Accedere

SOC Reports for Cloud Security and Privacy

Disclaimer

This publication contains general information only and Accedere is not, through this publication, rendering any professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Accedere shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Accedere" means Accedere Inc. Please visit https://accedere.io and email us at info@accedere.io for any specific services that you may be looking for.

Accedere Inc is a Colorado licensed CPA Firm listed with PCAOB. and Cloud Security Alliance as Auditors. Restrictions on specific services may apply.

Table of Contents

01

Introduction

Cloud adoption has increased by leaps and bounds adding to the already increasing cyber risks. Cost of doing business in the digital age is rising. Cloud service abuse rank among the greatest cyber security threats. To illustrate the potential magnitude of this threat, in a recent incident described how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't 4necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get not just that client's data, but every other clients' data as well.

Cyber Security Trends

Cost of Doing Business in the Digital Age

$10.5T

Expected Size Of Cyber Crime Market by 2025

$3.86M

Average Total Cost of a Data Breach

280 Days

Average time to identify and contain a breach

Cyber Attacks Remain Top Business Risk

The challenge in addressing this threat of data loss and data leakage is that "the measures you put in place to mitigate one can exacerbate the other". You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data. However, if you opt to keep offline backups of your data to reduce data loss, you increase your exposure to data breaches.

> **Data Security and Privacy are increasing challenges in today's Cloud based environments.**

Providing an independent third-party assurance such as a SOC 2 report helps address these concerns and helps Cloud Service Providers (CSP) stay above the competition.

02

Increasing Cloud Factor

93% of enterprises already have a multi-cloud strategy

19,188 SaaS Companies

$134B In Funding

A Crozdesk report on Global Cloud Start-up Clusters 2017 indicated that there were 19,188 Cloud Service Providers with $134B in funding.

"As cloud becomes increasingly mainstream through 2022, it will dominate ever-increasing portions of enterprise IT decisions."

https://crozdesk.com/software-research/saas-and-cloud-startup-report-2018/

Cloud shift represents both risk and opportunity. As cloud becomes increasingly mainstream through 2022, it will dominate ever-increasing portions of enterprise IT decisions (including, in particular, system infrastructure).

https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/

$1T cloud services market size expected by 2024- IDC

https://www.idc.com/getdoc.jsp?containerId=prUS46934120

$141B SaaS market size by 2022*

https://www.bmc.com/blogs/saas-growth-trends/

03

Cloud Challenges

01 Cloud services can provide organizations, including federal agencies, with the opportunity to increase the flexibility, availability, resiliency, and scalability of cloud services, which the organizations can, in turn, use to increase security, privacy, efficiency, responsiveness, innovation, and competitiveness. However, many organizations, especially those in regulated sectors like finance and healthcare, face additional security and privacy challenges when adopting cloud services.

02 Cloud platform hardware and software are evolving to take advantage of the latest hardware and software features, and there are hundreds or thousands of virtualized or containerized workloads that are spun up, scaled out, moved around, and shut down at any instant, based on business requirements. In such environments, organizations want to be able to monitor, track, apply, and enforce policies on the workloads, based on business requirements, in a consistent, repeatable, and automated way.

03 This is further complicated by organizations' need to comply with security and privacy laws applicable to the information that they collect, transmit, or hold, which may change depending on whose information it is (e.g., European's citizens under the General Data Protection Regulation), what kind of information it is (e.g., health information compared to financial information), and in what state or country the information is located. Additionally, an organization must be able to meet its own policies by implementing appropriate controls dictated by its risk-based decisions about the necessary security and privacy of its information.

04 Because laws in one location may conflict with an organization's policies or mandates (e.g., laws, regulations), an organization may decide that it needs to restrict the type of cloud servers it uses, based on the state or country. Thus, the core impediments to broader adoption of cloud technologies are the abilities of an organization to protect its information and virtual assets in the cloud, and to have sufficient visibility into that information so that it can conduct oversight and ensure that it and its CSP's are complying with applicable laws and business practices.

> **“In other words, organizations want to maintain consistent security protections and to have visibility and control for their workloads across on-premises private clouds and third-party hybrid/public clouds in order to meet their security and compliance requirements.”**

In addition, there are technical challenges and architectural decisions that have to be made when connecting two disparate clouds. An important consideration revolves around the type of wide area network connecting the on-premises private cloud and the hybrid/public cloud, because it may impact the latency of the workloads and the security posture of the management plane across the two infrastructures.

(Source NIST).

Misconfigured Cloud Servers

"According to a Symantec report, in 2018 nearly 70 million records were stolen or leaked due to misconfigured cloud storage buckets."

"Attackers are suspected to be having tools that allow them to detect misconfigured cloud storage to target ".

