Implications and the need for the cloud

By Christo-Odysseus Keramitzis

Christo-
Odysseus
Keramitzis

Digitally signed by Christo-Odysseus
Keramitzis
DN: cn=Christo-Odysseus
Keramitzis, c=AU,
email=CKbusinessemail@proton.me
Date: 2024.11.22 22:42:02 +11'00'

By Christo-Odysseus Keramitzis

Executive summary

As cloud services become more available, cost-effective and a more convenient option for business; there will be a gradual increase in threats and concerns relating to cloud migration from on premises storage. This paper will discuss the relationship between cloud migration and the relevant regulatory risks, security threats and concerns a company may face.

This research paper aims to outline the various technical, legal and financial implications of cloud migration. The purpose is for organisations to understand the commitment and requirements needed to achieve a successful cloud migration that is inline with their business goals; thus this paper can act as a guideline for future risk assessments of cloud migration.

A brief introduction to the proposed solution, the cloud service provider(CSP) amazon web services(AWS), will be discussed due to their cost-efficiency, ease of use and professional cloud migration supporting services. This will be examined by discussing the roles CSP plays in not only handling the data but also how organisations will interact with the various services available; to reduce overall costs, increase efficiency and security of workflow. Through this analysis and discussion, a company can take into consideration the risks involved in migrating to a public cloud model. Aiding in deciding whether it is economically viable and feasible to transition to public cloud storage.

Introduction

As organisations wish to transition from managing their own private clouds to public shared clouds, concerns over security, data and operational risks become more prevalent. CSP allows for on-demand convenient cloud resources that remove the need for managing extensive data centres and virtualisation. This risk assessment will use the cloud service provider AWS as the proposed solution.Through the AWS provider, this paper will cover how cloud storage infrastructure functions and the possible business drivers that entice organisations to migrate. An in-depth analysis will be generated on the various challenges the company may have before and during migration; to convey the various considerations management and operations need to understand before making the decision to migrate. These outsourced resources will run on third party hardware outside the control of organisations, thus creating risks impacting the confidentiality, integrity and availability of company services .As CSP provides opportunities for international digital expansion of company services and products; it is important for management to develop a compliance plan that takes into account local and international laws present in the country of operation.

Scope

This report will analyse the legal and technical considerations linked to using and migrating to cloud infrastructure. The focus of the paper involves different public cloud computing models such as Software as a service(Saas), infrastructure as a service (Iaas) and platform as a service (paas). Due to the proposed solution being a CSP that incorporates the three models; an analysis will be conducted regarding the measurable risks pertaining to migration and the public cloud model and how they are paired to various legal and governance compliance laws and regulations.

Financial reporting such as liability,expenditure analysis etc, although an important factor, will not be discussed as this paper primarily focuses on the process of migration and its various risks and rewards; rather than a financial feasibility analysis it will focus on the technical aspects that may aid the company in transitioning their existing hardware and software to a CSP.

AWS is the proposed solution, therefore risk analysis of other vendors will not be included or extensive comparisons for the purpose of maintaining a succinct and cohesive report. Many of the discussed governance, Legal and security threats will generally apply to other CSPs, especially if they have similar services or functions to the AWS framework.

Research objectives

This report will attempt to respond to the following questions and possible concerns the company may have in regards to migration and traditional cloud architecture. Therefore a comprehensive report will be generated outlining the Governance legal and security requirements the company will need to consider if they choose to migrate to AWS. These requirements will come in the form of a risk assessment of the various legal governance and security aspects evident when incorporating third party cloud infrastructure into operations. These ‘research objectives’ covering the content include:

1. Why use public cloud infrastructure?
2. Technical, operational and managerial considerations to migrating
3. Migration risk assessment
    a. Potential security risks of using a CSP
        i. Availability of the cloud
        ii. Disaster recovery
        iii. Access management
        iv. Data integrity
    b. Compatibility with current cloud infrastructure
4. Legal and governance considerations
5. Responsibilities and Roles of provider and user
6. Feasibility analysis of moving to the provider

Therefore, this report will act as guidelines, by conveying in an objective manner the relevant information and commitments the company may need to consider when deciding to migrate their operations to a public cloud infrastructure from the traditional private cloud.

Analysis

The Cloud service model

As depicted in figure 1, AWS hosts a myriad of services built in a functional way to mimic traditional cloud architecture. This was intentional as it simplifies the migration process while still following the National Institute of Standards and Technology (NIST) cloud computing characteristics. The figure also depicts the different roles each service provides in what aspect of cloud computing. Figure 1 is not an expansive list and within this report some of these services will be discussed.

