A Critical Evaluation of Cloud Computing Service Models, Security, and Governance

Table of Contents

Chapter 1 Introduction

Cloud computing has established itself as a ground breaking technology used in the contemporary organizations, changing the manner in which computing resources, applications as well as filing are provided and administered. Cloud computing enables by facilitating instant availability of compressible as well as shared computing resources on the web, improves operational efficiency, lowers frameworks expenditure, and advanced digital innovative, which fosters organizations to retain the advantages of cloud computing [1]. With the increasing use of cloud services, companies are also to mitigate built-up challenges associated with security, risk management, business continuity and regulatory compliance [2].

This paper is a critical assessment of important concepts and practices in cloud computing, specifically in the models of cloud service, risk management, application architecture, and legal governance [3]. The discussion starts with the Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) where the models can be differentiated on the basis of control, responsibility, and delivery of value [4]. A Business Impact Analysis is then applied in an effort to evaluate the potential risk to organizations that are dependent on clouds and that effective mitigation strategies can achieve business continuity and resilience [5].

Another issue that the portfolio addresses is the use of backup and disaster recovery policies by large cloud service providers, and how this can be used to guarantee the availability of services and protection of data [6]. The use of APIs, cloud architecture components and development of cloud applications are discussed to show how the principles of cloud-native design help promote possibilities of scalability and flexibility [7]. The portfolio can cover the legal and compliance issues, e.g., those related to HIPAA rules,

---

[1] Cloud computing enabled business model innovation - ScienceDirect
[2] Cloud-based business services innovation: A risk management model - ScienceDirect
[3] Cloud-based business services innovation: A risk management model - ScienceDirect
[4] A Comprehensive Analysis of Cloud Service Models: IaaS, PaaS, and SaaS in the Context of Emerging Technologies and Trend | IEEE Conference Publication | IEEE Xplore
[5] A Comprehensive Analysis of Cloud Service Models: IaaS, PaaS, and SaaS in the Context of Emerging Technologies and Trend | IEEE Conference Publication | IEEE Xplore
[6] fin_irjmets1700193452-libre.pdf
[7] Paper Title (use style: paper title)

SOC assurance reports, and related critical risk management terms, to name risk appetite and risk tolerance [8].

1.1 Cloud Service Models: IaaS, PaaS and SaaS

Cloud computing service models help organizations use computing resources in various forms based on their technical expertise, concerns cost-wise, and business needs. The National Institute of Standards and Technology (NIST) has made three major service models that include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The section shows one business model, revenue model and service provision, of each of the models.

1.1.1 Infrastructure as a Service (IaaS): Amazon Web Services – Amazon EC2

Amazon Elastic Compute Cloud (EC2) is an Infrastructure as a Service (IaaS) service core of Amazon Web Services (AWS) [9]. EC2 enables the organizations to on-demand the virtualized computing resources including servers, storage, and networking infrastructure without the need to invest in physical computing hardware.

1. Business Model:
   Amazon EC2 business model is aimed at offering scalable on-demand infrastructure to organizations that provide applications in full control of the operating system and the running environment. AWS manages and owns physical data center and customers manage and configure their virtual machines, middleware, operating systems and applications. This model is favored especially in any business that values flexibility, customization as well as controlling its infrastructure.
2. Revenue Model:
   Amazon EC2 is a pay-as-you-use service, in which the customer pays in proportion to actual usage of the resources, including computes time, storage and data transfer. Other types of pricing are also offered, such as reserved instances and savings plans, where a customer can save at the expense of longer contracts. The consumption revenue model is a type of revenue that can draw small startups and large corporations to AWS because it presents cost economy and scaling.

[8] Regulatory Compliance and Risk Management | Springer Nature Link (formerly SpringerLink)
[9] 2.pdf

3. Service Offerings:

   Among the key services provided by Amazon EC2 are virtual machine (instances), elastic block storage, virtual private networks, load balancing and auto-scaling services. These services enable the cloud consumers to build highly available and fault-tolerant infrastructures at the same time they are responsible to the system administration and security configurations.

1.1.2 Platform as a Service (PaaS): Google Cloud – Google App Engine

Google App Engine is a Platform as a Service (PaaS) service which gives application developers the ability to create and deploy applications and scale them without administering the hardware on which the service depends.