(Source Towards Data Science Inc.)

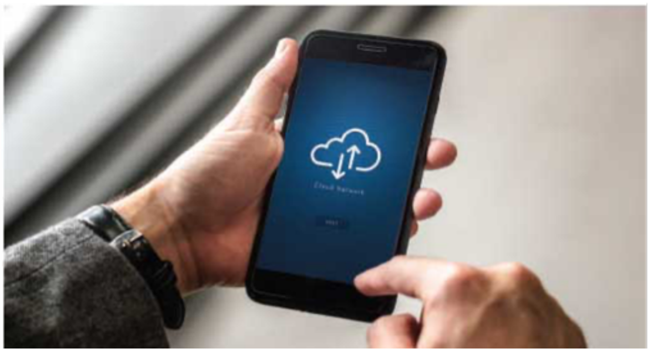
Organizations should check and monitor settings on cloud service architecture—do not maintain default settings. Vet third-party cloud vendors for high security standards before choosing to do business with them. Ensure you are aware of who controls each component of your cloud infrastructure and define policies for where and how security measures are deployed. Implement the same security policies you would employ for classic IT infrastructure.

(Source IBM 2018 Report).

Vendor (Third-party) Risks

From a cybersecurity perspective, third party risks frequently involve a set of threats that may exceed the scope of the organization's risk management activities. Some organizations focus too narrowly on risks. For example, when hosting data in the cloud, most organizations ask the vendor for attestations or some evidence of cybersecurity capability.

(Source Software Engineering Institute).



Breaches And Regulations Make Vendor Risk A Priority

Vendor-related Data Breaches On The Rise

63% **Of all data breaches can be linked directly or indirectlyto third parties**
- Soha Systems

Don't believe vendors would notify them of a data breach **37%**

(Source Ponemon Institute LLC).

Regulatory Liability Has Shifted

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of the subjects protected.

(Source Cloud Security Alliance).

IoT And Cloud

Connected devices and cyber-physical systems are becoming more prevalent in enterprise environments. As the cloud environment expands to encompass these technologies, the connected world depends on devices to manage, orchestrate and provision data.

"By 2023 the number of connected devices is forecast to reach 20 Billion."

This increase in volume is a growing challenge for service providers tasked with trying to keep their networks secure, as well as for enterprises and critical infrastructure entities deploying and managing devices.

Insecure data flow from the Edge to the Cloud is a concern of the IoT model of processing of data. Processing of data can be done either at the edge or at the Cloud. Edge computing provides a way to allow applications and services to gather or process data to the local computing devices, away from centralized nodes enabling analytics and knowledge generation to the logical extremes of the network.

Although edge computing enhances instantaneous response and subsequent decision making (e.g., use of machine learning to make autonomous decisions), it also results in a distributed, unsafe and uncontrollable disarray of data which can become critical when taking into account the amount and the sensitivity of data that is transmitted. Limited processing and storage capabilities of some endpoints may restrict security features, such as authentication, encryption and integrity protection mechanisms, jeopardizing both access control as well as the confidentiality or integrity of data transmitted to the Cloud. Even when security features are enabled, faulty implementation can have a great impact on the security of the entire model.

DDoS (distributed denial-of-service) botnet attack is another of the TOP 10 IoT Risks.

The Mirai botnet exploited a vulnerability in IoT devices to launch a DDoS attack against a critical DNS server that disrupted a number of the internet's biggest websites, including PayPal, Spotify, and Twitter.

Top 10 Internet Of Things 2018

01

Weak, Guessable, or Hardcoded Passwords
Use of easily brute forced, publicity available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

02

Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.

03

Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lock of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

04

Lack of Secure update Mechanism

Lack of ability to securely update the device. This incudes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anit-rollback mechanisms, and lack of notifications of security due to updates.

05

Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

06

Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

07

Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

08

Lack of Device Management

Lack of security support devices deployed in production, including asset management, updated management, secure decommissioning, systems monitoring, and response capabilities.

09

Insecure Default Settings

Devices or systems shipped with insecure with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10

Lack of Physical Hardening

Lack of physical hardening measures, allowing potential attaches to gain sensitive information that can help in a future remote attack or take local control of the devices.

According to OWASP, both aspects of security in this convergence are facing challenges from each other. Cloud Web Interface is listed as one of the attack surfaces of IoT, while Cloud Top 10 Security Risks include Service and Data Integration, which is bounded to the security of IoT devices.

Security Responsibilities in the Cloud

At a high level, security responsibility maps to the degree of control any given actor has over the architecture stack:

01

The CSP is responsible for nearly all security, since the cloud user can only access and manage their use of the application and can't alter how the application works. For example, a SaaS provider is responsible for perimeter security, logging/monitoring/auditing, and application security, while the consumer may only be able to manage authorization and entitlements.