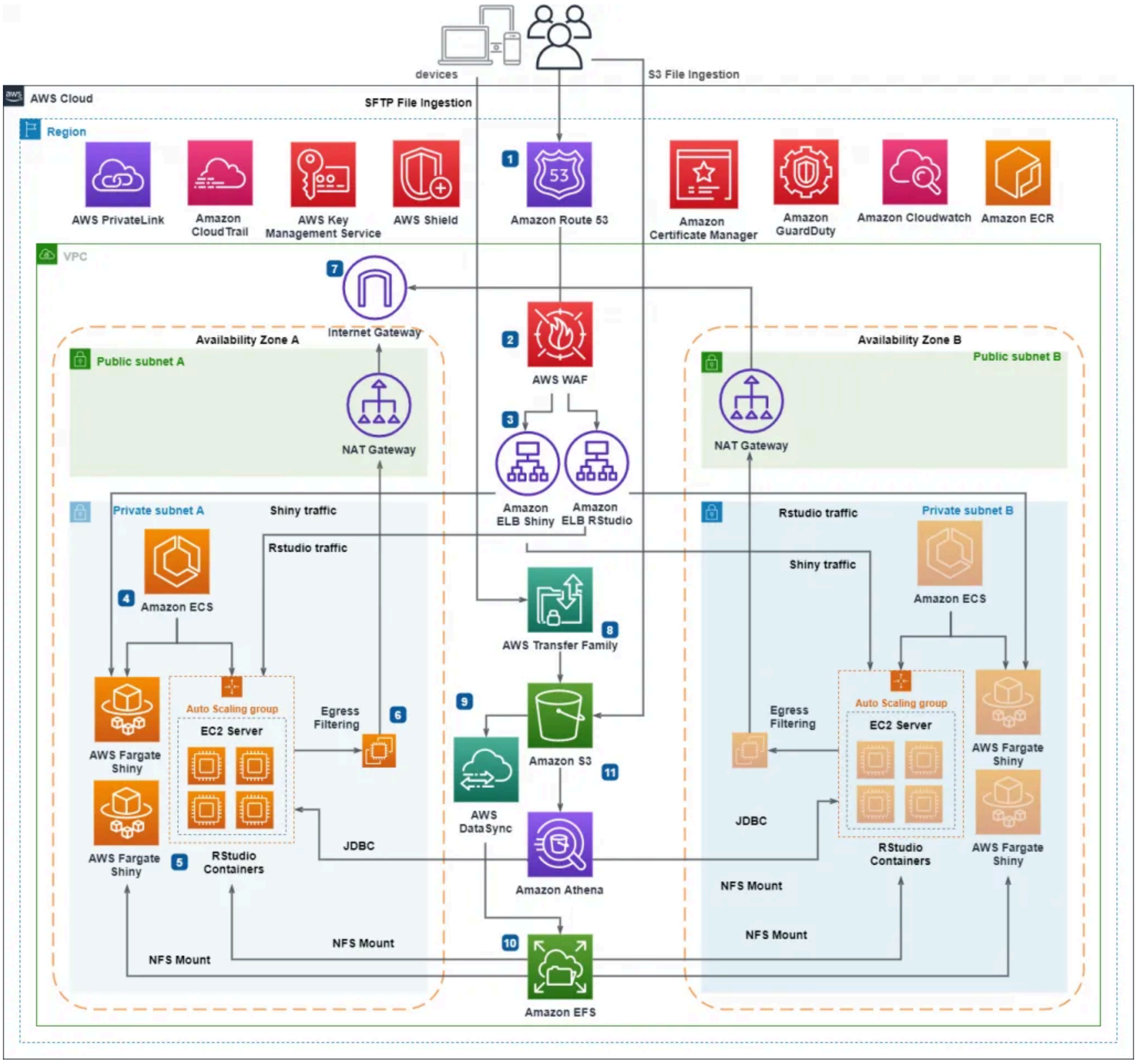
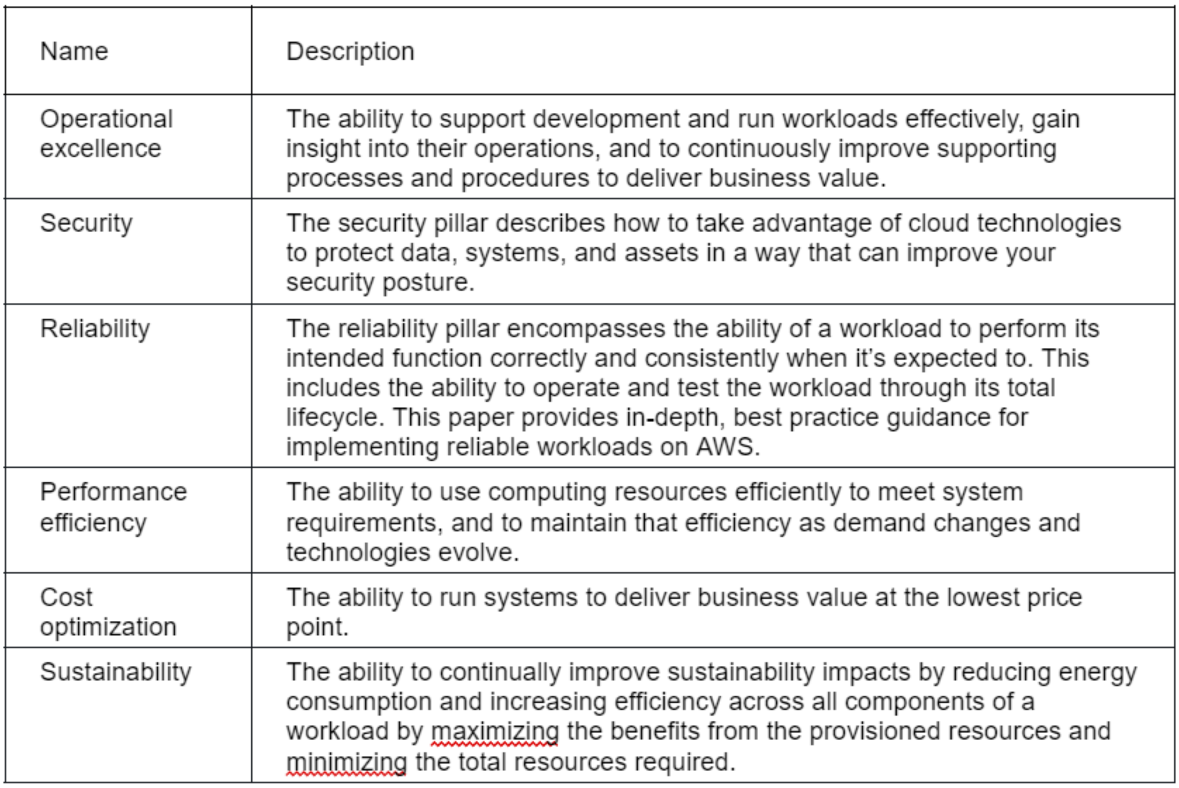


