-newkirk-data-breach

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems.* (National Institute of Standards and Technology Special Publication 800-30). https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01

Trustwave. (2020). *2020 Trustwave global security report*. https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

UCLA. (2015). *UCLA faces lawsuit after health data breach*. http://healthitsecurity.com/news/ucla-faces-lawsuit-after-health-data-breach

Valley Anesthesiology and Pain Consultants. (2016). *Valley Anesthesiology and Pain Consultants identifies and addresses information security incident*. http://www.prnewswire.com/news-releases/valley-anesthesiology-and-pain-consultants-identifies-and-addresses-information-security-incident-300312986.html

Vaughn, R. B., Henning, R., & Siraj. A. (2003). *Information assurance measures and metrics: State of practice and proposed taxonomy*. Proceedings of the Big Island, HI, USA, 2003, p. 10. doi: 10.1109/HICSS.2003.1174904. https://ieeexplore.ieee.org/document/1174904

Winton, R. (2013). Laptop thefts compromise 729,000 hospital patient files. *Los Angeles Times*. http://articles.latimes.com/2013/oct/21/local/la-me-hospital-theft-20131022

Xerox. (2014). Xerox reported for 2 million record HIPAA breach by Texas HHSC. http://www.hipaajournal.com/xerox-reported-for-2-million-hipaa-breach-texas-hhsc/