Software as a Service (SaaS)

02

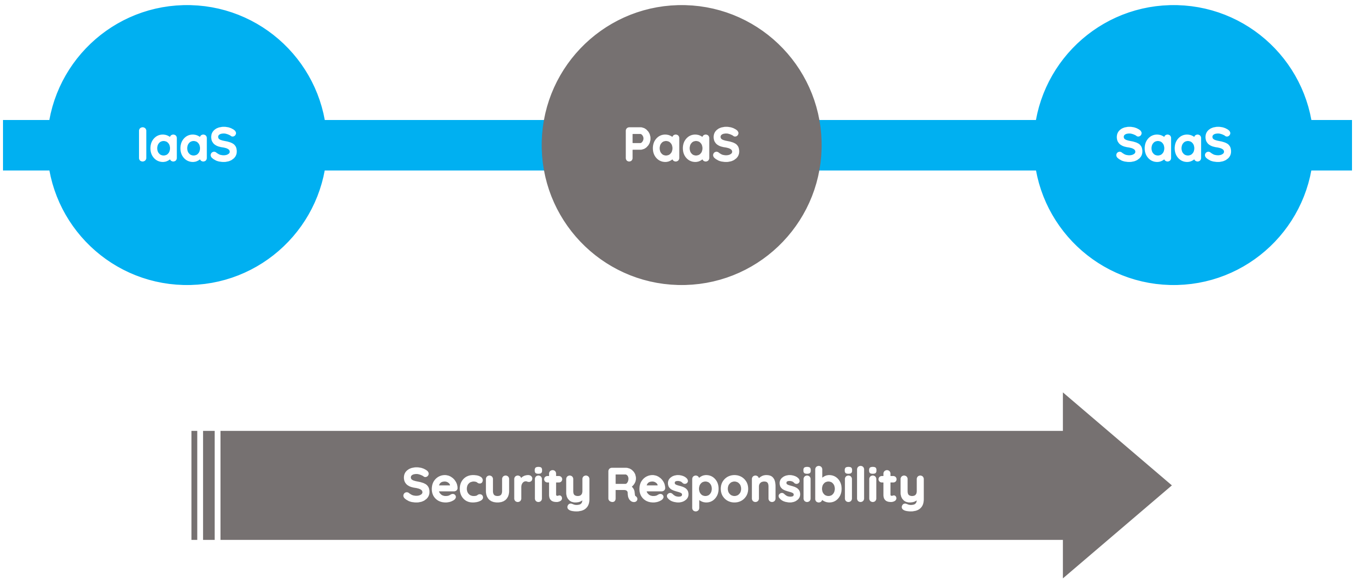
The CSP is responsible for the security of the platform, while the consumer is responsible for everything they implement on the platform, including how they configure any offered security features. The responsibilities are thus more evenly split. For example, when using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use managing accounts or even authentication methods.

Platform as a Service (PaaS)