1. Business Model:

   Google App Engine is a business whose model is directed towards abstraction and productivity of the developers. By the use of Google, it takes care of the infrastructure, operating systems, runtime environments, and scaling mechanisms so that the developers are only concerned with application logic and functionality. This goes a long way in making operations significantly simpler and shortens the application development and deployment cycles.
2. Revenue Model:

   The Google App Engine uses a pay-as-you-drive system where user-based charging system depends on how much of the computing resources (CPU time, memory and storage) by the application the customer has used. There is also a free tier when the application is used in low usage that offers to be adopted and tested. This is an elastic charge framework that sustains small developer setup, as well as undertaking high-level applications.
3. Service Offerings:

   Some of the critical service offerings are automated scaled service environments of popular programming languages, managed runtime environments, in-built security, monitoring systems, as well as interoperability with other Google Cloud services like databases and analytic platforms. Such characteristics render App Engine to be especially appropriate to web and mobile applications that need swift scalability and low administration of infrastructure.

1.1.3 Software as a Service (SaaS): Microsoft – Microsoft 365

Microsoft 365 is a well-known Software as a Service (SaaS) platform that provides productivity solutions like Word, Excel, Outlook, and Teams through the cloud-based platform.

1. Business Model:
   Microsoft 365 business model is focused on the provision of entirely controlled software programs online. The Microsoft has the responsibilities of updating, supporting, maintaining, and the security and availability of applications. The software does not require local software installation and management to be accessible by the end users, who do so using web browsers or through client software.
2. Revenue Model:
   The revenue streams of Microsoft 365 are more of subscriptions, whereby they have various pricing levels modified to individuals, businesses, and enterprises, every month or year. The price depends on the number of users and the features included, which can guarantee the recurrent revenues of Microsoft and the accuracy of cost disclosed to the clients.
3. Service Offerings:
   Its services are cloud-based productivity applications, cloud storage in one drive, email services in exchange online and team working in Microsoft teams. These services have high availability, automatic updates, inbuilt security controls and easy accessibility among various devices.

1.2 Business Impact Analysis and Risk Management

Business Impact Analysis (BIA) is a methodological procedure that is applied to the functions of the business as a way of identifying the functions that are vital and evaluates the effects that organizational operations can be affected in the event of a disruptive event [10]. BIA can be used in a cloud computing environment to ensure that effective risk management is deployed as it helps organizations to comprehend how technological risks, operational risks, and environmental risks could impact on the business continuity. This part gives a Business Impact Analysis of a particular organizational department, and then the identification of significant risks and threats associated with cloud-based infrastructure is given.

---

[10] Integrating business impact analysis and risk assessment for physical asset criticality analysis: A framework for sustainable operations in process industries - ScienceDirect

1.2.1 Department/Function Selection

A medium-sized retail organization has been chosen to complete this Business Impact Analysis in terms of the IT Department. This department is important in aiding the day-to-day running of the organization by managing cloud-hosted systems, such as the point-of-sale systems, inventory management systems, databases of customers, and e-commerce systems. The growing dependency on cloud computing in a retail organization places the IT function at the center of guaranteeing the availability, security and reliability of the system, data and services.

The IT department will take care of cloud infrastructure maintenance, third-party cloud service providers, the implementation of cybersecurity users, and compliance with data protection laws and regulations. Any failure of the IT services will have a direct effect on revenue generation, customer satisfaction and regulatory compliance. As an illustration, the system crashes can potentially deny customers the opportunity to make transaction, and data theft can spread sensitive customer information with sever repercussions.

The IT department is an appropriate choice of the analysis as it is a high-impact node with a high number of dependencies on cloud technologies. Reliance on external cloud service providers by the department also brings with it a consideration of shared responsibility in which both the organization and the provider have a responsibility to keep the issue of security and availability intact. In response to this, the IT department is vulnerably exposed to various types of operational, cyber and environmental risks hence making it an appropriate target to complete Business Impact Analysis and risk management planning.

1.2.2 Identification of Risks and Threats

After the identification of the IT department, five hypotheticals, though realistic, risks were developed based on the main threats that organizations enter under the cloud computing environment encounter. These risks have been chosen so that to have a balanced determination that covers malicious cyber threats, operational failure, insider risks as well as environmental hazards.