Figure 1 Otieno, K. M. (2023, September 15)

Throughout this report the AWS Well-Architecture Framework will be referenced. These 6 ‘pillars’ shown in table 1 represent best practices AWS encourages and offers within their services.



Name	Description
Operational excellence	The ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.
Security	The security pillar describes how to take advantage of cloud technologies to protect data, systems, and assets in a way that can improve your security posture.
Reliability	The reliability pillar encompasses the ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle. This paper provides in-depth, best practice guidance for implementing reliable workloads on AWS.
Performance efficiency	The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.
Cost optimization	The ability to run systems to deliver business value at the lowest price point.
Sustainability	The ability to continually improve sustainability impacts by reducing energy consumption and increasing efficiency across all components of a workload by maximizing the benefits from the provisioned resources and minimizing the total resources required.

(Table 1) Definitions - AWS Well-Architected Framework. (n.d.)

Business drivers to adopt public cloud

Corporations may consider migrating to a public cloud due to financial necessity, regional growth inhibitors such as access to faster and modern networking hardware and software limitations. AWS Enterprise design offers individuals many cost based options, operational efficiency and security toolkits that aid in managing and porting over data and threat models from private clouds. Therefore, migrating from traditional architecture to a public CSP provides a company with numerous advantages.

Financial benefits

These financial benefits would increase the company's return on investment and reduce ongoing expenditure; thus saving more capital for future ventures and enabling better management of company-wide finances.

- Economies of scale: The primary cost saving and convenience factor of the cloud is the NIST characteristic "pay per use". This allows companies to pay only for the resources they use; unlike traditional cloud solutions where there is either excess resources or a lack of.
- Upfront-costs reduction: Using public cloud solutions eliminates the need to purchase, host and manage the physical infrastructure of a cloud. Therefore initial upfront costs are reduced as the company would be using the CSP's existing infrastructure.

Rapid scalability

- With AWS there would always be an infinite number of available resources that can be incorporated into the cloud to be scaled with a new service or software. This convenience in accessing hardware resources reduces wait time of manually expanding hardware compared to traditional storage

Availability and internationalisation

- Managing a physical network of cloud servers spanning multiple countries or continents can become an operational challenge. CSP aids in overcoming this by providing existing international infrastructure that can be used by the company to "locally host" a cloud instance close to their users.

Challenges

Transitioning to a cloud format will inherently be paired with several challenges; Company management will need to discuss these challenges with the technician and software specialists so that compatibility and financial feasibility can be ensured before migration.

Technical

Applications

Services built on traditional hardware often are optimised around that hardware. Moving towards a cloud may come with compatibility issues if the application is not tested and improved to fit the new hardware.

Availability/continuity

Certain systems such as banks and databases require 24/7 connectivity to support a business critical service. If migration requires disconnection of these services for hours or days. Irreversible financial damage could occur; AWS attempts to remedy this issue with its seamless migration through resembling traditional data centres depicted in figure 2 of the VPC network structure.