03

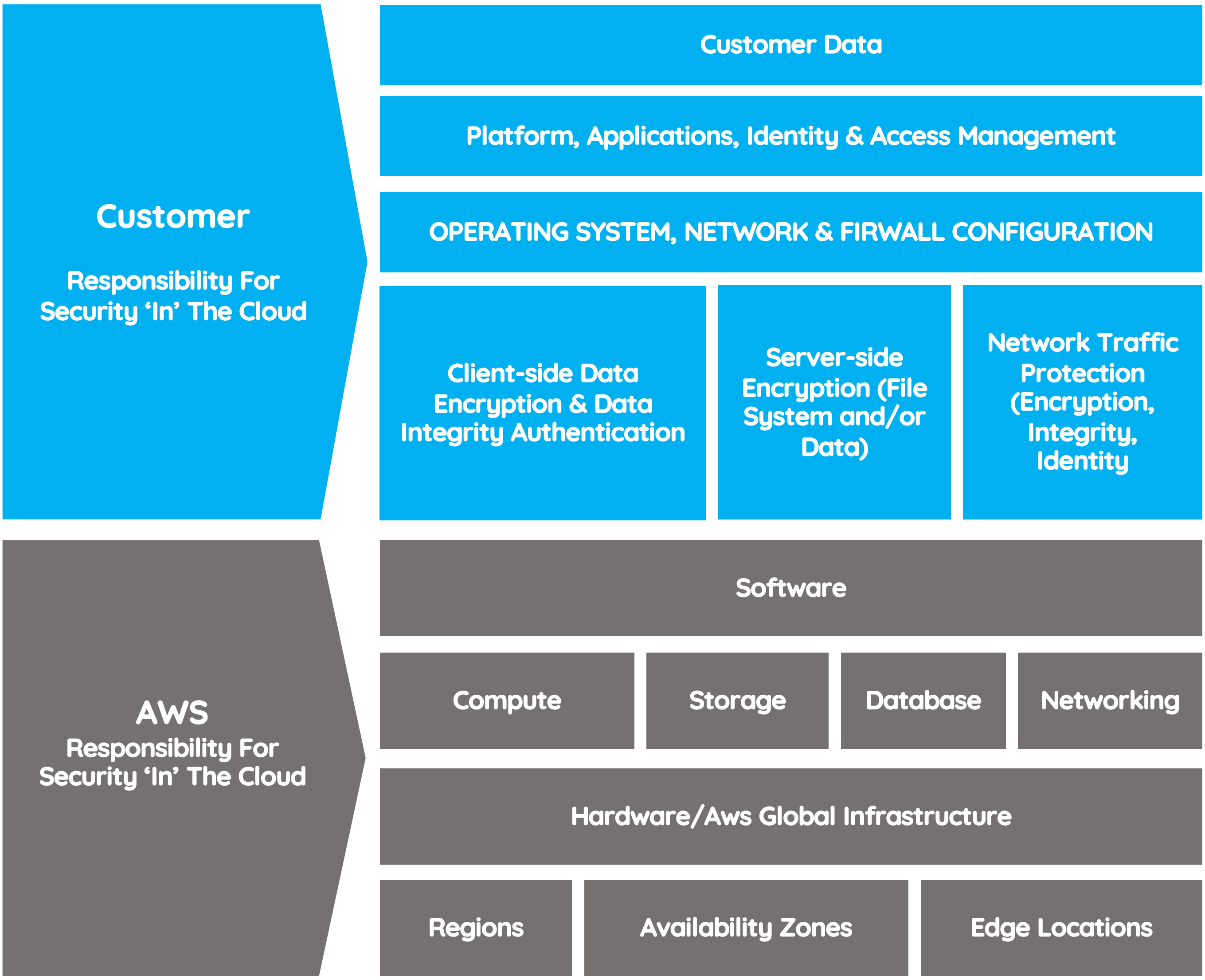
The CSP is responsible for the security of the platform, while the consumer is responsible for everything they implement on the platform, including how they configure any offered security features. The responsibilities are thus more evenly split. For example, when using a Database as a Service, the provider manages fundamental security, patching, and core configuration, while the cloud user is responsible for everything else, including which security features of the database to use managing accounts or even authentication methods.

Platform as a Service (PaaS)



Amazon's Shared Responsibility Model

Some SaaS providers believe that if they are hosting their application on Amazon AWS, they are automatically compliant just because Amazon AWS may be. This may be applicable to other IaaS or PaaS providers.


Customer
Responsibility For Security 'In' The Cloud
Customer Data
Platform, Applications, Identity & Access Management
OPERATING SYSTEM, NETWORK & FIRWALL CONFIGURATION
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption, Integrity, Identity
AWS
Responsibility For Security 'In' The Cloud
Software
Compute
Storage
Database
Networking
Hardware/Aws Global Infrastructure
Regions
Availability Zones
Edge Locations

SaaS CSP's may also need to review the exact controls in the SOC reports and examine whether the relevant controls and criteria are covered in those SOC reports. Availability of SOC report should not be just a checkbox for third-party (vendor) risk compliance.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation, and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