The ransomware attack on cloud-hosted systems is the first risk that was identified. Ransomware is a major risk to organizations in that it encrypts important data and systems which may result to extended service interruptions and loss of finances. Such an attack can interfere with transactions processing, inventory control and customer data in a retail market.

The second threat is the failure of cloud service provider. Even though this is provided by major cloud providers with high availability, sometimes outages are possible as a result of the technical failures, or as a result of maintenance undertakings. These disruptions may cause business-essential applications to be inaccessible, causing business to come to a halt and revenue to be lost.

The third threat pertains to a data breach of information of customers. The cloud-based systems retain large amounts of sensitive personal and payments information in retail organizations. The IT department would face the risk of regulatory fines, lawsuits, and a negative image due to a data breach.

The fourth threat is an insider threat, which is caused by either malicious or human error. Users who gain unquestioned access can either accidentally leak information or unscrupulously utilize cloud resources and provoke a security breach or breach of compliance.

The last risk is a natural disaster that will impact data center access or network connection. Natural disasters can also affect services or connectivity even when cloud providers are running distributed geographically based infrastructures, explaining why disaster recovery planning is critical.

1.2.3 Business Impact Analysis and Risk Management

Table 1: Business Impact Analysis and Risk Management Worksheet

BIA/RISK MITIGATION WORKSHEET: THREAT AND HAZARD ANALYSIS			
EF Number and Statement:			
	Step 1	Step 2	Step 3
Entry #	Threat or Hazard	Threat or Hazard Characteristics and Potential Impacts	Mitigation Strategy
1	Cloud-hosted system ransomware attack.	Ransomware attack would be capable of encrypting essential cloud-based system of inventory management, payment system and customer database. This would lead to downtime at work, loss of sales revenue, and possible loss of data, tarnished reputation, and even legal repercussions in case of data theft of customer information.	Practice routine automated cloud back-ups, endpoint protection, intrusion detection systems as well as staff training on cybersecurity awareness. Initiate and test a disaster recovery plan and incident response plan on a regular basis.
2	Cloud service provider failures.	The shutdown of the cloud service provider will partially lead to the unavailability of business-critical applications and services. This could interfere with sales over the internet, internal processes and access to services by customers, and result in losses and decreased trust in the company.	Apply multi-region deployment, redundancy and failover technologies. Sign Service Level agreements (SLAs) with cloud providers and have a business continuity plan in place in order to reduce the downtime.

3	Information leakage of customer information.	The sensitive customer information that may be exposed due to a data breach is the personal information and payment data. This can result in the penalties imposed by the regulators, lawsuits, the crisis of the customer trust and the discouragement of the organization.	Implement good access control measures, data encryption in transit and at rest and frequent security audit and adherence to data protection laws. Deploy solutions of identity and access management (IAM).
4	Insider threat (me malicious or careless worker)	Access rights can be used with ill intent or without intention, and can cause data to be leaked, disrupt the performance of a given system or cause unauthorized alteration of cloud resources. This may lead to a breakdown in operations, security breaches and breach of compliance.	Apply the principle of least privilege, monitor user activity, conduct regular access reviews, and provide staff training on acceptable use and security responsibilities.
5	Natural disaster affecting data center access	A natural disaster such as flooding or fire could impact physical access to cloud data centers or network connectivity, leading to service disruption and potential data unavailability. This could delay business operations and recovery efforts.	Enforce the principle of least privilege, gather and examine the user activity, perform periodic access audits, and train the staff about the acceptable use and its security obligations.
6			
7			

Chapter 2 Business Continuity/Disaster Recovery

2.1 Amazon Web Services (AWS) Backup Policies

AWS offers an all-in-one and very scalable backup infrastructure that helps backup business continuity as well as disaster recovery when working through cloud-based workloads [11]. AWS operates under a shared responsibility model, that is, the cloud provider guarantees the availability of infrastructure but customers built backup policies as necessary depending on their business conditions [12].

AWS provides AWS Backup which is a fully managed backup that gathers and automates all backups across various services within the Amazon AWS such as Amazon EC2, Amazon RDS, and Amazon S3, as well as Amazon EFS. That backup could be on schedule like on hourly, weekly, or monthly; or as scheduled under lifecycle policies. Although AWS does not support full real-time data backup in all services, it allows near real-time data protection using frequent snapshots, point-in-time recovery, and continuous replication of specific services like databases.