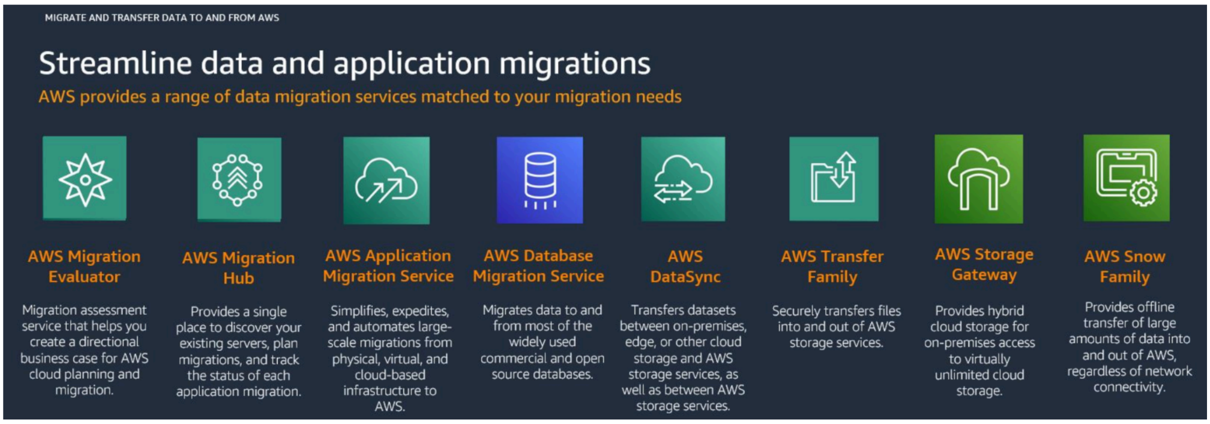
Data

It is a very common practice for CSPs to use Multi-tenancy; that is, where individuals 'share' the same hardware or 'space'. The Virtual private clouds(VPC) of multiple tenants are run on the same hardware. This creates data security issues where critical/confidential information is at risk from another individual who is not practising proper digital sanitisation and not implementing proper safeguards. Therefore, if that hardware becomes compromised, all VPCs are at risk. Thus it is important to consider the type of data that will be stored and whether it is feasible.

Financial

Financial challenges manifest due to product and data downtime during migration that prevent mission critical services from running. Additional financial challenges can be incurred through training needs as AWS uses their own proprietary software such as the dashboard to manage different cloud instances.

To aid with these challenges, AWS offers a myriad of migration services that specifically cater to these challenges and more. These tools and brief descriptions are depicted within figure 3.



MIGRATE AND TRANSFER DATA TO AND FROM AWS

Streamline data and application migrations

AWS provides a range of data migration services matched to your migration needs

AWS Migration Evaluator

Migration assessment service that helps you create a directional business case for AWS cloud planning and migration.

AWS Migration Hub

Provides a single place to discover your existing servers, plan migrations, and track the status of each application migration.

AWS Application Migration Service

Simplifies, expedites, and automates large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS.

AWS Database Migration Service

Migrates data to and from most of the widely used commercial and open source databases.

AWS DataSync

Transfers datasets between on-premises, edge, or other cloud storage and AWS storage services, as well as between AWS storage services.

AWS Transfer Family

Securely transfers files into and out of AWS storage services.

AWS Storage Gateway

Provides hybrid cloud storage for on-premises access to virtually unlimited cloud storage.

AWS Snow Family

Provides offline transfer of large amounts of data into and out of AWS, regardless of network connectivity.

Figure 3 Migration and Transfer - Overview of Amazon Web Services. (n.d.)

Cloud model and risks

With each consideration, a comparison will be made against traditional hardware to better depict the rigid dichotomy between public and private cloud solutions. AWS uses a myriad of services to automate and migrate successfully existing private infrastructure. Although AWS offers unique benefits over traditional and other CSP, there are some inherent risks and concerns regarding the mass movement of services, data and digital infrastructure used to a new hardware medium. Additionally, a brief overview of the AWS cloud deployment structure will be discussed; with the following sections being linked to the relevant cloud level and services.