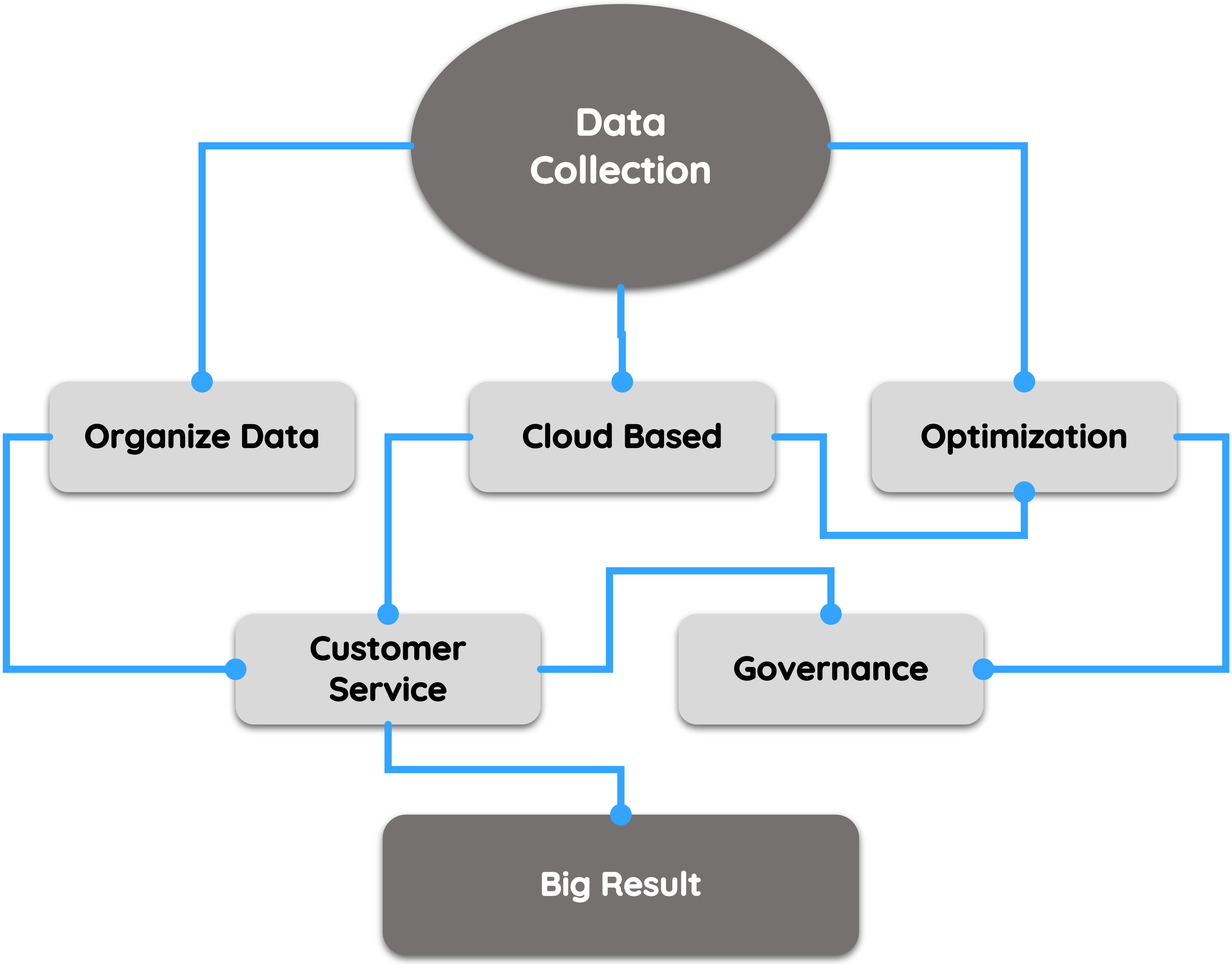
https://aws.amazon.com/compliance/shared-responsibility-model/

Governance in Cloud

Governance issues also relate to regulatory compliance, security, privacy, and similar concerns impacting today's organizations. Today's data management and storage landscape, where data entropy and data sprawl are rampant, has wide-reaching consequences for data security.

Many organizations are storing significant data in distributed and hybrid cloud and even unmanaged environments increasing challenges for regulatory compliance. A data inventory and data flow are often recommended. With increasing IoT devices and data lakes in the cloud, **the Visibility and Control are invariably lost resulting in Data Sovereignty challenges. Data Encryption is another factor to consider in the wake of compliance mandates such as GDPR, CCPA, HIPAA, PCI -DSS etc.**

Big Data Cycle



Disruptive technologies like Blockchain (Distributed ledger) has emerged as a candidate for financial institutions to reform their businesses. The speed and cost of doing business using distributed ledger technology are expected to improve by simplifying back-office operations and lowering the need for human intervention. However, a number of security concerns around this new technology remain.

Governance in Cloud

Governance and Enterprise Risk Management

The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may after these issues.

Legal Issues: Contracts and Electronic Discovery

Potential legal issues when using cloud computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.

Compliance and Audit Management

Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing effects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.

Information Governance

Governing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity and availability are mentioned.

CSA’s Cloud Security Threats

The way businesses use, store, and exchange data, software, and workloads is changing thanks to cloud computing. It has also brought with it a slew of new security risks and challenges. With so much data being sent to the cloud — and particularly to public cloud services — these tools are prime prey for malicious users.

TOP 11 CSA Cloud Security Threats

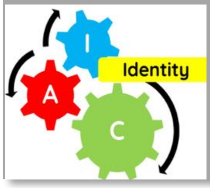
Data Breach

Sensitive, protected or confidential information is disclosed, either due to an attack or result of human error. Attackers want data, so businesses need to define the value of its data and the impact of its loss. Businesses need robust, tested incident response plans that take cloud service providers into account. Use of MFA and Encryption can protect from data breach.