It has a BC/DR aspect since AWS prioritizes the geographic backing by allowing backups to be duplicated in several Availability Zones and locations. The solution will safeguard organizations against regional outages and large-sized disasters and will aid in lowering Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Services of AWS back-up are combined with identity and access management (IAM), encryption, and audit logging to make sure the backup information is safe and compliant. On the whole, this backup strategy offered by AWS offers resiliency and flexibility to the institutions with challenging BC/DR needs [13].

---

[11] What is AWS Backup? - AWS Backup
[12] Disaster Recovery of Workloads on AWS: Recovery in the Cloud - Disaster Recovery of Workloads on AWS: Recovery in the Cloud
[13] Disaster Recovery of Workloads on AWS: Recovery in the Cloud - Disaster Recovery of Workloads on AWS: Recovery in the Cloud

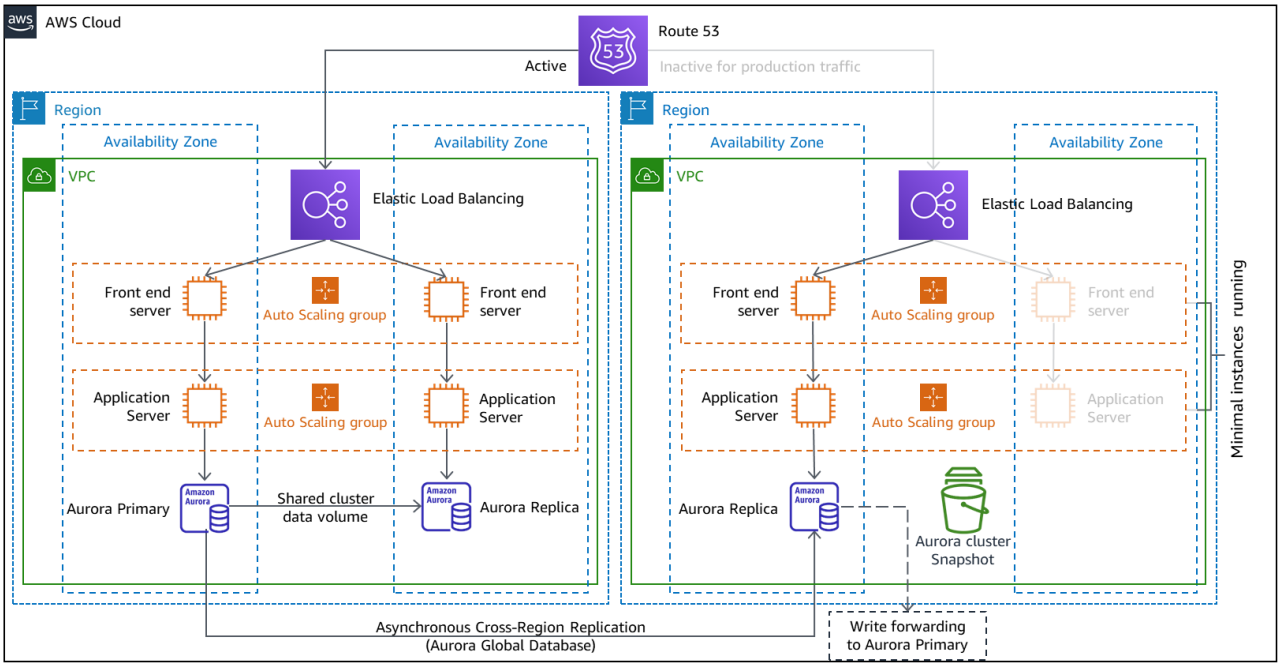

Fig 1: Data backup architecture of AWS

2.2 Microsoft Azure Backup Policies

Microsoft Azure offers a cloud-based backup and recovery environment as well as a disaster recovery system using Azure Backup and Azure Site Recovery. Azure Backup can facilitate companies to carry out automated, scheduled backups of virtual machines, databases, and file systems automatically without the need to involve extra infrastructure [14].

Azure has backup schedules and retention policies that the organizations can customize to recreate the information that is available at a certain time [15]. Whereas Azure does not offer continuous or real-time backmost of every service, it presents almost real-time duplication and automatically unstopped through Azure Site Recovery. This allows the quick restart of workloads in the event of an outage or a disaster situation [16].