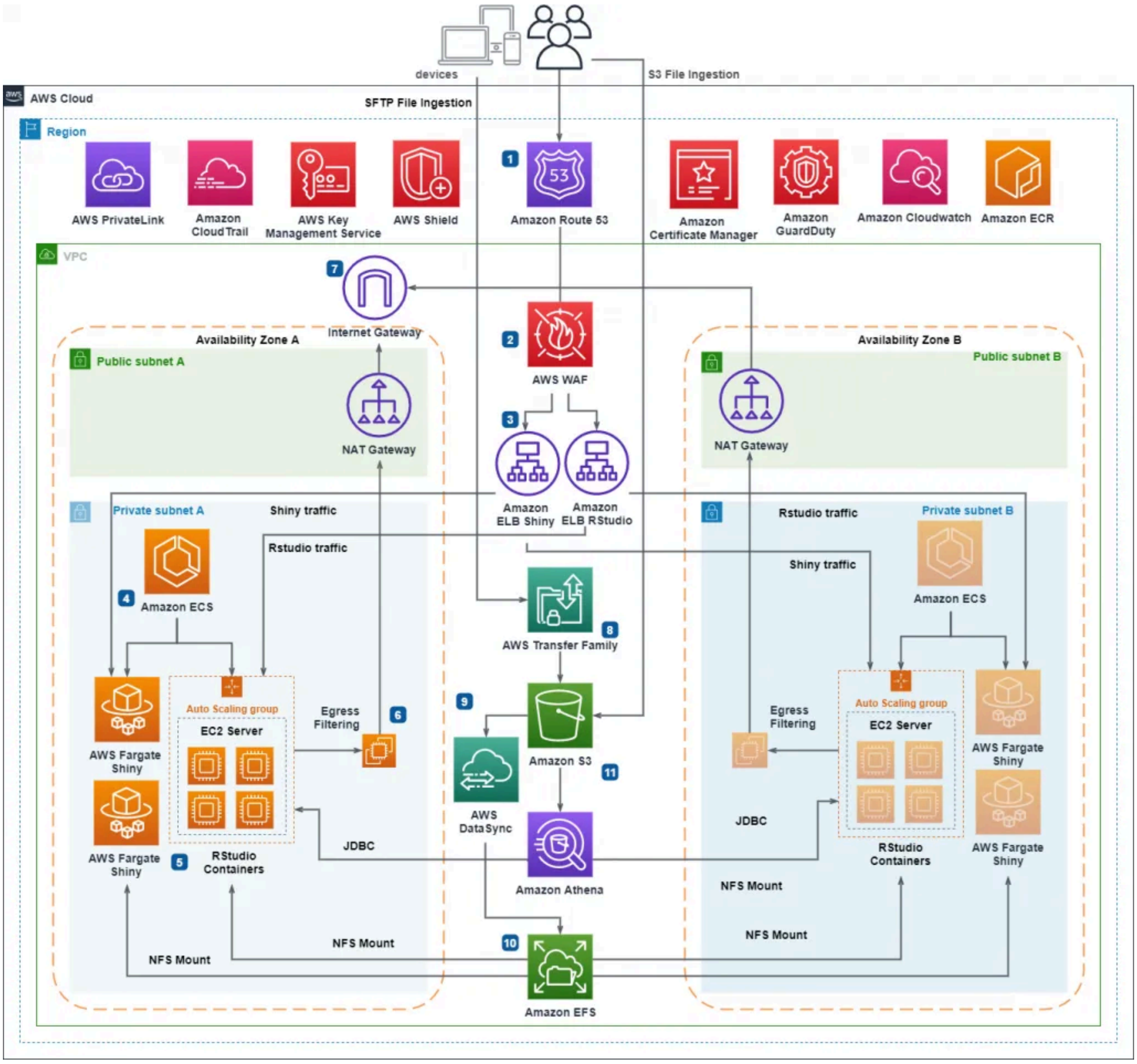


Figure 1

As discussed in the previous section, the VPC is generated to house the virtual cloud that houses the various components evident with private clouds like networking infrastructure, databases and servers. through the various routing services such as route 53 to mimic DNS connectivity, relational database (RDS) and DynamoDB that replicate existing database hardware and the elastic computing module (EC2) simulating cloud computing. Thus, AWS follows a high-level-design philosophy depicted in Figure 4.