Misconfiguration Inadequate Change Control

The complexity of cloud-based resources makes them difficult to configure. Misconfigured cloud can cause data breaches, service interruptions, unwanted deletion or modification of resources etc. The business should use automation and technologies that scan continuously for misconfigured resources.

Insufficient Identity, Credential, Access, and Key Mgmt



The cloud requires organizations to change practices related to identity and access management (IAM). Consequences of not doing so are security incidences and breaches. Use strict identity and access controls for cloud users and identities, segregation and segmentation of accounts on business needs and the principle of least privilege, remove unused credentials and access privileges and key rotation can prevent it.

Lack of cloud security architecture and strategy

To guard against cyber attacks, security measures need to be implemented properly. Many companies are migrating part of their IT Infrastructure to public cloud, and hence requirement of improved security implementation is necessary.

Account Hijacking

Account hijacking helps attackers to gain access to and manipulate highly protected or critical accounts. Once an attacker has obtained access to the system using a verified account, they can cause severe disruptions, such as data theft or damage, service blockage or delay, or financial fraud.

Insider Threat

An insider with malicious intent can cause more damage to an organization as he has more knowledge than anyone else. An insider does not need to have malicious intent to do damage; they could unintentionally put data and systems at risk. An organization must regularly conduct employee trainings and education, fix misconfigured cloud servers, and restrict access to critical systems.

Insecure Interfaces and API’s

APIs (Application Programming Interfaces) and UIs (User Interfaces) are the most exposed parts of a system and need to be protected at all costs, using all possible techniques. A weak set of interfaces and APIs exposes organizations to various security issues related to confidentiality, integrity, availability, and accountability.

Weak Control Plane

The control plane allows security and integrity to be applied to the data plane, which guarantees data reliability. A fragile control plane implies that the person in charge does not have total control over the logic, security, and verification of the data infrastructure. Perform due diligence to ensure the cloud service provider possesses an adequate control plane.

Metastructure and Applistructure Failures

In cloud services metastructure and applistructures play critical roles. Poor API implementation by the cloud provider offers attackers an opportunity to disrupt cloud customers by interrupting confidentiality, integrity, or availability of the service. At the same time, misconfigurations by the customer could disrupt the user financially and operationally.

Limited Cloud Usage Visibility

If an enterprise lacks the ability to imagine and evaluate whether cloud service use within the entity are secure or malicious, it is said to have limited cloud use visibility. It is a result of lack to governance, awareness and improper security implementation.

Abuse and Nefarious Use of Cloud Services

Malicious actors can use cloud infrastructure tools to exploit subscribers, organizations, or other cloud providers, and they can also use cloud services to execute malware. An organization must monitor their employees' activities and implement DLP and stop any unauthorized data exfiltration.

Cloud Risks are one the most critical risks to be looked at and addressed. Majority of data breaches happen due to misconfigured cloud servers. Insider Threat is also becoming popular. The cloud service providers and the users both require to educate and train their personnel on how to use the cloud services most efficiently.

> **“The complexity of cloud can be the perfect place for attackers to hide, offering concealment as a launchpad for further harm**
>
> **John Yeoh,**
> **Global Vice President of Research for CSA”**

04

Cloud Assurance For CSP'S

SOC 2 for cloud CSA STAR Attestation

Cloud Security Alliance (CSA) in collaboration with the AICPA, developed a third-party assessment program of CSP officially known as CSA Security Trust & Assurance Risk (STAR) Attestation. STAR Attestation provides a framework for CPAs performing independent assessments of CSP using SOC 2 engagements with the CSA's Cloud Controls Matrix (CCM).

www.cloudsecurityalliance.org/star/attestation/

Accedere is listed as auditors with CSA for their STAR Attestation

Cloud Controls Matrix (CCM)

The CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail, and clarity relating to information security tailored to cloud computing. CCM is currently considered a de-facto standard for cloud security assurance and compliance.

The CSA , STAR, logos are owned by Cloud Security Alliance

Cloud STAR Certification Roadmap

CSA Security Trust, Assurance and Risk (STAR) is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. The STAR program provides multiple benefits, including indications of best practices and validation of the security posture of cloud offerings.

		Audit Frequency	Security	Privacy
Type of Audit	●●●	STAR Level 3	Continuous Auditing	—
	●●○	STAR Level 3 Continuous	Level 2 + Continuous Self-Assessment	—
		STAR Level 2	3rd Party Certification	GDPR CoC Certification
	●○○	STAR Level 1 Continuous	Continuous-Self Assessment	—
		STAR Level 1	Self Assessment	GDPR CoC Self Assessment

Level 2 CSA STAR Attestation

The STAR Attestation is positioned as STAR Certification at Level 2 of the Open Certification Framework and STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. STAR Attestation is based on type I or type II SOC attestations supplemented by the criteria in the Cloud Controls Matrix (CCM).