Regarding BC/DR, Azure relies on Recovery Services vaults which implement built-in redundancy, encryption of data, and role-based access control, whereby backup data is guarded. Azure also offers the

[14] What is Azure Backup? - Azure Backup | Microsoft Learn
[15] What is Azure Backup? - Azure Backup | Microsoft Learn
[16] What is Azure Backup? - Azure Backup | Microsoft Learn

geo-redundancy of storage, which provides the possibility of backup even in case of the failure of the region [17].

The built-in backup and recovery ecosystem offered by Azure is highly compatible with regulatory and compliance standards, which makes it specifically favorable to the companies whose activities are regulated. Azure also ensures ongoing business processes and reduces downtime by facilitating backup and replication as well as automated recovery processes [18].

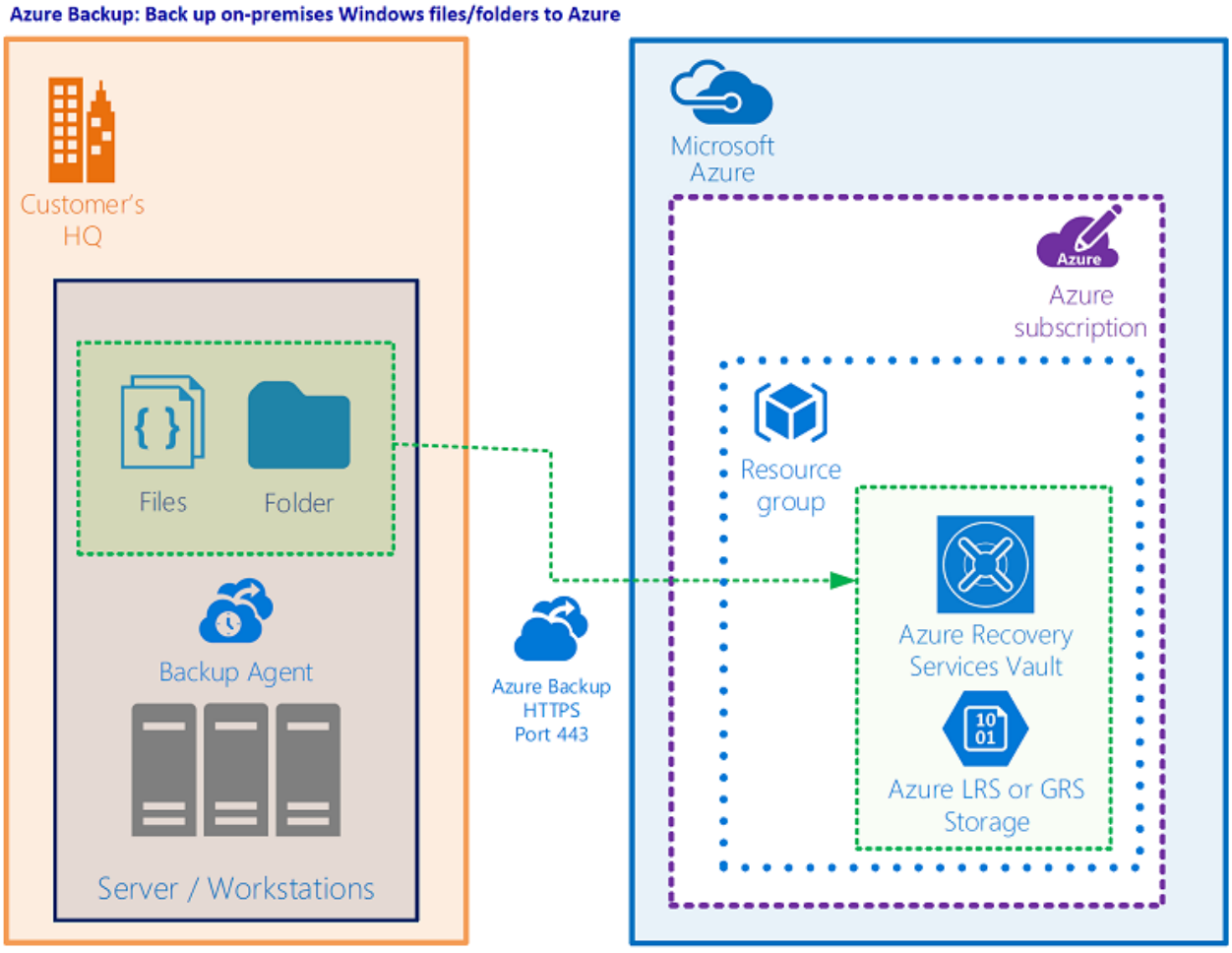

Fig 2: Data backup architecture of Azure.