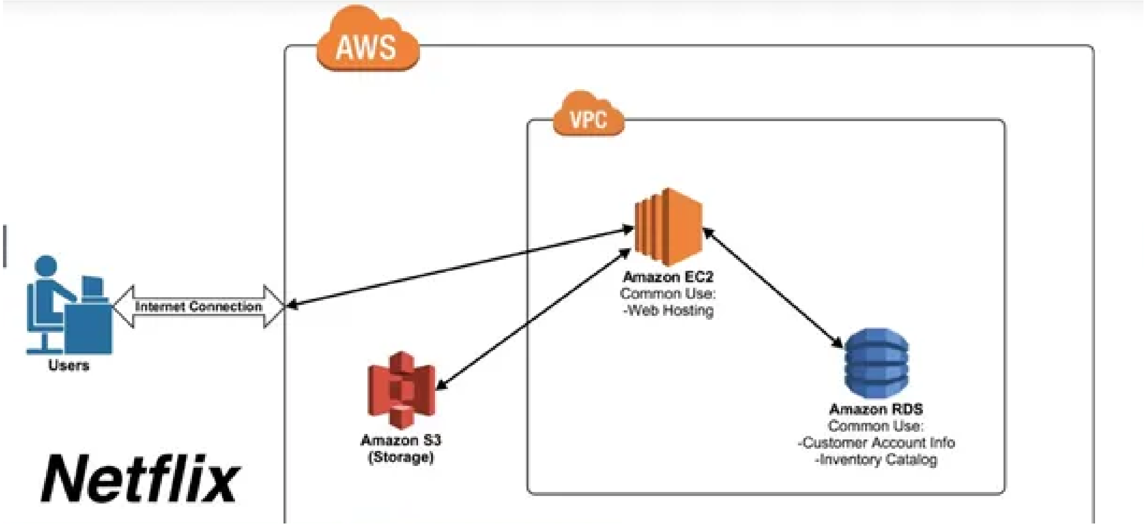


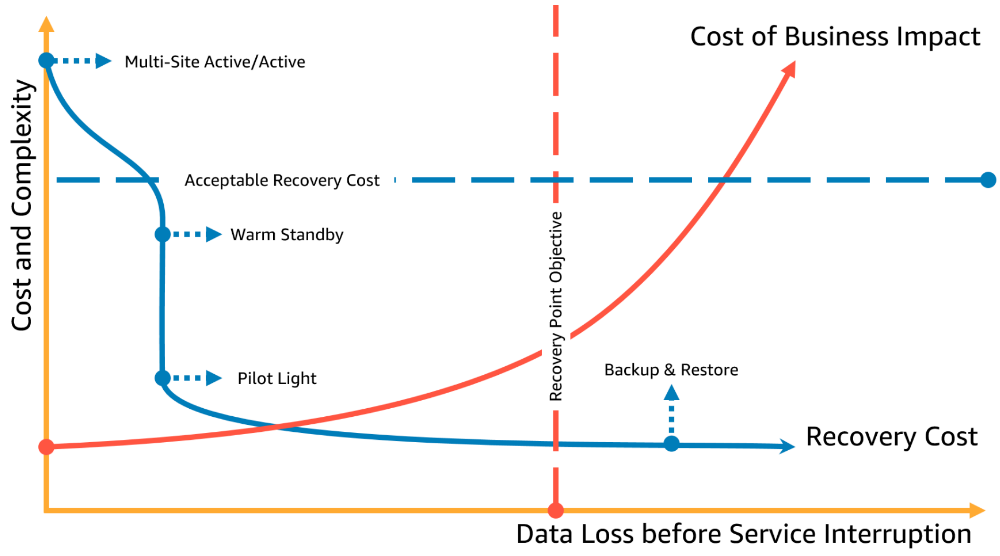
Figure 4 is a simple example of amazon cloud architecture Singh, P. (2021, May 4)

A common theme throughout the risk assessment of cloud service modulus is reliance and trust in the cloud providers ability to keep these services functioning in a stable and reliable manner.

Business continuity/Disaster recovery

Business continuity is reliant on AWS's ability to maintain a high level design that allows for 24/7 availability. Through multi-tenancy and access to AWS managed hardware, if there is a failure of cloud hardware the VPC will be ported to other hardware seamlessly to ensure high availability. Organisations need to consider whether AWS's SLA aligns with their operational needs.

AWS also provides a business continuity plan documenting best practices embedded within their well-architectured framework. This plan aids in using the available services to prepare for the eventual data loss that can occur, by creating recovery points and times where images of databases or EC2 can be made.



Graph 1 depicts the disaster recovery plan Business Continuity Plan (BCP)

Risks

When companies choose to use CSPs, they place a level of trust within the provider to maintain constant connectivity and hardware stability. If another shared user runs heavy-workload programs, the shared resources of the hardware can slow increasing latency and responsiveness due to Multi-tenancy.

Networking

AWS's suite of networking tools such as route 53 and AWS WAF mirror physical network infrastructure similarly to how private clouds are designed. This allows for the reliable transmission of packets in a controlled and configured environment that can be monitored through VPC flow logs, and AWS cloudwatch. It also simplifies connectivity between the various instance types located in different availability zones.

Risks

Strategic placement of EC2 instances and buckets need to be considered so that company users can achieve low latency without connectivity issues; thus management will need to conduct a thorough user study. AWS's defensive services can conflict with network traffic through weak API calls and mis-managed firewall configurations through AWS shield. Therefore consideration of how the workload interacts with the network needs to be analysed, especially if the services being run require elevated network privileges.

Storage

CSP offers elastic, pay-per-use storage, allowing for accurate scaling of cloud resources to match workload intensity. AWS has an auto scaling feature that fits the workloads size allowing for constant access to compute resources through EC2.

These storage requirements extend towards data storage through DynamoDB and the S3 buckets utilised by the company. To aid in disaster recovery of data, AWS allows for the rapid replication of cloud databases/images that can be stored in multiple regions internationally through AWS backup and EBS. It is important for management to consider periodic and on-demand backups of their various clouds as part of the disaster recovery plan

Risk

Placing sensitive information within shared hardware places company data at risk of data leaks through mismanagement of access control and hardware failure. By using third party hardware to store workloads and databases, companies put at risk their data by relying on the CSP's outlined data privacy and protection policies.

Security risk of the public cloud

As AWS uses multi-tenancy, it opens possible avenues for security attacks and resource allocation risks to occur; the threats will be divided by who is responsible for managing/preventing the threats..