The STAR Assessment

- Is based on a mature attestation standard.
- Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change.
- Does not require the use of any criteria that were not designed for, or readily accepted by CSP.
- Provides for robust reporting on the service provider's description of its system and on the service, provider's controls, including a description of the service auditor's tests of controls in a format very similar to the current SSAE 18 reporting, thereby facilitating market acceptance.

STAR Attestation builds on the key strengths of SOC 2:

- Is a mature attest standard (it serves as the standard for SOC 2 and SOC 3 reporting).
- Provides for robust reporting on the service provider's description of its system and on the service, provider's controls, including a description of the service auditor's tests of controls in a format very similar to the current SSAE 18 reporting, thereby facilitating market acceptance.
- Evaluation over a period of time rather than a point in time.
- Recognition with an AICPA Logo.

(STAR is a registered trademark of Cloud Security Alliance).

CSA Continuous Assessment (Level 2 & 3 Continuous)

STAR Level 2 Continuous builds on top of the STAR Level 2 requirement of third-party assessments and improves it by allowing the CSP to demonstrate a higher level of assurance and transparency by the addition of a Continuous Self-Assessment.

In STAR Level 2, a CSP is assessed by a third-party through one of the Level 2 programs against a determined and appropriate scope. The Level 2 programs, including STAR Certification, STAR Attestation, and C-STAR, are based on varied but demanding cloud security criteria of the CSA CCM,ISO/IEC 27001 or the AICPA Trust Services Criteria (TSC), applied towards the CSP's assessment scope.

The CSA , STAR, logos are owned by Cloud Security Alliance

Level 3 Continuous

Certification is a highly selective cloud security assessment program, extending the assurance level of a cloud service beyond the trust given by the certification cycle of ISO/IEC 27001 and the audit period of AICPA SOC 2 Type II reports.

STAR Level 3 Continuous requires all continuous assessments to be performed under the supervision of a third-party auditor. This differs from Level 2 Continuous, which requires a frequently submitted self-assessment on top of Level 2 by the CSP itself.

SOC 2 V/S ISO 27001

Many CSP's may also have adopted ISO 27001 (ISMS) and add-ons for their cloud environment. How SOC compares to this standard is provided in the table below:

Area	ISO 27001 (ISMS)	SOC 2 TYPE II
Standard	International Standard ISO/IEC 27001, Second Edition 2013-10-01, ISMS- Information Security Management Systems	Trust Services Criteria for Security, Availability, Process Integrity, Confidentiality and /or Privacy and other specific control framework/s
Governance	IAF Accreditation Body	AICPA/US State Board
Purpose	Assist organization's management in establishment and certification of ISMS that meets specified requirements and is able to be certified as best practice	• Oversight of the organization • Vendor management programs • Internal corporate governance and risk management processes • Regulatory oversight
Applicability	Statement of Applicability (SoA)of controls	System Description by Management
Period Covered	Point in Time. i.e. as on a date	Period of Time i.e., for the period xxxx (date) to yyyy(date)
Objective	Establish, implement, maintain, and improve the ISMS	Measure a service organization against specific Trust Services Criteria
Period Covered	Re-Certified for every 3 years	Attestation provided for min 6 months and max 1 year
Audit Frequency	Surveillance audit conducted Annually	Continuous monitoring during the period
Certified/ Attested by	ISO Accredited Registrar-Certification Body	Attestation by a Licensed CPA
Nature of Testing	Design effectiveness	Design and operating effectiveness
Controls in report	Details of controls not provided	Details of controls provided

Area	ISO 27001 (ISMS)	SOC 2 TYPE II
Focus	Organization's ability to maintain an ISMS	information and assurance about the controls at a service organization
Report	Single page Certification	Report containing the auditor's opinion, management's assertion, description of controls, user control considerations, tests of controls, and results
Difficulty to Achieve	Moderate	Higher
Structure	Information Security Framework	Trust Services Criteria and other specific control framework/s

C5 Cloud Controls

In February 2016, the Bundesamt fur Sicherheit Institute (BSI), or the German Federal Office for Information Security, established the Cloud Computing Compliance Controls Catalog (C5) certification after they noted the rise in cloud computing in the country. With the C5, the BSI redefined the bar that CSP should meet when dealing with German data. The establishment of the C5 elevated the demands on CSP by combining the existing security standards (including international certifications like the ISO 27001) and requiring increased transparency in data processing.C5 controls can be applied globally.

C5 is intended primarily for professional cloud service providers, their auditors, and customers of the CSP's. The catalogue is divided into 17 thematic sections (e.g., organisation of information security, physical security). C5 makes use of recognised security standards such as 27001, the Cloud Controls Matrix of the Cloud Security Alliance as well as BSI publications and uses these requirements wherever appropriate.