[17] About Azure Site Recovery - Azure Site Recovery | Microsoft Learn
[18] https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview

2.3 Comparison of Cloud Backup Offerings

This part provides the comparison of the offers proposing backups of the Amazon Web Services (AWS) and Microsoft Azure in terms of bandwidth management of backup, cost model, and data portability. These are the reasons why these factors are significant in determining the appropriateness of cloud backup solution to Business Continuity and Disaster Recovery (BC/DR).

Table 2: Comparison of AWS and Azure Backup Offerings

Feature	Amazon Web Services (AWS)	Microsoft Azure
Backup Type	Scheduled backups, snapshots, point-in-time recovery, near real-time replication for selected services	Scheduled backups, point-in-time recovery, near real-time replication via Azure Site Recovery
Bandwidth for Backups	Optimized snapshot-based backups reduce data transfer by storing incremental changes only	Uses incremental backups and replication to minimize bandwidth consumption
Pricing Structure	Pay-as-you-go based on storage used, backup frequency, and data transfer	Pay-as-you-go based on protected instances, storage consumed, and recovery operations
Scalability	Highly scalable with support for large, multi-region architectures	Scalable and tightly integrated within the Azure ecosystem
Data Portability	Data export supported but migration to other providers may require reconfiguration and additional tools	Supports data export; migration simplified within Microsoft ecosystem but less flexible across providers
BC/DR Suitability	Strong support for complex, multi-region disaster recovery strategies	Well-suited for integrated backup and recovery with simplified management

Chapter 3 Cloud Application Design and Security Components

3.1 Cloud Application and API Overview

On-demand application applications: This is a core element of the current computing world, and it allows users to achieve service and information retrieval on the internet without using the local

infrastructure. Google drive is one of the popular cloud applications that comes in form of a Software as a Service (SaaS) which offers cloud storage facilities, file synchronization and collaboration services.

The most essential functions that the Google Drive API has to offer are the uploading and downloading of files, searching files, managing the metadata, the control of the access permissions and the sharing of the files. To give an example, the API can be used by third-party applications to either automate document uploads, retrieve files to process them or control user access permissions. This makes it compatible with other systems like content management systems, backup systems and workflow automation systems [19].

APIs used in cloud applications increase scalability, interoperability and flexibility. The access to the Google Drive API is authenticated with the help of such authentication schemes as OAuth 2.0, provided that the access to the cloud-based resources is limited to authorized users and apps [20].

Generally, the adoption of APIs in cloud computing project like Google drive illustrates how cloud computing aids safe interaction, automation and scalability of contemporary computing systems.

3.2 Cloud Software Development Lifecycle (SDLC) vs Agile Model

Cloud Software Development Lifecycle Cloud SDLC is a collection of procedures and practice applied in the design, development, deployment and maintenance of applications within the specifics of the cloud environment. In contrast to the older paradigms of software development, Cloud SDLC is configured to be able to scale, deliver continuously, and respond quickly to the changes on the basis of cloud-based technologies, including virtualization, containerization, and automation.

Cloud SDLC is also a process that generally involves requirements examination, plan, code creation, testing, deployment, supervising, and constant enhancements [21]. The main attribute of Cloud SDLC is that it is highly compatible with DevOps and Continuous Integration/Continuous Deployment (CI/CD) practices that can provide automated testing, frequent releases, and real-time monitoring.

Conversely, the Agile model of software development is an iterative, incremental model, which focuses on flexibility, customer involvement, and speedy implementation of working software. Although Cloud SDLC and Agile are similar as they involve the development by iterations as well as continuous

[19] Data Exchange Service using Google Drive API
[20] Secure-and-Efficient-API-Design-for-Next-Generation-Cloud-Computing.pdf
[21] Cloud security engineering: Early stages of SDLC - ScienceDirect

improvement, they are different in their scope. Agile is basically, a development approach and Cloud SDLC is a technology specific approach-based lifecycle model that is designed to be used in cloud-based systems.