Common security threats

Tenant liability

1. IAM mis-configuration
2. Data encryption
3. Exposure of databases
4. Malware (trojan horse)
5. Phishing
6. Firewall misconfiguration

CPS liable

1. Multi-tenancy infrastructure
2. Hardware failure
3. Man-in-the-middle attacks (data interception,replay attack)
4. Injection attacks (sql, cross-site scripting)
5. DDOS

Security management and controls

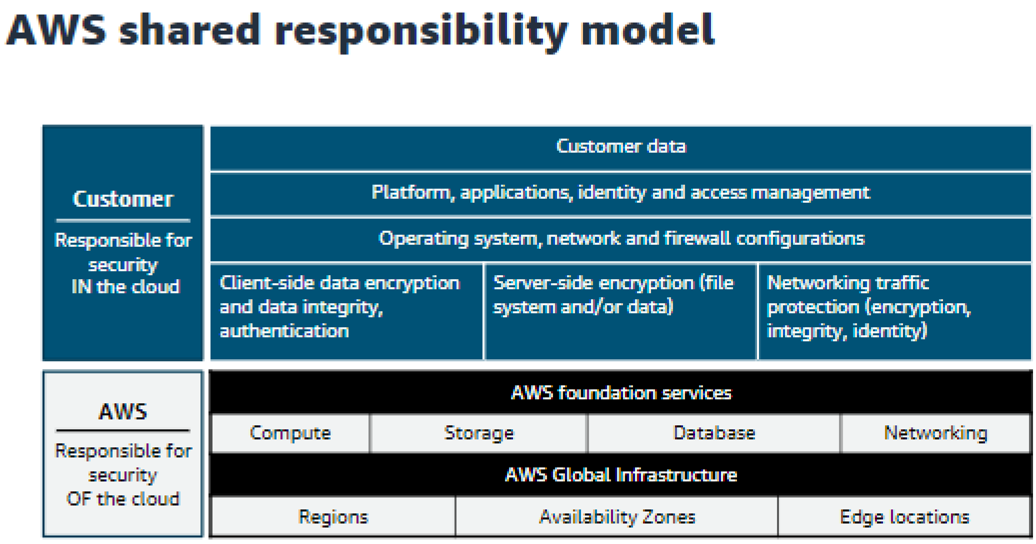
AWS has a myriad of security tools at the connectivity layer that analyses and monitors network traffic. It is mostly the responsibility of the tenant to configure and utilise most of these services; some automatically defend against common threats while other tools are optional and require professional configuration to respond to the company's chosen threat model.

- Firewall: AWS offers the ability to configure a firewall(AWS WAF) for advance control of inbound and outbound traffic. Additionally , there are a plethora of tools such as route 53 for automatic and manual DNS management, certificate manager for Public key infrastructure etc.
- DDOS protection: AWS shield is the primary defence against ddos attacks that AWS provides. Advance firewall rules can also aid in preventing denial of service attacks.
- Antivirus software and IPS: There is a plethora of server and database antivirus software that can be used to periodically scan for malicious files. AWS offer several tools such as Amazon guard duty, amazon cloudwatch for resource monitoring and data tracking etc

Governance and compliance

Role responsibilities

When incorporating the public cloud, it is important to understand who is accountable for what risk. The cloud is a complex piece of digital architecture that places different liabilities on different individuals. Therefore, AWS has manufactured a model for identifying responsibilities that defines clear boundaries the company and AWS will follow. Thus dividing risk between each other. This comes in the form of the AWS shared responsibility model depicted in figure 5.



AWS shared responsibility model

Customer

Responsible for security IN the cloud

Customer data

Platform, applications, identity and access management

Operating system, network and firewall configurations

Client-side data encryption and data integrity, authentication

Server-side encryption (file system and/or data)

Networking traffic protection (encryption, integrity, identity)

AWS

Responsible for security OF the cloud

AWS foundation services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge locations

Figure 5

The provider

The responsibilities model simplifies risk management as it generally takes charge of the hardware, virtualization and availability of the cloud. AWS's role is to ensure the healthy functioning of the hardware being used by the tenants and the global infrastructure that offers multi region connectivity. AWS manages the virtualization and software layer needed to provide their cloud service

The Tenants

Clients of AWS are mostly responsible for the data, authentication, IAM and services they chose to run on the VPC. tenants are responsible for what they choose to use within the cloud and how their users will interact with the VPC.

Service level agreement (SLA)

This shared responsibility can be extended towards the different contractual and service level agreements accepted by each party; this forms the basis of governance. AWS's SLA documentation offers clear status and expectations of each service provided. This may help corporations in deciding whether the relevant services and expected availability is adequate for their operations.

SLA's provide contractual service standards providers must follow; Both CSPs and their users should consider the following infrastructure critical responsibilities and roles:

- Availability: SLAs clearly define the expected availability of services and uptime responsiveness to ensure business continuity.
- Clear definitions of service functions/Type of services provided: All provided services need to be listed in a clear format with definitions explaining the primary functions and use cases of each service.
- Service monitoring and reporting: CSPs must provide continuous monitoring and live status reports of their services so users may know when connectivity issues occur.