Federal Office for Information Security
Cloud Computing
Cloud Computing Compliance Controls Catalogue (C5)
Criteria to assess the information security of cloud services

A SOC 2 report proves that a CSP complies with the requirements of the catalogue and that the statements made on transparency are correct.

This report is based on the internationally recognised attestation system of the SOC 2 (ISAE 3000), which is used by public auditors. When auditing the annual financial statements, the auditors are already on site and auditing according to

C5 can be performed with not too great additional effort.

http://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

05

Privacy Compliance for Cloud

Privacy has grabbed the attention of Boards of Directors as regions look to implement privacy regulation and compliance standards similar to GDPR. Privacy is the new buzzword, and the potential impact is very real. Personal data is processed for political and economic reasons without users' consent, as happened in the Cambridge Analytica. In view of the recent incident's privacy laws are changing and going forward they may become more stringent. It may be prudent for organizations to be more proactive and adopt measures for Privacy Governance.

SOC 2 Privacy Category of Trust Services

To demonstrate the privacy related controls, Organizations can include the privacy category as part of the scope of their SOC 2 report. Additionally, controls for any other specific laws too can be included as Additional Subject Matter. The AICPA Trust Services Criteria, privacy category's broad requirements are described in the following paragraphs. Many of these requirements match to the legislation like GDPR, CCPA etc.. **In the wake of such new privacy mandates organizations are encouraged not only include the privacy category in their SOC 2 report but also to demand including them in their vendors SOC 2 report.**

SOC 2 Description for Privacy

When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described.

When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses, and disclosures of personal information permitted by user entity agreements.

Principal System Requirements

System requirements are the specifications about how the system should function to do thefollowing:

- Meet the service organization’s service commitments to user entities and others (such as user entities’ customers).
- Meet the service organization’s commitments to vendors and business partners.
- Comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations.
- Achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description.

Requirements are often specified in the service organization’s system policies and procedures, system design documentation, contracts with customers, and government regulations.

The following are examples of system requirements:

01 Workforce member fingerprinting and background checks established in government banking regulations.

02 System edits that restrict the values accepted for system input, which are defined in application design documents.

03 Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual.

04 Data definition and tagging standards, including any associated meta data requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP).

05 Processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA).

Data

Disclosures about the data component include types of data used by the system, transaction streams, files, databases, tables, and output used or processed by the system. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following:

The principal types of data created, collected, processed, transmitted, used, or stored by the service organization and the methods used to collect, retain, disclose, dispose of, or anonymize the data.

Personal information that warrants security, data protection, or breach disclosures based on laws or commitments (for example, personally identifiable information, protected health information, and payment card data).

Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants security, data protection, or breach disclosures based on laws or commitments.

AICPA Trust Services Criteria (TSC) for Privacy category

With about **50 points of focus,** the TSC organizes the privacy category as follows:

Notice and communication of objectives.	The entity provides notice to data subjects about its objectives related to privacy.
Choice and consent.	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
Collection.	The entity collects personal information to meet its objectives related to privacy.
Use, retention, and disposal.	The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
Access.	The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
Disclosure and notification.	The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

Quality.	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
Monitoring and enforcement.	The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

06

Cloud Security & Privacy for Users

Cloud users, at a minimum, should consider implementing the following controls:

Include cloud security and privacy risks, as part of your risk management life cycle.

Evaluate SOC reports with relevant controls of your CSP's.

Create a secure architecture using concept of security and privacy by design.

Implement secure access methodology e.g. TLS, MFA etc.

Document your data flow and implement data security controls.

Implement resiliency controls.

Implement and review Role Based Access Controls (RBAC).

Follow a Deming Cycle approach to cloud security & privacy.

Perform VA/PT of your cloud applications and environment.

Perform periodic audits of your hybrid environment.

Our Value Delivery

Knowing how much extra value and assurance a SOC reports can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a SOC engagement is a matter of clear thinking and smart planning. Working with a cyber security specialist such as Accedere helps you dig into areas such as cloud security, data security, privacy, incident response, and much more.

Some of the advantages of working with us are:

01 End to end process for SOC Reporting & Attest Services

02 Project management methodology consistently applied to each engagement

03 Efficient service delivery with minimal disruption to operations

04 Our engagements are executed by senior experienced professionals

05 CEO has 18 years of Information/ Cyber Security experience

06 Reduced time to complete assignments

07 Colorado licensed CPA Firm listed with PCAOB and Cloud Security Alliance

08 Prompt services with engagements completed in record time

09 Ongoing support

10 We are with you when you need us

For more information visit:

https://accedere.io