Cloud Security Consultancy Report

Assignment 1 Group 9

Members: Ziyuan Jing (480153157) Yuanchen Shi(540451168)

Weiran Wang(540421677) Xijiu Wang(500437485)

Ilce Andrea Aquino(530594664)

Fengquan Jiang(540784103)

1. Considerations for Moving to the Cloud

1.1 The cloud deployment model

When moving to the cloud, selecting the right cloud deployment model is crucial. This decision should be based on your organization's size, complexity, and security requirements. The main cloud deployment models include public, private, hybrid, and multi-cloud. Each has its advantages and disadvantages, catering to different organizational needs.

Public Cloud

The public cloud marks a significant shift in IT infrastructure management, offering a shared platform for computing services that is accessible over the public internet and operates on a pay-as-you-go pricing model, thus presenting a cost-effective alternative to traditional on-premises data centers. This model's primary advantages include its cost-efficiency, which allows organizations to save on capital expenditures; unparalleled scalability to meet fluctuating demands without financial overcommitment; location independence that supports remote work and business continuity; and the rapid provisioning of resources that enhances business agility and accelerates the deployment of new services. Despite these benefits, the public cloud poses challenges in data security and privacy, especially in a shared environment that may not meet the stringent regulatory requirements of certain organizations. Additionally, the model requires careful management of spending to avoid escalating costs and offers less customization and control than private clouds, potentially making it less suitable for organizations with specific needs. However, the public cloud is particularly beneficial for startups and SMEs seeking low upfront costs and scalability, testing and development environments, web-based applications with variable demand, and as a cost-effective disaster recovery solution. Organizations are advised to consider their unique requirements, particularly regarding security and compliance, before adopting the public cloud to ensure strategic alignment and informed decision-making (Alzakholi, et al., 2020).

Private Cloud

The private cloud represents a cloud computing deployment model that provides a dedicated environment exclusively for a single organization, ensuring a high level of control and enhanced security measures that are particularly advantageous for businesses operating under stringent regulatory compliance and security mandates. Unlike public clouds, where resources are shared among multiple tenants, a private cloud's resources are solely allocated to one entity, offering an optimized infrastructure that can be tailored to the specific needs and goals of that organization. This exclusivity not only facilitates better alignment with complex compliance requirements, including those related to data protection and industry-specific regulations but also enables businesses to implement and enforce customized security policies and controls, significantly reducing the risk of data breaches and other security threats. Moreover, the private cloud model empowers organizations with the flexibility to configure and manage their computing environment according to their operational demands and scalability needs, thereby supporting dynamic business processes and applications with potentially sensitive data that cannot be hosted on public clouds. However, this elevated level of control and security comes with a higher cost, as organizations must invest in the necessary infrastructure, software, and skilled personnel to

develop, maintain, and secure their private cloud. Despite these expenses, for businesses that prioritize data sovereignty, require tight control over their IT environment, or operate within heavily regulated industries, the benefits of a private cloud can outweigh the costs, making it an indispensable part of their digital transformation strategy. This model's capacity to provide dedicated resources, combined with its adaptability to stringent legal and regulatory compliance, positions the private cloud as an ideal solution for entities looking for a balance between the cloud's scalability and flexibility and the traditional on-premises data centers' security and control (Sadeeq et al., 2021).

Hybrid Cloud

The hybrid cloud architecture seamlessly integrates public and private clouds, fostering an environment where data and applications can fluidly move between the two. This model is the epitome of flexibility, offering businesses the agility to adapt to changing demands and workloads by leveraging the scalability inherent to public cloud resources while maintaining sensitive data and applications in a more controlled, secure private cloud. Such a blend not only enhances operational efficiency but also optimizes cost management by allowing organizations to only pay for public cloud resources as needed. Moreover, the hybrid cloud model stands out for its ability to uphold rigorous regulatory compliance standards. By keeping sensitive data in a private cloud, businesses can ensure they meet industry-specific regulations and data sovereignty requirements, all the while benefiting from the expansive computing power and storage capacity of the public cloud for less sensitive tasks. This dual infrastructure also bolsters security measures, as organizations can apply robust protection in their private cloud and utilize the public cloud's extensive security features, thus creating a comprehensive defense strategy against cyber threats. Scalability, another hallmark of the hybrid cloud, empowers businesses to swiftly scale their IT infrastructure up or down based on real-time demands without significant upfront investments in physical hardware. This elasticity not only ensures that organizations can handle peak loads efficiently but also contributes to a more sustainable IT strategy, where resources are allocated and used more judiciously. Given these advantages, the hybrid cloud model emerges as a superior choice for organizations looking to navigate the complexities of digital transformation, offering a strategic mix of security, compliance, scalability, and cost-efficiency that is hard to achieve with other cloud computing models.

Multi-Cloud

The multi-cloud strategy involves leveraging cloud services from various providers to build a more resilient, flexible, and cost-efficient infrastructure. By distributing workloads across different clouds, organizations can significantly improve their disaster recovery and business continuity plans, ensuring that their operations remain uninterrupted even if one provider faces downtime. This approach also mitigates the risk of vendor lock-in, granting businesses the freedom to move applications and data between platforms as needed to take advantage of better pricing, features, or performance, thereby maintaining operational agility and avoiding dependence on a single vendor's ecosystem. Moreover, a multi-cloud strategy enables cost optimization through the ability to select the most economical services for specific needs from a broader marketplace, potentially driving down overall IT expenses. However, realizing these benefits demands sophisticated management and integration capabilities, as organizations must navigate the complexities of coordinating across different

platforms, ensuring security and compliance standards are met, and optimizing performance across their cloud environments. Despite these challenges, the strategic use of multiple clouds offers a competitive advantage by providing a scalable, agile, and cost-effective way to support diverse business requirements, making it an increasingly popular choice among forward-thinking enterprises.

Considering these options, hybrid cloud often emerges as a balanced choice for many businesses. It provides the flexibility and cost-effectiveness of the public cloud while retaining the security and control of the private cloud. This model supports dynamic or highly changeable work environments and is particularly beneficial for organizations that deal with sensitive data but also require the scalability provided by cloud resources .

Ultimately, the choice depends on your specific business needs, including compliance, scalability, cost, and security considerations. Conducting a thorough analysis of these requirements will guide you to the most suitable deployment model.

1.2 Identify the service model and type of cloud services

For most organizations, the choice of cloud service model largely depends on their specific needs, such as the level of control they wish to maintain, the technical expertise available in-house, and their budget constraints. However, among the primary cloud service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—SaaS often emerges as the most beneficial for a wide range of organizations.

Software as a Service (SaaS) represents a transformative approach to software delivery, where applications are hosted by a service provider and made accessible over the internet, offering a compelling alternative to traditional on-premise software installation. This innovative model significantly simplifies the deployment and management of software, eliminating the complexities associated with installation, maintenance, and support that businesses traditionally face. By delivering applications directly through a web browser, SaaS allows users to bypass the substantial infrastructure and hardware investments typically required for running software, resulting in substantial cost savings. Moreover, the inherent flexibility of SaaS provides scalability that can dynamically adjust to an organization's fluctuating demands, enabling businesses to efficiently scale their software usage up or down based on current needs without the need for significant capital expenditure or long-term commitments. This scalability ensures that organizations can remain agile and responsive to market changes or business growth, without the constraints imposed by physical infrastructure limitations. Additionally, SaaS offers access to advanced applications, which might otherwise be inaccessible due to high licensing costs or the expertise required for setup and ongoing management. The pay-as-you-go pricing model of SaaS further amplifies its appeal, aligning operational costs with actual usage, thereby optimizing expenditure and eliminating wasteful spending on unused licenses or capacity. This model not only facilitates better cash flow management but also allows businesses to invest more strategically in their core operations, fostering innovation and competitive advantage. Furthermore, SaaS provides a level of security and compliance that is continuously updated to meet evolving threats and regulatory standards, offering peace of mind and freeing up internal resources to focus on business-critical tasks rather than software and infrastructure security concerns. The combination of reduced IT overhead, scalability, and accessibility to

cutting-edge technology, along with cost-effective pricing and enhanced security, positions SaaS as an ideal solution for businesses looking to leverage the power of cloud computing to drive efficiency, innovation, and growth.

In the evolving landscape of modern work environments, the accessibility of Software as a Service (SaaS) applications from any internet-connected device has become a cornerstone for enhancing organizational productivity and flexibility. This ubiquitous access ensures that employees can collaborate seamlessly, regardless of their physical location, breaking down traditional barriers to communication and project management. Moreover, the inherent flexibility offered by SaaS applications supports a more dynamic and mobile workforce, enabling employees to work efficiently from home, co-working spaces, or any other remote location. This level of accessibility is not just a convenience but a strategic asset in the current climate, where the prevalence of remote work has surged due to global challenges and the ongoing shift towards more digital, agile work practices. The ability to access work-related applications and data from anywhere fosters a culture of collaboration and innovation, as teams can stay connected and continue to work on projects without the need for physical proximity. This digital approach to the workplace aligns with the growing demand for work-life balance, offering employees the flexibility to manage their work schedules and locations in a way that suits their personal needs and preferences, while still meeting organizational goals. In essence, the SaaS model, with its emphasis on accessibility, collaboration, and flexibility, is instrumental in supporting the transition to more adaptable, resilient, and efficient work environments, where the quality of work is not tethered to the location of the workforce, thereby enabling businesses to maintain continuity and thrive in an increasingly remote and digital world.

In summary, SaaS provides flexibility, efficiency, scalability, and cost savings, making it an ideal cloud service model for organizations looking to leverage cloud computing's advantages without the complexity and overhead associated with managing infrastructure or platforms. This model supports a wide range of applications and services, from email and collaboration tools to customer relationship management (CRM) and enterprise resource planning (ERP) systems, making it versatile across different organizational needs.

1.3 risks and security concerns

Selecting the right cloud deployment model—be it public, private, hybrid, or multi-cloud—and the subsequent adoption of Software as a Service (SaaS) comes with its unique set of risks and security concerns. These considerations are crucial for ensuring data protection, maintaining privacy, and safeguarding against potential breaches and threats.

Data Security and Privacy

In the landscape of cloud computing, particularly within public cloud environments where data is stored and managed off-premises by third-party providers, the paramount concerns of data security and privacy come to the forefront due to the inherent vulnerabilities associated with the shared nature of these services. The public cloud's architecture, designed to serve a multitude of clients on the same infrastructure, inherently increases the risk of data breaches and unauthorized access, thereby necessitating a comprehensive understanding and stringent evaluation of the cloud provider's security measures by

organizations. It is imperative for these organizations to diligently assess whether these measures are in sync with their own security standards and regulatory compliance requirements. The complexity of maintaining data privacy in such an environment is further compounded by the vast scale and dynamic nature of cloud resources, making it challenging to track and protect sensitive information effectively. Organizations must navigate these challenges by implementing robust encryption methods for data in transit and at rest, employing advanced threat detection systems, and ensuring regular security assessments and audits are carried out. Additionally, understanding the shared responsibility model, where security obligations are divided between the cloud provider and the client, is vital for ensuring comprehensive data protection. The selection of a cloud provider should thus be predicated not only on the cost and efficiency benefits but also on the provider's commitment to security, transparency in their operations, and the ability to offer customizable security features that can be tailored to meet the specific needs of the organization. This approach towards prioritizing data security and privacy in public cloud environments is not just a precautionary measure but a necessary strategy to safeguard against the evolving landscape of cyber threats, thereby ensuring the integrity and confidentiality of critical data assets.

Compliance and Regulatory Challenges

Navigating compliance and regulatory challenges in a cloud environment, particularly when adopting a multi-cloud strategy that involves data storage across multiple jurisdictions, demands a sophisticated and strategic approach due to the inherent complexity of adhering to various regulatory standards like GDPR, HIPAA, or PCI DSS. Organizations are required to have a deep understanding of not only where their data is stored and processed but also how it's protected, which becomes significantly more challenging when dealing with multiple cloud service providers (CSPs). This complexity is exacerbated by the dynamic nature of cloud computing, where data can be moved and processed across different regions and systems, potentially complicating compliance with laws that have strict data residency or sovereignty requirements. Implementing appropriate controls in such a scenario involves deploying advanced data protection measures, ensuring encryption both in transit and at rest, and maintaining rigorous access management to ensure that data is only accessible to authorized personnel. Furthermore, organizations must regularly audit their cloud environments to ensure continuous compliance, which includes keeping abreast of changes in regulatory requirements and adjusting their cloud security posture accordingly. This endeavor requires not only technical solutions but also a culture of compliance within the organization, where adherence to regulatory standards is woven into the fabric of the organization's operational processes. Engaging with CSPs that offer compliance certifications and tools designed to help manage compliance can alleviate some of the burden, but ultimate responsibility lies with the organization to ensure their cloud usage complies with all applicable laws and regulations. The stakes are high, as non-compliance can result in hefty fines, legal repercussions, and damage to an organization's reputation, making it imperative that companies approach cloud compliance with the seriousness and rigor it demands (Zhang et al., 2020).

Vendor Lock-in

Vendor lock-in, a significant concern in the realm of Software as a Service (SaaS) and cloud services, manifests when organizations become excessively reliant on a single vendor's ecosystem, creating a scenario where switching providers or integrating with other services becomes a formidable challenge. This dependency not only constrains operational flexibility but also poses the risk of escalating costs over time as organizations may find themselves in a position where negotiating more favorable terms becomes difficult due to the high switching costs—monetary, psychological, effort-based, and time-based—associated with moving to a different platform. Moreover, the lack of standardization across cloud services exacerbates this issue, further entrenching organizations into their current vendor's infrastructure. The critical analysis of vendor lock-in highlights it as a major barrier to cloud adoption, underscoring the importance of diversification in vendor selection to mitigate the risks of over-dependence. Strategies to combat vendor lock-in include adopting multi-cloud strategies, ensuring interoperability through the use of open standards, and carefully negotiating contract terms to include clauses that facilitate easier migration and integration with other services. By taking proactive measures to manage vendor dependency, organizations can preserve their ability to innovate and adapt to changing market conditions, thereby maintaining a competitive edge while avoiding the pitfalls of vendor lock-in (León-Castillo et al., 2020).

Management and Integration Complexity

In the ever-evolving digital landscape, organizations leveraging hybrid and multi-cloud environments face the intricate challenge of managing and integrating disparate cloud services and platforms, a task that necessitates a high degree of coordination and technical acumen. The complexity inherent in these environments arises from the need to maintain consistent security policies, enforce rigorous access controls, and implement robust data protection measures across a diverse array of cloud infrastructures. This complexity is further amplified by the need to ensure seamless interoperability between services provided by different cloud vendors, each with its own set of tools, standards, and interfaces. Consequently, organizations must invest in advanced management tools that offer comprehensive visibility and control over their multi-cloud ecosystems. Moreover, these tools should be capable of automating routine tasks and enforcing security policies uniformly, thereby mitigating the risk of human error and ensuring compliance with regulatory requirements. Additionally, expertise in cloud management and security becomes indispensable, as professionals equipped with the necessary skills can navigate the nuances of multi-cloud environments, optimizing resource utilization while safeguarding against potential vulnerabilities. The integration of such management tools and expert knowledge is essential for organizations to capitalize on the benefits of hybrid and multi-cloud strategies, such as increased flexibility, scalability, and resilience, without succumbing to the complexities that could jeopardize their security posture and operational efficiency (De Rojas et al., 2021).

Threats to Availability and Service Continuity

The dependency on cloud providers to host critical services inherently carries risks of service outages and disruptions, which can significantly impact organizational operations. Among

these threats, Distributed Denial of Service (DDoS) attacks stand out as a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic, thereby jeopardizing the availability of cloud services. Natural disasters such as earthquakes, floods, hurricanes, and others pose additional risks, as they can physically damage data centers, leading to prolonged outages. Furthermore, technical failures within the cloud infrastructure, including hardware malfunctions, software bugs, or human error, can unexpectedly interrupt services. These varied threats underline the critical importance of implementing comprehensive disaster recovery and business continuity planning. Such plans ensure that organizations can quickly recover and maintain their operations with minimal downtime in the event of an incident, regardless of its nature. Effective planning includes not only the replication of data and applications across multiple geographically diverse locations to mitigate the risk of natural disasters but also the deployment of robust security measures to guard against DDoS attacks and the establishment of failover mechanisms to address technical failures. Additionally, continuous monitoring, regular testing of disaster recovery protocols, and clear communication strategies are essential components of a resilient business continuity plan, empowering organizations to navigate the complexities of cloud computing environments while minimizing the impact of disruptions on their operations (Crook et al., 2021).

Addressing these risks requires a proactive approach, including conducting regular security assessments, implementing end-to-end encryption for sensitive data, employing robust access controls, and choosing cloud providers that offer transparent compliance certifications and robust security features. Additionally, adopting a multi-cloud strategy can mitigate the risk of vendor lock-in and service continuity threats but requires careful management to avoid complexity and integration challenges.

2. Cloud Storage

2.1 Cloud storage options

Depending on the client's background, financial institutions have both unstructured data such as emails and structured data such as financial records and customer information to store and analyze. Therefore, we recommend using Azure Blob Storage and Azure Files.

Azure Blob Storage

Azure Blob Storage, Microsoft's cloud object storage solution, is optimised for storing large amounts of unstructured data. Blob Storage is suitable for storing images or documents, video and audio, log files, data for backup and restore, and data for analysis on-premises or by Azure Managed Services (Microsoft, 2022).

Customer financial institutions need to store unstructured data, such as emails and logs, etc., and the characteristics of Blob Storage itself can meet these needs. At the same time, for the data accessibility and confidentiality of the client financial institution, users or client applications can access the objects in Blob Storage within the organization via HTTPS. HTTPS encrypts communications using the SSL/TLS protocol. SSL/TLS confirms the true identity of a website or application server and prevents impersonation, which prevents a wide range of network attacks (CLOUDFLARE, 2024). With HTTPS, data is encrypted in both directions during transmission. This protocol secures communications so that malicious parties cannot observe the data being sent. Encryption also protects sensitive or personal data, such as bank account information, if a user must send it to a financial institution.

Clients can also securely connect to Blob Storage using SSH File Transfer Protocol (SFTP) and mount Blob Storage containers using Network File System (NFS) 3.0 protocol (Microsoft, 2022). This data can then be used across different departments and internationally. The speed, accessibility, security and scalability of cloud storage offered by Blob Storage are extremely attractive to all medium and large organizations (SnapLogic, 2024).

Another security consideration is Microsoft Defender for Storage. An Azure-native security intelligence layer called Microsoft Defender for Storage detects potential risks to storage accounts. It assists in preventing three primary impacts on data and workloads: data corruption, sensitive data exfiltration, and malicious file uploads. The Azure Blob Storage service generates data-plane and control-plane telemetry data, which Microsoft Defender for Storage analyses to provide comprehensive security (ElazarK, 2023). Defender for Storage offers malware scanning, activity monitoring, and sensitive data threat detection for Blob Storage.

Azure Files

Azure Files is another cloud storage service offered by Microsoft that is perfect for storing data that needs to be accessed by multiple users or applications. Azure Files can be used to replace or supplement traditional on-premises file servers. Popular operating systems, including Windows, macOS, and Linux, can mount Azure Files shares natively and access

them globally (khdownie, 2023). Azure Files shares can be replicated to Windows servers on-premise or in the cloud using Azure Files Synchronisation. Azure Files shares can also be replicated to Windows servers on-premises or in the cloud using Azure Files Synchronisation, improving performance and enabling distributed data caching.

Azure Files is a good choice because the customer's financial institution has multiple departments, each with different types of data to capture and utilize, such as the Finance Department, which needs credit card details and financial records; the Customer Care Department, which needs customer-related data; and multiple employees in each department who need to work with this data.

For other security considerations, Azure Files supports Azure Active Directory (Azure AD) integration for authentication and access control. This integration allows applications to securely access Azure File Shares without the need to store or manage credentials. Instead, applications can use managed identities to ensure secure access to all file shares (Viswanath, 2023). By granting permissions to managed identities, application users can establish identity-based access to application file shares.

2.2 Data Classification Categories

Data classification involves intentionally assigning a sensitivity level to data during its creation, modification, enhancement, storage, or transmission. When classifying intellectual property, it's crucial to consider not only the degree of control and protection required but also the data's value as a business asset (Wright, 2008). Organizing data systematically assists businesses in managing, monitoring, and analyzing individual pieces of information effectively. Meanwhile, data classification is a crucial aspect of managing data throughout its lifecycle, determining the specific standard category or group to which data objects belong. Once classified, data categorization assists in ensuring that companies comply with their internal data handling protocols and various local, state, and federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) (Lutkevich, 2020). Particularly in heavily regulated sectors, companies often establish data classification processes or workflows to aid in compliance audits and data discovery procedures. While data classification is essential for categorizing structured data, it holds even greater significance in optimizing the utilization of unstructured data (Kranz, 2022). Moreover, data classification plays a role in identifying redundant data copies. By eliminating duplicate data, organizations can efficiently manage storage space and enhance data security measures.

Based on the importance of data classification, we recommend that client financial institutions categorise data into three main types: **Public**, **Restricted** and **Confidential**.

Public Data

Public data refers to information that is freely shareable, usable, and distributable without any restrictions. This encompasses a wide range of forms and sizes, including datasets, statistics, structured data, and unstructured data that has been processed or remains raw (Hashemi-Pour, 2023). According to the background provided by the client financial

institution, some data such as company information and pictures that need to be provided to the user on the website and other data that need to be used on the front end of the website can be divided into public data. As the data is public-facing and does not contain sensitive information about customers and organisations, there is no obvious security risk in terms of security considerations. Therefore, it is more appropriate to classify it as public data.

Restricted Data

Restricted data is highly sensitive and can cause serious damage to a business or its customers if compromised. This is often heavily regulated personal or financial information (Slagle, 2023). Controlling access to this data is crucial to prevent unauthorized usage. Encrypting this data adds an extra layer of protection (Brook, 2022). The loss of such restricted data can significantly impact the security of an organization or individual's information. Based on the information provided by the client financial institution, the following data is proposed to be classified as restricted data:

- Credit card details and financial records processed by the Finance Department.
- Customer-related data and inquiries handled by the Customer Care Department.
- Employee records, such as social security numbers and salaries managed by HR Department

At the same time, these data must be accessed, processed and analysed only by the corresponding departments and responsible personnel through authorised operations. This ensures the security of data handling.

Confidential Data

Confidential information pertains to data that hasn't been disclosed publicly, encompassing business details and any other sensitive information. Trade secrets fall under this category of "confidential information" and may encompass various forms of technical data (Housing and Digital Economy Communities, 2016). When confidential data is compromised, it is the organisation itself that will suffer the most. By studying the background of our client's financial institution, we found that the Management Department deals with sensitive business data, performance metrics, and strategic plans, which are relatively confidential as they relate to the future growth of the organisation. In addition, we noted that the IT Department may be developing applications for internal use within the organisation that involve data on online banking, transactions, and reporting, which are also confidential. Therefore, it is recommended that all of the above data be classified as confidential and only be accessed by a limited number of internal members of the organisation.

Finally, the following table summarises our data classification:

Data Classification	**Data Name**
Public	● Public-facing web contents
Restricted	● Credit card details ● Financial records ● Customer-related data and inquiries

	● Employee records, such as social security numbers and salaries
Confidential	● Sensitive business data ● Performance metrics ● Strategic plans ● Online banking, transactions, and reporting data

Table2.2.1 Data Classification Table

2.3 Storage policies

Data retention involves preserving and utilizing data for a set duration, known as the data retention period, to meet business, technical, and legal needs. Its purpose is to facilitate easy data recovery in case of unexpected disasters or data loss events. A practical data retention strategy considers not just the initial data state but also its evolving value and legal responsibilities. A data retention policy outlines how an organization uniformly stores and disposes of data, including the duration for which various types of data should be retained, their storage location, and format (Ayuya, 2023).

Azure Storage Accounts provides three storage access tiers to suit different needs (Belmansour, 2021):

- **Hot tier**: designed for frequently accessed data.
- **Cold tier**: intended for data accessed infrequently, with a minimum storage duration of 30 days.
- **Archive tier**: optimized for rarely accessed data that needs to be stored for at least 180 days, with flexible access latency requirements, typically in the range of hours.

Combined with the above, this section establishes storage policies based on the type of data classification, including data retention periods and data backup procedures as shown in the table below.

Data Type	**Data Retention Periods**	**Data Backup**	**Data Storage Tier**
Public Data	2 years	Monthly	Hot
Restricted Data	5 years (in general)	Weekly	Cool
Confidential Data	7 years	Daily	Archive

Table2.3.1 Storage Policies Table

Public Data

Public data has low sensitivity and the relevant laws do not indicate how long the data should be retained. However, we recommend that public data may be retained for up to two years, depending on the organisation's own needs. In terms of backup, since public data

needs to be accessed and updated frequently, it is recommended that backups be made every month to ensure data confidentiality, integrity, and availability. Meanwhile, the storage access tier can be set to the Hot tier.

Restricted Data

Since restricted data contains many personal information, both customers and employees. Therefore, the relevant laws and regulations have clear rules and recommendations. Since restricted data contains personal information, both customers and employees. Therefore, the relevant laws and regulations have clear rules and recommendations. However, the relevant legal regulations vary from country to country and region to region. The Sarbanes-Oxley Act (SOX), for example, requires companies to retain customer data for five years (Lekatis, 2002). The Australian government requires related data to be encrypted and retained for at least two years (Australian Home Affairs, 2019). However, The General Data Protection Regulation (GDPR) stipulates that personal data, such as employee information, can only be retained for a maximum of two years after the employee has left the company, and that the employee has the right to request that the data be deleted earlier (GDPR, 2018). Hence, our suggestion is to maintain restricted data for five years, deleting data preemptively for departed employees and upon customer request. This aligns with regulations across various countries and regions globally. Regarding data backup, we propose weekly backups with versioning activated, along with off-site backups to a distinct Azure region for disaster recovery purposes. Meanwhile, the storage access tier can be set to the Cool tier since different departments need to access and analyse these data.

Confidential Data

Because confidential data contains highly sensitive data such as financial records and company programme reports, longer data retention periods are required for this type of data. Confidential data, such as financial records, are generally required to be retained for seven years under the GDPR and company law (Fisk, 2023). Australia also has a corresponding seven-year data retention policy, for example, companies must retain transaction records for seven years (AUSTRAC, 2022). In summary, we recommend that confidential data be retained for seven years and that data be backed up daily to ensure data security and integrity. The storage access tier can be set to the Archive tier since this type of data needs to be stored for seven years and not frequently accessed by different people.

2.4 Suggested Encryption Techniques and Key Management Practice

Encryption Techniques

Because most of the data from client financial institutions is highly sensitive, we recommend platform-level encryption by using AES-256 encryption to encrypt the data before the data stored in Azure storage services. AES, also known as the Advanced Encryption Standard, is a symmetric block cipher that the U.S. government has selected to safeguard classified data. AES-256 encryption operates by encrypting and decrypting data blocks with a 256-bit key length. It employs 14 rounds of the 256-bit key, with each round involving substitutions,

shifts, and mixing of the plaintext to transform it into ciphertext (Jena, 2023). It enhances the security of data during storage and transmission.

Here are the specific reasons why we recommend AES-256 encryption:

1. *AES-256 encryption is highly resistant to brute-force decryption attempts*
   This type of attack involves systematically trying numerous key combinations until the correct one is found (BuffALO, 2023). Due to the extensive computing power required, it is extremely improbable for a malicious actor to successfully crack AES-256 encryption through brute force.

2. *AES employs symmetric encryption, making it well-suited for internal data protection*
   It offers a faster and less computationally intensive method compared to other encryption techniques. This efficiency makes AES particularly effective for securing large volumes of data (Franklin, 2020).

3. *The implementation of AES-256 encryption plays a crucial role in safeguarding against data breaches*
   Such breaches can severely damage an organization's reputation built over years of effort. AES-256 encryption acts as a formidable barrier, preventing unauthorized access to data even if the underlying security infrastructure is compromised (Squirrel, 2023). This robust encryption not only shields against hackers but also helps mitigate compliance risks, ransomware threats, and data theft incidents.

4. *AES-256 encryption stands out as a top-tier security measure*
   Its strength extends to protecting data against sophisticated attacks, including potential threats from quantum computers in the future (Basatwa, 2023). While AES-128 and AES-192 are also formidable encryption standards, AES-256 offers an additional layer of defence, ensuring data security in evolving threat landscapes and emerging technological scenarios.

In summary, the use of AES-256 encryption in storage and transmission can effectively increase the data security of financial institutions and prevent possible future hacking attacks.

Key Management

Effective key management serves as the cornerstone of data security. Encryption keys are essential for encrypting and decrypting data. Therefore, the loss or compromise of any encryption key can render data security measures ineffective. Adhering to specific standards and regulations ensures that a company follows best practices in safeguarding encryption keys (Puneet, 2020). Properly protected keys are accessible solely to authorized users.

We suggest utilizing Azure Key Vault for managing encryption keys to achieve centralized control and enable auditing capabilities. Azure Key Vault is a key management solution within Azure that addresses key management challenges effectively. It simplifies the creation and management of encryption keys crucial for data encryption (msmbaldwin, 2024). For IT developers in financial institutions, Azure Key Vault offers centralized storage for application secrets, ensuring better control over their distribution. This minimizes the risk of

unintentional exposure of secrets. By leveraging Key Vault, application developers can avoid embedding security information directly into their code. For instance, rather than including a database connection string in the application code, it can be securely stored and accessed from Key Vault. In addition, Azure Key Vault can be utilized without requiring expertise in hardware security modules, and it can quickly scale to accommodate an organization's peak usage (msmbaldwin, 2024). With data replication ensuring high availability, administrators are not required to initiate failover procedures.

In addition to Azure Key Vault, implementing Azure AD for identity and access management is also required by financial institutions. As mentioned in the Cloud storage options section, Azure AD ensures that only authorised users can access encryption keys. For example, only Finance Department staff can access data such as financial records and credit card details using the appropriate keys.

2.5 Data Loss Prevention Measures

This section will introduce three data loss prevention measures aimed at preventing unauthorized access or inadvertent disclosure.

1. *Implement Role-Based Access Control (RBAC) with Azure Active Directory (AD)*
   Role-based access control (RBAC) is a system for regulating resource access by associating permissions with the roles of users in an organization. Role-Based Access Control (RBAC) reduces the risk of unauthorized data access by restricting access to specific data to only those with relevant roles. Unlike traditional methods that involve assigning individual permissions, RBAC streamlines this process by assigning roles, cutting down on errors and administrative burdens.

   For companies struggling with managing permissions individually, RBAC offers a way to boost operational efficiency significantly. By categorizing users into roles and granting them corresponding access rights, operations run more smoothly with fewer errors (Herzberg, 2023). Clearly defined roles and access logs also facilitate auditing, enabling quick identification of who accessed what, when, and why. This transparency not only ensures compliance but also fosters trust among stakeholders, customers, and regulators. As organizations expand, their data access needs grow more intricate, and RBAC's scalability ensures it can adapt to these evolving demands alongside changes in the organizational structure.

2. *Utilize Data Loss Prevention (DLP) tools to monitor and mitigate unauthorized data access or leakage*
   There are a number of DLP tools available on the market today, such as Microsoft DLP, which can be deployed to help insiders identify current data security vulnerabilities. These tools analyze content across various platforms to detect information related to authorized users or regulatory standards, thereby pinpointing potential threats to user and network security. Administrators have the flexibility to establish personalized data identifiers and categorization structures, ensuring the detection and safeguarding of proprietary enterprise information (Brook, 2023). Once sensitive data is identified, the DLP system enforces pre-established access

protocols to manage user interactions with the data, whether stored in the cloud or on local systems.

Key DLP features like real-time monitoring and intervention are pivotal in swiftly detecting and preventing unauthorized data transfers and access attempts. These functionalities operate continuously, overseeing mobile, stored, and actively used data across organizational networks, endpoints, and cloud platforms (Cocoara, 2024). This proactive response mechanism is crucial for preventing data breaches before they occur, rather than simply reporting them after potential threats have compromised data security, operational stability, and reputational trust. For instance, if an employee tries to send an email containing confidential information to an unauthorized recipient, the DLP system can automatically stop the transmission and alert administrators, thereby mitigating a potential data breach.

3. *Conduct regular security awareness training for staff to reduce the risk of accidental data breaches*
   Financial institutions must prioritize security awareness training for their employees to safeguard sensitive information, comply with regulations, and fortify their cybersecurity infrastructure. Educating employees on identifying and avoiding phishing attempts is crucial as these are common entry points for cybercriminals. Aware employees are less likely to inadvertently aid cyber threats. Moreover, they can detect suspicious internal activities and report them promptly.

   Compliance with regulations like the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability (HIPAA), or California Consumer Privacy Act (CCPA) is essential, and employee awareness training plays a pivotal role in meeting these standards and preventing financial and legal repercussions (The Security Company Limited, 2023). Employees who understand the value of data are more inclined to take security measures seriously, thus safeguarding organizational assets. Training significantly reduces human errors, the primary cause of data breaches, and equips employees to identify social engineering tactics such as phishing, pharming, or entrapment.

   Data breaches can severely tarnish an organization's reputation, but well-trained employees mitigate such risks and uphold the organization's public image. Ultimately, investing in security awareness training is more cost-effective than dealing with the aftermath of a cyber breach in terms of financial and legal ramifications.

The above three options prevent data leakage from three aspects: technical structure, third-party tool assistance and internal education of the organisation. If a financial institution can implement these three solutions well, the data will be protected in a good environment and the risk of leakage will be greatly reduced. This will reduce the potential loss to the institution in the future.

3. Access Security

In a cloud computing environment, the key of access security is ensuring data confidentiality, integrity, and availability. When financial organization migrate to cloud, achieving efficient and secure controlled access is critical. IAM, enhanced authentication mechanisms and permission allocation are fundamental to building a secure cloud environment. For financial organizations, the use of advanced security access measures requires compliance with industry rules and standards, as well as ensuring that guests' private data is protected.

In the process of cloud migration, it is necessary to develop a detailed and comprehensive security access policy to ensure that the data is not compromised, but also not subject to unauthorized access and other threats. Therefore, it is necessary to choose a suitable IAM scheme, set up a strict password test, achieve multi-factor authentication, privileged access and so on.

These methods will be discussed in detail in this part to provide a complete framework for financial organizations, which will be analyzed from both theoretical and practical aspects. The goal is to ensure that data and resources are protected in the cloud environment while also meeting the business efficiency of financial organizations. We will also ensure that any actions of financial organizations in the cloud environment are legal and compliant.

3.1 IAM

IAM is key to the structure of cloud security because it serves as both a basis for operational security and an important part in ensuring data integrity. IAM systems give companies the ability to limit user access to cloud resources, making sure that only authorised users have access to confidential information and services. By providing detailed access control, user authentication, and permission management, IAM assists in enforcing policies, keeps watch on user behaviour, and works to stop data breaches and illegal access. (Microsoft cloud, 2024)

One of the reasons IAM is an important part of cybersecurity is that IT can help an organization's IT department strike the right balance between keeping important data and resources inaccessible to most people but still accessible to some. IAM can set controls that grant secure access to employees and devices while making it difficult or impossible for outsiders to get through. Another reason IAM is important is that cybercriminals are improving their methods every day. Sophisticated attacks such as phishing emails are one of the most common sources of hacking and data breaches, and they target users with existing access rights. Without IAM, it is difficult to manage who and what has access to an organization's systems. Breaches and attacks can run rampant because it is difficult not only to see who has access, but also to revoke access for infected users. Unfortunately, while perfect protection does not exist, IAM solutions are an excellent way to prevent and minimize the impact of attacks. Many IAM systems are AI-enabled and are able to detect and block attacks before they become more serious, rather than limiting everyone's access when a breach occurs. (Microsoft cloud, 2024)

3.1.1 Recommended IAM Solution

The recommendation for this financial organization's IAM solution is to use Microsoft Azure.All of Azure's services operate in the cloud, including identity and access management functions. Azure provides high scalability and security.

Conditional access controls, RBAC, and other highly customised needs may be met by Azure in a multitude of sophisticated business scenarios. Additionally, