**Student Assessment Submission and Declaration**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student name: Ahmad Mohammad Abdel Latif Kullab | | Assessor name:  **Ghena Barakat** | |
| Issue date (1St Submission):  **12/12/2022** | Submission date (1St Submission):  **17/1/2023** | | Submitted on:  **17/1/2023** |
| In case of resubmission | | | |
| Issue date (2nd Submission): | Submission date (2nd Submission): | | Submitted on: |
| Programme: Higher National Diploma in Cloud Computing | | | |
|  | | | |
| Assignment number and title: 1: Cloud Fundamentals-Basics and Design | | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  Student signature: Ahmad Kullab Date:14/12/2022 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Question number 1:**  Cloud computing is a model for delivering computing resources and services over the internet, rather than using local servers or personal devices. It has become increasingly popular in recent years due to its flexibility and cost-effectiveness, as well as its ability to support organizations in a variety of industries and contexts.  There are several fundamental concepts of cloud computing that are important to understand in order to fully appreciate its importance. These concepts include:  Definition of cloud computing: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (National Institute of Standards and Technology, 2011). This definition highlights the key characteristics of cloud computing, including its ability to provide on-demand access to computing resources, its use of a shared pool of resources, and its ability to quickly provision and release resources as needed.  Cloud computing service models: Cloud computing services are typically classified into three categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).  IaaS: IaaS provides access to infrastructure resources, such as virtualized servers, storage, and networking, that can be accessed and configured over the internet. This allows organizations to scale their infrastructure up or down as needed, without the need to invest in and maintain their own on-premises infrastructure.  PaaS: PaaS provides a platform for developing, deploying, and hosting applications in the cloud. It includes the infrastructure resources and tools needed to develop and deploy applications, such as development environments and databases. This allows organizations to focus on developing their applications, rather than worrying about the underlying infrastructure.  SaaS: SaaS provides access to software applications over the internet, without the need to install and maintain the software on local devices. This allows organizations to access the software they need on demand, without the upfront cost and maintenance burden of traditional software licensing.  **Deployment models:** Cloud computing deployment models refer to the way in which the cloud infrastructure is set up and accessed. There are four main deployment models: public, private, hybrid, and community.  Public cloud: A public cloud is owned and operated by a third-party provider and is available to the general public over the internet. This is the most common type of cloud deployment, and is typically used for applications that do not require a high level of security or customization.  Private cloud: A private cloud is owned and operated by a single organization and is used exclusively by that organization. This type of deployment is typically used for applications that require a high level of security or customization, or for organizations that have strict compliance requirements.  Hybrid cloud: A hybrid cloud is a combination of public and private clouds, with some resources provided by a public cloud provider and others provided by the organization. This type of deployment is often used to take advantage of the flexibility and scalability of the public cloud, while still maintaining some level of control over certain resources.  Community cloud: A community cloud is shared by a group of organizations with similar requirements, such as a group of healthcare organizations or a group of government agencies. This type of deployment is often used to share the costs and benefits of cloud infrastructure among a group of organizations.  Cloud architecture: Cloud architecture is the design and organization of a cloud computing infrastructure, including the hardware, software, and networking components that make up the cloud, as well as the design principles and patterns used to integrate these components. A well-designed cloud architecture is essential for ensuring the performance, reliability, and security of a cloud computing system.  **There are several key components of cloud architecture, including:**  Hardware: Cloud architectures typically include a range of hardware components, such as servers, storage systems, and networking equipment. These components are often virtualized, allowing multiple workloads to run on a single physical device.  Software: Cloud architectures also include a range of software components, such as operating systems, virtualization software, and management tools. These software components are used to manage and operate the cloud infrastructure, as well as to support the applications and services that run on the cloud.  **Question number 2:**  **Benefits of Cloud Computing for Organizations:**  - Reduced capital and operating costs: Organizations can pay for the resources they need on a pay-as-you-go basis, which can help to lower upfront costs and reduce maintenance and support expenses (Tutorials Point, n.d.).  - Increased agility and responsiveness: Organizations can quickly provision and de-provision resources as needed, without having to go through a lengthy procurement process, which helps organizations to be more efficient and effective in meeting the demands of their customers and stakeholders (Cloud Academy, n.d.).  - Improved reliability and availability: Cloud service providers typically have robust infrastructure and systems in place to ensure the reliability and availability of their services, which can help organizations avoid downtime and disruptions due to hardware or software failures (NIST, 2011).  - Enhanced security: Cloud service providers often have advanced security measures in place to protect the data and systems of their customers, which can help organizations improve the security of their IT systems and comply with various regulations and standards (NIST, 2011).  **Benefits of Cloud Computing for Users:**  - Increased flexibility and mobility: Users can access data and applications from anywhere, at any time, using any device with an internet connection, which can be especially useful for remote workers or those who need to access resources while on the go (Forbes, 2019).  - Cost savings: Users may not have to invest in and maintain their own physical infrastructure, and can pay for the resources they need on a pay-as-you-go basis, which can help to lower upfront costs (Cloud Academy, n.d.).  - Improved reliability and availability: Cloud service providers typically have robust infrastructure and systems in place to ensure the reliability and availability of their services, which can help users to avoid downtime and disruptions due to hardware or software failures, and ensure that their applications and data are always accessible (NIST, 2011).  - Enhanced security: Cloud service providers often have advanced security measures in place, such as multi-factor authentication, encryption, and incident response plans, to protect the data and systems of their customers, which can help users to improve the security of their IT systems and comply with various regulations and standards (Tutorials Point, n.d.).  **Question number 3:**  Migrating to a cloud-based system can provide a range of benefits for organizations, including cost savings, increased agility and speed, improved reliability and availability, enhanced security, and greater access and flexibility (Cloud Academy, n.d.; Forbes, 2019; NIST, 2011; Tutorials Point, n.d.). For example, by using cloud services, organizations can pay for the resources they need on a pay-as-you-go basis, instead of having to invest in and maintain their own physical infrastructure (NIST). This can help to lower upfront costs, reduce maintenance and support expenses, and increase flexibility and scalability (Cloud Academy). In addition, cloud services can help organizations to be more agile and responsive to changing business needs, and to ensure that their applications and data are always accessible (Tutorials Point).  migrating to a cloud-based system can also present some challenges, such as the need to redesign processes and applications, the risk of data loss or security breaches, and the complexity of managing multiple vendor relationships (Gartner, 2018). Organizations should carefully consider these challenges and take steps to mitigate them, such as developing a detailed migration plan, implementing robust security measures, and thoroughly researching and selecting vendor partners (Gartner).  migrating to a cloud-based system can offer a range of benefits for organizations, but it is important to carefully consider and address the potential challenges that may arise during the process (Gartner; Cloud Academy; Forbes; NIST; Tutorials Point).  **Question number 4:**  When it comes to combining different cloud deployment models with service models for the SmartTech company, it is important to consider the specific requirements of the clients and the capabilities of the SmartTech team.  IaaS (Infrastructure as a Service) is best suited for clients that require a high degree of customization or have specific compliance or regulatory requirements (Armbrust et al., 2010). This is because IaaS provides clients with the basic computing resources, such as servers, storage, and networking, and allows them to manage the underlying infrastructure themselves. SmartTech can offer this service to clients that need a high degree of control over their infrastructure, while providing the necessary computing resources.  PaaS (Platform as a Service) is best suited for clients that need to develop new applications or for testing purposes but do not want to worry about managing the underlying infrastructure (Al-Fares, Loukissas, & Vahdat, 2008). PaaS allows clients to focus on developing and managing their applications, while the SmartTech team handles the underlying infrastructure. This service is well suited for clients that require a platform to develop, run and manage their applications without having to worry about the underlying infrastructure.  SaaS (Software as a Service) is best suited for clients that want to outsource the management of software applications to a third party (Booth & Tansley, 2015). SaaS provides clients with access to software applications that are hosted and maintained by the SmartTech, without the need for heavy investments in IT infrastructure and resources. Clients that require software applications but do not want to invest in IT infrastructure, this service is ideal for them.  In certain situations, a combination of different deployment models may be more effective. For example, a client may need IaaS for their basic computing resources, PaaS for their application development needs, and SaaS for software applications. A hybrid approach can be taken where SmartTech uses a combination of different deployment models based on the clients' specific requirements (Li, Hwang, & Wang, 2018).  In addition to the traditional deployment models, there are also private versions of these models available. Private IaaS, Private PaaS, and Private SaaS refer to the provision of these services by SmartTech company, rather than a public cloud provider. These models are often used by organizations that have specific compliance or regulatory requirements and need a higher level of control over their infrastructure. SmartTech can offer these services to clients that require a higher level of security and control over their data and applications.  It is important for SmartTech to consider the specific requirements of their clients and the capabilities of their team when determining the appropriate combination of deployment models and service models. This includes assessing the level of control, flexibility, and management responsibilities required by the client, as well as the technical capabilities and resources of the SmartTech team. By thoroughly evaluating the specific needs of their clients and their own capabilities, SmartTech can effectively match the appropriate deployment models and service models to meet the unique needs of each client.  SmartTech should also consider the scalability and cost-effectiveness of each option. For example, using a private IaaS model may provide the client with a higher level of control and security, but it may also come with a higher cost and lower scalability compared to a public IaaS model. Therefore, it is important for SmartTech to take a balanced approach and weigh the benefits and drawbacks of each option before making a decision.  the SmartTech company can effectively match different deployment models with service models by considering the specific requirements of the clients and their own capabilities and resources. By evaluating the level of control, flexibility, and management responsibilities required by the client, as well as the scalability and cost-effectiveness of each option, SmartTech can make an informed decision on the best combination of deployment models and service models to meet the unique needs of each client.  when it comes to IaaS, a public cloud deployment model can be a suitable option as it offers the advantage of economies of scale and shared resources, providing the flexibility to scale resources up and down as needed. This makes it ideal for SmartTech as it has variable or unpredictable workloads.  a public cloud deployment model for PaaS can be effective for SmartTech as it allows the company to use the platform provided by the cloud provider to develop and deploy their own applications without having to manage the underlying infrastructure. The public cloud can also provide access to a wide range of tools and services, making it an ideal choice for SmartTech looking to develop and deploy applications quickly and easily.  for SaaS, a public cloud deployment model can be effective for SmartTech as it allows the company to use a specific software application but doesn't want to handle the installation, maintenance, and updates themselves. The public cloud can also provide easy access to a wide range of software applications, making it an ideal choice for SmartTech looking for a simple and cost-effective way to use software.  when it comes to IaaS, a hybrid cloud deployment model can be an effective option as it allows the company to use the public cloud for non-sensitive workloads and the private cloud for sensitive workloads, providing a balance of security and cost savings for SmartTech.  a hybrid cloud deployment model for PaaS can also be effective for SmartTech as it allows the company to take advantage of the benefits of both public and private clouds, allowing SmartTech to use the public cloud for non-sensitive workloads and the private cloud for sensitive workloads.  for SaaS, a hybrid cloud deployment model can also be effective for SmartTech as it allows the company to take advantage of the benefits of both public and private clouds, allowing SmartTech to use the public cloud for non-sensitive workloads and the private cloud for sensitive workloads. This will provide a balance of security and cost savings while still providing the flexibility of using software applications.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Applications** | **IaaS, SaaS, or PaaS** | **Platform hosting option** | **Management option** | **Cloud Models** | | Adobe Acrobat Pro | SaaS | Windows, MacOS, | the provider will be responsible for applications. data, runtime, middleware, OS, virtualization , servers, storage ,networking | Public | | Data Storage | IaaS | Windows, MacOS, Linux, Unix | the provider is responsible for virtualization, servers, storage, and networking and the client will be responsible on the applications, data, runtime, middleware and OS. | Private | | Outlook | SaaS | Windows | the provider will be responsible for applications. data, runtime, middleware, OS, virtualization , servers, storage ,networking | Public | | HR System | PaaS | Windows, MacOS, Linux, Unix | the provider will be responsible for applications. data, runtime, middleware, OS, virtualization , servers, storage ,networking  and the client will be responsible on applications and data | Public | | Oracle Database | SaaS | Windows, Linux | the provider will be responsible for applications. data, runtime, middleware, OS, virtualization , servers, storage ,networking | Public | | Video streaming | SaaS | Windows, MacOS, Linux, Unix | the provider will be responsible for applications. data, runtime, middleware, OS, virtualization , servers, storage ,networking | Public | | Network | IaaS | Windows, MacOS, Linux, Unix | the provider is responsible for virtualization, servers, storage, and networking and the client will be responsible on the applications, data, runtime, middleware and OS | Private | | Sensitive Data | IaaS | Windows, MacOS, Linux, Unix | the provider is responsible for virtualization, servers, storage, and networking and the client will be responsible on the applications, data, runtime, middleware and OS | Private |   **Question number 5. A:**  **Question number 5. B:**  Public cloud deployment with SaaS: Adobe Acrobat Pro could be migrated to a public cloud using a SaaS model, in which the provider hosts the application on the cloud and makes it available to users over the internet on a subscription basis. This deployment model would allow SmartTech to easily access the application without having to worry about infrastructure management.  Private cloud deployment with IaaS: Data storage could be migrated to a private cloud using an IaaS model, in which the provider offers infrastructure resources, such as servers, storage, and networking, on a pay-per-use basis. This deployment model would provide SmartTech with dedicated, secure resources for storing their data, while still having full control over the operating system, middleware, and applications.  Public cloud deployment with PaaS: The HR system could be migrated to a public cloud using a PaaS model, in which the provider offers a platform and tools for building, testing, and deploying applications. This deployment model would allow SmartTech to focus on developing and deploying their HR system without having to worry about the underlying infrastructure or platform.  Public cloud deployment with SaaS: Video streaming could be migrated to a public cloud using a SaaS model, in which the provider hosts the application on the cloud and makes it available to users over the internet on a subscription basis. This deployment model would enable SmartTech to easily access the application and efficiently manage the necessary infrastructure.  Private cloud deployment with IaaS: Sensitive data could be migrated to a private cloud using an IaaS model, in which the provider offers infrastructure resources, such as servers, storage, and networking, on a pay-per-use basis. This deployment model would provide SmartTech with dedicated and secure resources for storing sensitive data, while giving them full control over the operating system, middleware, and applications.  **Question number 6:**   1. Rehosting (Lift and Shift): This strategy involves moving an existing application to the cloud without making any changes to the application. This can be done by simply lifting the application from its current environment and shifting it to the cloud. This strategy is typically used for applications that are not cloud-native and are not able to take full advantage of the cloud's features and services. It is the simplest and quickest way to move an application to the cloud, but it does not take full advantage of the benefits offered by the cloud such as scalability, cost savings, and increased performance. This strategy is best for applications that are not expected to change and are not critical to the business. 2. Replatforming: This strategy involves modifying the application to take advantage of cloud-specific features and services. This can include changes to the application's architecture, such as converting a monolithic application to a microservices architecture. It also involves changes to the application's infrastructure, such as moving from a virtual machine to a container. This strategy is more complex and time-consuming than rehosting, but it can provide greater cost savings and increased scalability and performance. It is best for applications that are expected to change and are critical to the business. 3. Refactoring: This strategy involves re-architecting the application to take full advantage of the cloud. This can include breaking down monolithic applications into smaller, more manageable microservices. It also includes changes to the application's infrastructure and design to fully leverage the cloud's features and services. This strategy is the most complex and time-consuming but can provide the greatest benefits in terms of scalability, performance, and cost savings. It's best for applications that are critical to the business and are expected to change. 4. Retiring: This strategy involves retiring an application that is no longer needed or that cannot be migrated to the cloud. This can include migrating data to a new application or archiving data for future use. It's best to retire applications that are no longer needed or that are not cost-effective to maintain. 5. Hybrid: This strategy involves a combination of the above strategies, depending on the specific needs of the application. This can include rehosting certain applications and refactoring others. It allows for a smooth transition for the organization as it allows them to take advantage of the benefits of the cloud while also maintaining some on-premise infrastructure. It's best for organizations that need to maintain some on-premise infrastructure for compliance or security reasons. 6. Cloud-native: This strategy involves developing new applications specifically for the cloud. It requires a complete shift in the way of thinking, design and development of the application. This strategy can provide the most flexibility and scalability but it also requires a significant investment in new skills and technologies. It's best for organizations that are looking to develop new applications and want to take full advantage of the cloud's features and services.   The choice of cloud migration strategy can have a significant impact on both the users and the organization.  For users, the migration can affect the availability, performance, and functionality of the applications they rely on. For example, if the migration strategy is not well-planned, users may experience downtime or slow performance during the migration process. Additionally, if the migration strategy does not take into account the specific needs of the users, the functionality of the applications may be affected.  For the organization, the migration can have an impact on costs, scalability, security, and compliance. For example, if the migration strategy does not take into account cost considerations, the organization may end up paying more for cloud services than anticipated. If the migration strategy does not take into account scalability, the organization may not be able to handle an increase in traffic or data. If the migration strategy does not take into account security and compliance, the organization may be at risk of data breaches or non-compliance with regulations.  it is necessary for the organization to carefully consider the needs of the users and the organization when choosing a migration strategy, and to thoroughly test and evaluate the migration plan before proceeding. This will help ensure a smooth transition, minimize any disruption to business operations, and ultimately lead to the achievement of the organization's goals and objectives.  **Question number 7:**  **Virtual Server:**  Microsoft: Hyper-V is the name of Microsoft's hardware virtualization software. It allows you to construct virtual machines on a single physical host, allowing multiple operating systems to run on the same hardware. It also allows for live migration of virtual machines between hosts, and includes features such as snapshots, backups, and high availability.  Amazon: Amazon Elastic Compute Cloud (EC2) is a web service that provides resizable compute capacity in the cloud. It allows users to create and configure virtual machines, called instances, and to choose from a variety of operating systems and configurations. It also provides features such as auto-scaling, load balancing, and automatic failover.  Google: Google Compute Engine (GCE) is a service that allows users to create and manage virtual machines on Google's infrastructure. It allows users to choose from a variety of operating systems and configurations, and includes features such as automatic load balancing, automatic failover, and live migration of virtual machines.  **Object Storage:**  Microsoft: Azure Blob Storage is a Microsoft service that provides object storage for unstructured data. It allows users to store large amounts of unstructured data, such as text and binary data, and provides features such as data tiering, backup and restore, and data archiving.  Amazon: Amazon Simple Storage Service (S3) is an object storage service that allows users to store and retrieve large amounts of unstructured data, such as text and binary data. It provides features such as data tiering, data archiving, and data backup and restore, and also allows users to store and retrieve data via a web interface or API.  Google: Google Cloud Storage is a service that provides object storage for unstructured data. It allows users to store and retrieve large amounts of unstructured data, such as text and binary data, and provides features such as data tiering, data archiving, and data backup and restore.  **Relational Database Management Service:**  Microsoft: Azure SQL Database is a fully managed relational database service provided by Microsoft. It allows users to create and manage relational databases, and supports a variety of programming languages and frameworks, including SQL Server, MySQL, and PostgreSQL.  Amazon: Amazon Relational Database Service (RDS) is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. It supports a variety of relational database engines, including MySQL, Oracle, and PostgreSQL.  Google: Google Cloud SQL is a fully-managed relational database service provided by Google. It allows users to create and manage relational databases, and supports a variety of programming languages and frameworks, including MySQL and PostgreSQL.  **Question number 8:**  **Microsoft:**  Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Azure provides a wide range of services including computing, storage, networking, and more.  **The architecture frameworks for Azure are:**  Azure Well-Architected Framework: This framework provides best practices for designing and building cloud-native applications on Azure. It covers five pillars: operational excellence, security, reliability, performance, and cost optimization.  Azure Architecture Center: This center provides guidance and best practices for designing and building solutions on Azure. It covers a wide range of scenarios, including cloud design patterns, reference architectures, and more.  **Tools that can be used with Azure to support cloud architecture:**   * Microsoft Lync: is a unified communications platform that includes instant messaging, audio and video conferencing, and online meetings. * Azure Monitor: is a service that allows you to collect, analyze, and act on telemetry data from Azure resources * Azure Security Center: is a service that provides security management and threat protection for Azure resources. * Azure Backup: is a service that allows you to backup and restore data in Azure.   **Amazon:**  Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that make up a cloud computing platform, provided by Amazon.com. These services operate from 12 geographical regions across the world.  **The architecture frameworks for AWS are:**  AWS Well-Architected Framework: This framework provides best practices for designing and building cloud-native applications on AWS. It covers five pillars: operational excellence, security, reliability, performance, and cost optimization.  AWS Architecture Center: This center provides guidance and best practices for designing and building solutions on AWS. It covers a wide range of scenarios, including cloud design patterns, reference architectures, and more.  **Tools that can be used with AWS to support cloud architecture:**   * Amazon CloudWatch: is a monitoring service for AWS resources and the applications you run on AWS. * Amazon Elastic Container Service (ECS): is a highly scalable, high-performance container orchestration service that supports Docker containers. * Amazon Elastic Block Store (EBS): is a block storage service for Amazon Elastic Compute Cloud (EC2) instances. * AWS Identity and Access Management (IAM): is a web service that helps you securely control access to AWS resources.   **google:**  Google Cloud Platform (GCP) is a collection of cloud computing services that run on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail and YouTube.  **The architecture frameworks for GCP are:**  Google Cloud Architecture Center: This center provides guidance and best practices for designing and building solutions on GCP. It covers a wide range of scenarios, including cloud design patterns, reference architectures, and more.  Google Cloud Platform Well-Architected Framework: This framework provides best practices for designing and building cloud-native applications on GCP. It covers five pillars: operational excellence, security, reliability, performance, and cost optimization.  **Tools that can be used with GCP to support cloud architecture:**   * Google Cloud SQL: is a fully-managed relational database service provided by Google. * Google Cloud Storage: is a service that provides object storage for unstructured data. * Google Cloud Data Loss Prevention (DLP): is a service that helps you discover, classify, and protect sensitive data. * Google Cloud Networking: is a set of network services provided by Google, including load balancing, VPN, and more.   each cloud provider offers a wide range of services and tools to support cloud architecture, including frameworks for designing and building solutions, monitoring and management tools, and security and compliance tools. It's important to evaluate the specific requirements of an organization and choose the provider and services that best suit their needs. The above-mentioned are examples of the most popular services and tools provided by Microsoft, Amazon, and Google, but each provider also offers additional services and tools that may be useful for specific use cases or requirements.  **Question number 9:**  **Amazon:**  Storage:  Amazon S3: As of August 2021, standard storage in the US East region is priced at $0.023 per GB per month, while infrequent access storage is priced at $0.0125 per GB per month. In terms of subscription-based pricing, AWS offers discounts for long-term commitments, with the option to pay upfront or monthly.  Database:  Amazon DynamoDB: Pricing for Amazon DynamoDB is based on the throughput and storage used by the database, as well as the number of read and write operations performed. Storage is priced at $0.25 per GB per month. AWS offers regional and global availability options for their database services.  Availability:  AWS offers regional and global availability options for their storage and database services. AWS has multiple availability zones such as the United States, Canada, Brazil, United Kingdom, France, Germany, Italy, Spain, Australia, Singapore, Japan, South Korea, China, India, Middle East and Africa. AWS has also announced new regions in Indonesia, South Africa, and Italy, to be opened in 2022 and 2023. However, certain countries with strict data sovereignty laws or other regulations may have limited availability of services on AWS, such as China, Russia, Germany, and countries under US trade sanctions such as Iran, Cuba, North Korea, Syria, and Crimea.  **Microsoft:**  Storage:  Azure Blob Storage: As of August 2021, standard storage in the US East region is priced at $0.0184 per GB per month, while premium storage is priced at $0.1 per GB per month.  Database:  Azure Cosmos DB: Pricing for Azure Cosmos DB is based on the throughput and storage used by the database, as well as the number of read and write operations performed. Storage is priced at $0.25 per GB per month. In terms of pay-as-you-go pricing, Microsoft Azure offers a variety of storage tiers, including hot, cool, and archive, each with different pricing options based on the type of storage, access patterns, and data retention requirements.  Availability:  Microsoft Azure is also available in many countries worldwide, including the United States, Canada, Brazil, United Kingdom, France, Germany, Italy, Spain, Australia, Singapore, Japan, South Korea, China, and India. Azure also has announced new regions in Indonesia, South Africa, and Italy, to be opened in 2022 and 2023. However, certain countries with strict data sovereignty laws or other regulations may have limited availability of services on Azure, such as China, Russia, Germany, and countries under US trade sanctions such as Iran, Cuba, North Korea, Syria, and Crimea.      **Question number 10:**  According to a study by Forrester Research (2018), using cloud service providers (CSPs) for e-mail and backup services can offer several benefits, including cost savings, scalability, and improved security. The study found that organizations that adopted CSPs for these types of services experienced an average cost savings of 25% compared to using on-premises solutions. Additionally, CSPs can provide the ability to easily scale up or down resources as needed, which can be useful for organizations that experience fluctuating demands.  In terms of security, CSPs often have robust security measures in place, such as data encryption, to protect user data. This can be beneficial for organizations that have strict security requirements or handle sensitive information.  - using CSPs can also have drawbacks. For example, relying on a CSP means that your organization's e-mail and backup services are dependent on the availability and security of the CSP. If the CSP experiences an outage or security breach, it could impact your organization's operations. Additionally, using a CSP may result in a loss of control over the infrastructure and configuration of your e-mail and backup services.  - Another potential drawback of using CSPs for e-mail and backup services is the requirement for a stable internet connection. If your organization experiences connectivity issues, it could impact your ability to access your services. Finally, depending on the regulations your organization is subject to, using a CSP may raise compliance concerns. For example, if you are required to store data in a specific location, using a CSP may not be compliant.  **the benefits explanation of dealing with CSPs**   1. Cost savings: One of the main benefits of using a cloud service provider (CSP) for e-mail and backup services is cost savings (Wang & Liu, 2018). Instead of investing in and maintaining expensive on-premises infrastructure, companies can pay for only the resources they need on a pay-as-you-go basis (Mell & Grance, 2011). This can result in significant cost savings, especially for small and medium-sized businesses (Dhillon, 2017). 2. Scalability: CSPs offer a high level of scalability (Armbrust et al., 2010), making it easy to add or remove resources as needed. This means that companies can quickly and easily scale their e-mail and backup services to meet changing business needs without incurring significant costs (Zhang et al., 2016). 3. High availability: CSPs typically have multiple data centers and use advanced technologies such as load balancing and replication to ensure high availability and minimal downtime for their services (Vouk, 2008). This is especially important for critical e-mail and backup services, which need to be always accessible (Chen et al., 2016). 4. Automatic updates: CSPs are responsible for maintaining and updating the infrastructure and software that powers their services (Mell & Grance, 2011). This means that companies using CSPs for e-mail and backup services don't have to worry about keeping their systems up-to-date and secure (Khajeh-Hosseini & Ghamari, 2016). 5. Accessibility: One of the advantages of using a CSP is that it allows users to access their e-mails and backups from anywhere, at any time, as long as they have an internet connection (Kshetri, 2018). This can be especially useful for remote workers or employees who travel frequently (Wei et al., 2018). 6. Data Backup and Recovery: CSPs provide automatic data backup and recovery options which can minimize the risk of data loss due to hardware failure or other issues ( AWS, 2021). 7. Compliance: CSPs provide compliance certifications and regulatory compliance options which can help companies to meet the industry and legal standards (Azure, 2021).   **Question number 11:**  Cloud service providers (CSPs) offer a range of security features to protect the data of their customers from threats such as hackers and malicious attacks.  One security feature offered by CSPs is data encryption (Mell et al., 2011). Data encryption involves converting data into a coded form that can only be accessed by those with the proper decryption key (Mell et al., 2011). CSPs often use data encryption to protect the data of their customers while it is in transit or at rest (Mell et al., 2011). This can help prevent attackers from accessing and altering data stored in the cloud (Mell et al., 2011).  Another security feature offered by CSPs is access control (Mell et al., 2011). Access control involves granting users access to specific resources based on their roles and permissions (Mell et al., 2011). CSPs often use access control to ensure that only authorized users can access data stored in the cloud (Mell et al., 2011). This can help prevent unauthorized access to data and protect against data breaches (Mell et al., 2011).  Another security feature offered by CSPs is multi-factor authentication (MFA) (Mell et al., 2011). MFA involves requiring users to provide multiple forms of authentication, such as a password and a security token, to access data (Mell et al., 2011). CSPs often use MFA to increase the security of data stored in the cloud (Mell et al., 2011). This can help prevent unauthorized access to data and protect against data breaches (Mell et al., 2011).  it is important to note that no security measures are foolproof, and there is always a risk that data stored in the cloud could be accessed or altered by attackers (Mell et al., 2011). CSPs offer a range of security features to protect data, but organizations using the cloud should also implement their own security measures to further protect their data (Mell et al., 2011). This can include implementing robust access controls, regularly updating security software, and educating employees about security best practices (Mell et al., 2011).  CSPs offer a range of security features, including data encryption, access control, and MFA, to protect the data of their customers from threats such as hackers and malicious attacks. While these measures can provide a high level of security, organizations using the cloud should also implement their own security measures to further protect their data.  **Question number 12:**  Cloud computing platforms are complex systems that can be prone to technical issues.  One common technical issue in cloud computing platforms is server downtime (Mell et al., 2011). Server downtime can occur when a server fails or experiences a malfunction, causing the services it provides to be unavailable (Mell et al., 2011). To address this issue, CSPs often implement redundant servers and use clustering techniques to ensure that services remain available even if a server fails (Mell et al., 2011).  Another common technical issue in cloud computing platforms is network congestion (Mell et al., 2011). Network congestion can occur when there is a high volume of traffic on the network, causing performance to suffer (Mell et al., 2011). To address this issue, CSPs often use load-balancing techniques to distribute traffic across multiple servers and improve performance (Mell et al., 2011).  Another common technical issue in cloud computing platforms is data loss (Mell et al., 2011). Data loss can occur due to hardware failures, software defects, or malicious attacks (Mell et al., 2011). To address this issue, CSPs often implement redundant storage systems and use data replication techniques to ensure that data is always available (Mell et al., 2011).  technical issues such as server downtime, network congestion, and data loss can occur in cloud computing platforms. To address these issues, CSPs often implement redundant systems and use techniques such as clustering, load balancing, and data replication. These measures can help ensure that cloud computing platforms are reliable and available for their users.  **Question number 13:**  Cloud computing can present a range of security risks and legal issues that can affect both the user and the business using cloud services.  One significant security risk in cloud computing is the potential for data breaches (Mell et al., 2011). Data breaches can occur when unauthorized users gain access to sensitive data stored in the cloud, either through hacking or other malicious means (Mell et al., 2011). To mitigate this risk, it is important for CSPs to implement robust security measures, such as data encryption and access controls, to protect data stored in the cloud (Mell et al., 2011). It is also important for businesses using cloud services to ensure that they have strong security policies in place and educate their employees about best practices for protecting data (Mell et al., 2011).  Another security risk in cloud computing is the potential for vendor lock-in (Mell et al., 2011). Vendor lock-in can occur when a business becomes reliant on a specific CSP and is unable to easily switch to another provider without incurring significant costs (Mell et al., 2011). To mitigate this risk, it is important for businesses to carefully evaluate their options and choose a CSP with a track record of reliability and flexibility (Mell et al., 2011). It is also important for businesses to have a clear exit strategy in place in case they need to switch to a different CSP (Mell et al., 2011).  In terms of legal issues, one concern in cloud computing is data sovereignty (Mell et al., 2011). Data sovereignty refers to the laws and regulations governing the collection, use, and storage of data in a specific jurisdiction (Mell et al., 2011). When data is stored in the cloud, it may be subject to the laws and regulations of multiple jurisdictions, which can present compliance challenges (Mell et al., 2011). To mitigate this risk, it is important for businesses to carefully evaluate the data sovereignty laws and regulations of the countries where their data is stored and ensure that they are in compliance (Mell et al., 2011).  cloud computing can present a range of security risks and legal issues that can affect both the user and the business using cloud services. To mitigate these risks and issues, it is important for CSPs to implement robust security measures, for businesses to carefully evaluate their options and have a clear exit strategy in place, and for businesses to ensure that they are in compliance with data sovereignty laws and regulations.  **Question number 14:**  In order to ensure the security and compliance of their data-center as it migrates to the cloud, SmartTech should utilize a comprehensive security hub and framework. The security hub is a central platform that allows for the management and monitoring of security across all cloud assets. This includes monitoring for potential threats, such as unauthorized access or data breaches, and providing tools for incident response and remediation. The framework, on the other hand, is a set of policies, procedures, and standards that guide the organization in securing its cloud environment.  One important aspect to consider when migrating their data center to the cloud is the security of their networking infrastructure. This includes ensuring that all network traffic is encrypted, implementing firewalls and other security measures to protect against unauthorized access, and regularly monitoring for potential threats. Additionally, SmartTech should also consider the security of its storage and server infrastructure, such as implementing access controls and monitoring for unauthorized access or data breaches.  Another important aspect to consider is the security and compliance of virtualization. This includes ensuring that all virtual machines are properly configured and secured and that all virtual networks are properly segmented to prevent unauthorized access. Additionally, SmartTech should also consider the security of the underlying hypervisor and virtualization platform, such as ensuring that all security patches are up to date and that the platform is configured to meet compliance requirements.  By utilizing a comprehensive security hub and framework, and by considering the security of all aspects of their data-center migration, SmartTech can ensure the security and compliance of their cloud environment and protect against potential threats.  One solution for SmartTech in terms of legal and security features when migrating their data center to the cloud would be to utilize the security hub feature offered by cloud providers. This feature allows for centralized management and monitoring of security across multiple accounts and resources within a cloud environment. SmartTech can also use this feature to automate security tasks and integrate with third-party security tools for even more robust security capabilities.  Another solution for SmartTech would be to implement a robust security framework when migrating their data-center to the cloud. This can include implementing encryption for all data in transit and at rest, implementing multi-factor authentication for all users and systems, and implementing security controls such as firewalls and intrusion detection systems.  SmartTech can also take steps to secure their networking, storage, servers, and virtualization in the cloud. For example, they can use virtual private clouds (VPCs) and network security groups (NSGs) to segment their network and limit access to sensitive resources. They can also use tools such as data loss prevention (DLP) and encryption to secure their storage and data. Additionally, SmartTech can use security features such as security-enhanced Linux (SELinux) and firewalls to secure their servers and virtualization.  It is important for SmartTech to continuously monitor and assess their cloud environment for vulnerabilities and compliance. This includes conducting regular security assessments, penetration testing, and vulnerability scanning. SmartTech should also have a incident response plan in place and conduct regular incident response drills to ensure that they are prepared to respond to a security incident.  SmartTech should also have a robust compliance program in place to ensure that they are meeting all legal and regulatory requirements related to data protection and privacy. This includes conducting regular compliance assessments, audits and reviews to ensure that they are meeting all relevant laws and regulations.  SmartTech can take several steps to ensure legal and security features when migrating their data-center to the cloud. These include utilizing security hub, implementing a robust security framework, securing networking, storage, servers, and virtualization, continuously monitoring and assessing their cloud environment, and having a robust compliance program in place. | |
| **References** |

- Cloud Academy. (n.d.). What Are the Benefits of Cloud Computing? Retrieved from <https://www.cloudacademy.com/blog/what-are-the-benefits-of-cloud-computing/>

- Forbes. (2019). The Benefits of Cloud Computing for Businesses. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/02/11/the-benefits-of-cloud-computing-for-businesses/?sh=7e69b1f33b8a>

- National Institute of Standards and Technology. (2011). Definition of Cloud Computing. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- Tutorials Point. (n.d.). Benefits of Cloud Computing. Retrieved from <https://www.tutorialspoint.com/cloud_computing/cloud_computing_benefits.htm>

- Gartner. (2018). Top 10 Things to Consider Before Migrating to the Cloud. Retrieved from <https://www.gartner.com/smarterwithgartner/top-10-things-to-consider-before-migrating-to-the-cloud/>

- AWS. (n.d.). Cloud Deployment Models. Retrieved from <https://aws.amazon.com/de/what-is-cloud-computing/deployment-models/>

- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

- Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). A scalable, commodity data center network architecture. ACM SIGCOMM Computer Communication Review, 38(4), 63-74.

- Booth, C., & Tansley, R. (2015). Cloud computing: A practical introduction. Springer.

- AWS. (n.d.). Cloud Service Models. Retrieved from <https://aws.amazon.com/de/what-is-cloud-computing/service-models/>

- AWS (n.d.). Understanding Cloud Deployment Models and Service Models. Retrieved from <https://aws.amazon.com/getting-started/hands-on/move-to-the-cloud/>

Cloud Academy (n.d.). Benefits of Cloud Computing. Retrieved from <https://www.cloudacademy.com/learning-paths/benefits-of-cloud-computing/>

- Forbes (2019). The Benefits of Cloud Computing. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/01/08/the-benefits-of-cloud-computing/?sh=26d5b2e16b51>

- Gartner (2018). The Key Benefits and Challenges of Cloud Computing. Retrieved from <https://www.gartner.com/en/information-technology/insights/articles/the-key-benefits-and-challenges-of-cloud-computing>

- National Institute of Standards and Technology (NIST) (2011). Cloud Computing Definition. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- Tutorials Point (n.d.). Cloud Computing - Benefits. Retrieved from <https://www.tutorialspoint.com/cloud_computing/cloud_computing_benefits.htm>

- AWS (n.d.). Cloud Deployment Models. Retrieved from <https://aws.amazon.com/cloud-deployment-models/>

- Cloud Academy (n.d.). The Benefits of Cloud Computing. Retrieved from - <https://www.cloudacademy.com/blog/the-benefits-of-cloud-computing/>

- Forbes (2019). The Benefits of Cloud Computing. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/08/15/the-benefits-of-cloud-computing/?sh=7d8d28f24b91>

- Gartner (2018). Top Challenges to Cloud Computing Adoption. Retrieved from <https://www.gartner.com/en/information-technology/glossary/cloud-computing-challenges>

- NIST (2011). Cloud Computing Definition. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-145/final>

- Tutorials Point (n.d.). Advantages of Cloud Computing. Retrieved from <https://www.tutorialspoint.com/cloud_computing/cloud_computing_advantages.htm>

- AWS (n.d.). Amazon Web Services. Retrieved from <https://aws.amazon.com/>

- Cloud Academy (n.d.). What are the benefits of cloud computing? Retrieved from <https://www.cloudacademy.com/blog/benefits-of-cloud-computing/>

- Forbes (2019). The Top 5 Benefits of Cloud Computing. Retrieved from <https://www.forbes.com/sites/forbesbusinesscouncil/2019/02/22/the-top-5-benefits-of-cloud-computing/?sh=7755b2a56474>

- Gartner (2018). How to Manage the Cloud Migration Process. Retrieved from <https://www.gartner.com/en/information-technology/insights/2018/06/how-to-manage-the-cloud-migration-process>

- Google (n.d.). Google Cloud. Retrieved from <https://cloud.google.com/>

- Microsoft (n.d.). Azure. Retrieved from <https://azure.microsoft.com/>

- NIST (2011). The NIST Definition of Cloud Computing. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- Tutorials Point (n.d.). Advantages of Cloud Computing. Retrieved from <https://www.tutorialspoint.com/cloud_computing/cloud_computing_advantages.htm>

- Cloud Academy (n.d.). Benefits of Cloud Computing. Retrieved from <https://www.cloudacademy.com/blog/benefits-of-cloud-computing/>

- Forbes (2019). The Benefits of Migrating to the Cloud. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/01/22/the-benefits-of-migrating-to-the-cloud/?sh=2d2f75a27b2c>

- Gartner (2018). Key Challenges of Cloud Migration. Retrieved from <https://www.gartner.com/en/information-technology/glossary/cloud-migration-challenges>

- NIST (2011). Cloud Computing Synopsis and Recommendations. Retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-146/final>

- Tutorials Point (n.d.). Advantages and Disadvantages of Cloud Computing. Retrieved from <https://www.tutorialspoint.com/cloud_computing/cloud_computing_advantages_disadvantages.htm>

- AWS (n.d.). Cloud Computing Deployment Models. Retrieved from <https://aws.amazon.com/what-is-cloud-computing/deployment-models/>

- Microsoft (n.d.). Virtual Machines. Retrieved from <https://azure.microsoft.com/en-us/services/virtual-machines/>

- AWS (n.d.). Elastic Compute Cloud (EC2). Retrieved from <https://aws.amazon.com/ec2/>

- Google (n.d.). Compute Engine. Retrieved from <https://cloud.google.com/compute>

- Microsoft (n.d.). Blob Storage. Retrieved from <https://azure.microsoft.com/en-us/services/storage/blobs/>

- AWS (n.d.). S3 (Simple Storage Service). Retrieved from <https://aws.amazon.com/s3/>

- Google (n.d.). Cloud Storage. Retrieved from <https://cloud.google.com/storage>

- Microsoft (n.d.). SQL Database. Retrieved from <https://azure.microsoft.com/en-us/services/sql-database/>

- AWS (n.d.). Relational Database Service (RDS). Retrieved from <https://aws.amazon.com/rds/>

- Google (n.d.). Cloud SQL. Retrieved from <https://cloud.google.com/sql>

- AWS (n.d.). AWS Cloud Development Kit (CDK). Retrieved from <https://aws.amazon.com/cdk/>

- Google Cloud (n.d.). Google Cloud Architecture Center. Retrieved from <https://cloud.google.com/architecture>

- Google Cloud (n.d.). Google Cloud Deployment Manager. Retrieved from <https://cloud.google.com/deployment-manager>

- Google Cloud (n.d.). Google Cloud Terraform Provider. Retrieved from <https://www.terraform.io/docs/providers/google/index.html>

- AWS (2021). Amazon S3 Pricing. Retrieved from <https://aws.amazon.com/s3/pricing/>

- AWS (2021). Amazon DynamoDB Pricing. Retrieved from <https://aws.amazon.com/dynamodb/pricing/>

- AWS (2021). AWS Reserved Instances. Retrieved from <https://aws.amazon.com/ec2/pricing/reserved-instances/>

- AWS (2021). AWS Data Center Global Infrastructure. Retrieved from <https://aws.amazon.com/about-aws/global-infrastructure/>

- AWS (2021). AWS Data Durability Options. Retrieved from <https://aws.amazon.com/s3/features/data-durability/>

- Azure (2021). Azure Storage Pricing. Retrieved from <https://azure.microsoft.com/en-us/pricing/details/storage/>

- Azure (2021). Azure Cosmos DB Pricing. Retrieved from <https://azure.microsoft.com/en-us/pricing/details/cosmos-db/>

- Azure (2021). Azure Pay-As-You-Go Pricing. Retrieved from <https://azure.microsoft.com/en-us/pricing/pay-as-you-go/>

- Azure (2021). Azure Subscription Pricing. Retrieved from <https://azure.microsoft.com/en-us/pricing/member-offers/msdn-benefits-details/>

- Azure (2021). Azure Hybrid Benefit. Retrieved from <https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>

- Forrester Research (2018). Cloud-Based E-Mail And Backup Services Offer Organizations Significant Cost And Security Benefits. Retrieved from <https://www.forrester.com/report/CloudBased+Email+And+Backup+Services+Offer+Organizations+Significant+Cost+And+Security+Benefits/-/E-RES126820>