3.3 Cloud Architecture Components

The cloud application architecture entails a set of various components interconnected to one another that collaborate to provide scale services, reliability and security. In this section, two important elements that are prominent in a cloud computing set up are Virtual Machines (VMs) and Load Balancers.

3.3.1 Virtual Machines (VMs)

Virtual Machines (VMs) are a fundamental component of cloud architecture, enabling the virtualization of physical computing resources such as CPU, memory, and storage [22]. VMs allow multiple operating systems and applications to run independently on shared physical hardware, improving resource utilization and deployment flexibility. In cloud environments, VMs support scalability by allowing organizations to provision, resize, or terminate instances on demand. They also provide fault isolation, ensuring that failures in one virtual machine do not directly affect others running on the same host. Additionally, VMs integrate with automation tools and Infrastructure as Code (IaC) to support efficient cloud resource management.

3.3.2 Load Balancers

Load balancers are a necessary part of any cloud architecture, and their functions are to allocate any incoming network traffic between several computing resources [23]. Load balancers by balancing the workloads in scheduling the work, they do not work a single server and instead enhance the performance and availability of applications. Load balancers can be used in clouds to enable high availability, and diverting traffic to unhealthy or failed instances by routing traffic to healthy instances. They even support horizontal scaling, when combined with auto-scaling services, which means that one can add and remove resources dynamically, according to the needs. In combination with the virtual machine, the load balancers enable the cloud application to be scalable, reliable and fault tolerant.

---

[22] Virtual machine migration in cloud data centers: a review, taxonomy, and open research issues | The Journal of Supercomputing

[23] Preparation_Instruction

3.4 Identity Management in the Cloud

Load balancers are a necessary part of any cloud architecture, and their functions are to allocate any incoming network traffic between several computing resources. Load balancers by balancing the workloads in scheduling the work, they do not work a single server and instead enhance the performance and availability of applications. Load balancers can be used in clouds to enable high availability, and diverting traffic to unhealthy or failed instances by routing traffic to healthy instances. They even support horizontal scaling, when combined with auto-scaling services, which means that one can add and remove resources dynamically, according to the needs. In combination with the virtual machine, the load balancers enable the cloud application to be scalable, reliable and fault tolerant.

Chapter 4 Legal, Compliance and Risk Governance

4.1 HIPAA Rules and Their Distinctive Characteristics

The HIPAA is a federal statute in the United States that meets the privacy, security, and integrity requirements of medical information that is sensitive and critical. HIPAA defines set standards of processing of Protected Health Information (PHI) by medical organizations, health insurers, and their technology service patients [24]. With cloud computing, HIPAA becomes of special concern in the light of massive adoption of cloud-based solutions in terms of storing, processing, and transferring healthcare data.

HIPAA consists of a few prominent rules, an overwhelming majority of which are the Privacy Rule, the Security Rule, and the Breach Notification Rule [25]. The Privacy Rule provides the way that PHI can be disclosed and utilized so that patients can control their personal health information. The Security Rule is aimed at protecting ePHI (ePHI) by the use of administrative, physical, and technical security measures. Breach notification Rule is an agreement mandating organizations to report breach of information to individual persons and government bodies in case of a PHI breach.

---

[24] Exploring Current Practices and Challenges of HIPAA Compliance in Software Engineering: Scoping Review | IEEE Journals & Magazine | IEEE Xplore

[25] Exploring Current Practices and Challenges of HIPAA Compliance in Software Engineering: Scoping Review | IEEE Journals & Magazine | IEEE Xplore

The industry-specific approach to data protection is one of the major factors that enable the definition of HIPAA as different compared to other regulatory data protection measures. In comparison to other generic data protection regulations like the General Data Protection Regulation (GDPR), HIPAA is used solely in the healthcare-related sectors, and also by their business partners. This limited scope enables HIPAA to deal with the special sensitivity and vulnerability to medical data that may contain detailed personal, financial, and clinical information.

The other important difference is the prescriptive security requirements in HIPAA. HIPAA clearly provides protection in the form of access mechanisms, audit mechanisms, integrity mechanisms, and transmission protection of the electronic health data [26]. Where other rules talk about general principles, HIPAA offers greater specifications of the nature of control that has to be adopted especially in environments that are technology oriented like cloud computing.

There are also differences between HIPAA and other regulatory structures in the enforcement mechanisms. HIPAA privacy breach can attract hefty civil and criminal fines, and penalties depend on the extent of negligence and intent [27]. Through this robust enforcement model, healthcare organizations and cloud service providers are motivated to put an emphasis on compliance and security.

Shared responsibility is something that is brought about by HIPAA compliance in cloud environments. Providers of cloud services with PHI qualify as business associates and have to sign Business Associate Agreements (BAAs) with healthcare organizations. These contracts establish obligations to do with data security, data breach notifications, and data protection measures. Consequently, HIPAA becomes very important in the development of secure handling of healthcare data at cloud entities.

In general, HIPAA is not similar to other data protection laws as it is healthcare-specific, has specific security standards, and strict enforcement measures. Its applicability on cloud computing is also on the increase as the use of cloud services to provide an efficient, scalable, and secure healthcare solution by healthcare organizations increases.

---

[26] A HIPAA Security and Privacy Compliance Audit and Risk Assessment Mitigation Approach: Security & Forensics Book Chapter | IGI Global Scientific Publishing

[27] HIPAA PRIVACY: Liability Beyond Regulatory Enforcement | Journal of Healthcare Finance

4.2 SOC 1, SOC 2 and SOC 3 Reports

Service Organization Control (SOC) reports are also independent assurance reports that were created by the American Institute of Certified Public Accountants (AICPA) in assessing controls among service organizations. Such reports are especially important in cloud computing systems that customers are relying on third parties to operate key systems and information. The SOC 1, SOC 2, and SOC 3 reports are different in terms of scope, purpose, and target audience.

Table 3: Comparison of SOC 1, SOC 2 and SOC 3 Reports

Feature	SOC 1	SOC 2	SOC 3
Primary Focus	Controls relevant to financial reporting	Controls related to trust services criteria	Summary of SOC 2 controls
Trust Services Criteria	Not applicable	Security, availability, processing integrity, confidentiality, privacy	Same criteria as SOC 2 (high-level)
Intended Audience	User entities and auditors	Management, customers, regulators	General public
Level of Detail	Detailed description of financial controls	Detailed description of system and controls	High-level summary only
Use in Cloud Computing	Financial transaction assurance	Information security and compliance assurance	Marketing and transparency
Distribution	Restricted	Restricted	Publicly available

4.3 Risk Appetite vs Risk Tolerance

Stakeholder Organizational risk management is fundamentally based on risk appetite and risk tolerance which determine how much risk an organization will take to achieve its goals. The concepts are used interchangeably but are actually different facets of governance and decision making especially in technology driven habitats like cloud computing.

Risk appetite is the general magnitude and nature of the risk an organization has chosen to assume in order to meet its strategic objectives. It is a top-level statement determined by the senior management or the board of directors and expresses strategic priorities of the organization, the culture of risk and long-term objectives. The more risk-taking organizations might even be more willing to work with

developing cloud technologies sooner in order to obtain an advantage, even though the risk of loss or exposure is greater [28].

Conversely, risk tolerance is the specified value of variability of certain goals during the handling of individual risks. Risk tolerance is a working concept that is applied on the process or activity level which establishes some measurable boundaries indicated by the threshold of unacceptable risks, which necessitate action to be taken. As an illustration, an organization can come up with hard tolerances of acceptable downtime in the cloud-hosted services [29].

The major distinction between risk plus and risk tolerance is their staff and use. Risk appetite is a strategic and long-term risk-taking behavior whereas risk tolerance is tactical and measurable, which helps the risk manager make decisions on day-to-day risk management. This is a key difference to be understood when using cloud computing as a provider that organizations need to prioritize innovation over security and regulatory compliance.

[28] Risk appetite: A crucial consideration for effective board risk o...: Ingenta Connect
[29] Making sense of risk tolerance criteria - ScienceDirect

Chapter 5 Conclusion

This portfolio has taken a critical look at some of the most important elements of cloud computing which are the models of service, business continuity, application architecture, security and compliance with regulations. Infrastructure as a service, platform as a service, and software as service analysis revealed that various models of clouds can support the needs of different organizations by adopting different business and revenue models. The role of proactive risk management was emphasized through the Business Impact Analysis, and the assessment of the backup and disaster recovery plan demonstrated how the leading cloud providers ensure business continuity. On the whole, what establishes the portfolio is the fact that successful cloud adoption demands an equitable combination of technology, security and governance to introduce operational stability and sustainability in an organization.