- Incident response: Parties should be made aware of incident response time through an incident resolution metric.
- Outcomes if the CPS or customer do not uphold the SLA: If SLAs are not upheld by the parties, options to terminate the service or claim compensation can be outlined.

Reasons for careful SLA consideration:

- Prepare for network/service down time
- Protection of data integrity and confidentiality
- Understanding responsibilities
- Service overview.

SLAs define what users and CSPs are responsible for in an informative manner. This allows corporations to clearly understand how AWS functions; therefore allowing businesses to cater their database, networking and monitoring infrastructure to the CSP for successful cloud compatibility. It also enables for a pre-emptive disaster recovery plan to be created before complete migration to the cloud occurs, thus aiding in securing electronic data and records. It is important that company management and operations understand clearly the SLA so that the relevant services influencing data governance can align with business objectives.

Government regulation and legal requirements

CSPs offer international service and operational availability; consequently, Data usage and its handling are virulently regulated by local and national courts differently internationally. Due to this, compliance and governance laws need to be understood in the countries corporate wishes to operate in; to avoid government penalties from a lack of compliance.

Data

Data privacy

Data privacy laws are one of the primary data compliance standards/laws that influence data usage, transformation and transport. Local laws such as the data privacy act 1988, is the primary privacy regulatory law that protects how personal information is handled. In comparison, the General Data Protection Regulation(GDPR) of the European union; prohibits the transfer of certain data outside of the European economic zone.

Privacy regulations incur additional need for data governance, such as the accurate identification of critical user information, that management will need to consider before moving to the cloud.

Data Security

Security not only includes protection of databases but also data in transit and its integrity during transformation. Under the consumer data right act OAIC. (2023, March 10); “businesses must meet strict information security requirements. This includes ensuring your data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. Any data that is no longer needed for a permitted purpose must be deleted or de-identified”.

Furthermore, international recognised standards such as ISO and NIST can be enforced that ask for a certain level of protection through access control, encryption and data controls.

Data storage

The Competition and Consumer Act 2010 Data rights section influences how the data needs to be stored; but also forces companies to extensively monitor their databases for any abnormalities. The Act forces 'data safeguards' that limit how companies can access, store and share user data; as well as levels of data transparencies such as declaring data breaches. In comparison, the USA enforces a collection of regulations such as the Driver's Privacy Protection Act of 1994, Children's Online Privacy Protection Act and The Video Privacy Protection Act. These regulations and regulatory bodies dictate the type of data that can be stored, from what individuals allowed and where it can be transferred.

These example compliance laws issued by governments need to be understood as AWS offers easy international access. The places in which corporations choose to operate require an understanding of compliance laws between CSPs and governments to prevent compliance breaches.

Conclusion

Cloud service providers such as AWS allow for rapid scaling of business resources on an international level. Thus providing new opportunities for business expansion into new markets by limiting digital barriers. As the use of public clouds rises, it is important for companies to consider the digital risks to their data and operations; but also to be aware of the various service level agreements and international compliance laws to prevent breach of contract. Thus aiding in analysing the risk of migrating from private to the public cloud effectively.

References

- Otieno, K. M. (2023, September 15). Simplifying AWS Architecture Diagrams: A Beginner's Guide. Medium. https://medium.com/@KeithMOtieno/simplifying-aws-architecture-diagrams-a-beginners-guide-9f2b9db57976
- Definitions - AWS Well-Architected Framework. (n.d.). Docs.aws.amazon.com. https://docs.aws.amazon.com/wellarchitected/latest/framework/definitions.html
- Migration and Transfer - Overview of Amazon Web Services. (n.d.). Docs.aws.amazon.com. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/migration-services.html
- Singh, P. (2021, May 4). AWS High-Level Architecture. Analytics Vidhya. https://medium.com/analytics-vidhya/aws-high-level-architecture-42f049bae6f0
- AWS. (2023). AWS Service Legal Agreements. Amazon Web Services, Inc. https://aws.amazon.com/legal/service-level-agreements/?aws-sla-cards.sort-by=item.

additionalFields.serviceNameLower&aws-sla-cards.sort-order=asc&awsf.tech-category-filter=

- OAIC. (2023, March 10). Consumer Data Right privacy safeguards. OAIC. https://www.oaic.gov.au/consumer-data-right/information-for-consumers/cdr-privacy-safeguards
- Office of the Victorian Information Commissioner. (n.d.). Privacy law – an overview. Office of the Victorian Information Commissioner. https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/privacy-law-an-overview/
- Business Continuity Plan (BCP) - Disaster Recovery of Workloads on AWS: Recovery in the Cloud. (n.d.). Docs.aws.amazon.com. https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html
- Creating backup copies across AWS Regions - AWS Backup. (n.d.). Docs.aws.amazon.com. https://docs.aws.amazon.com/aws-backup/latest/devguide/cross-region-backup.html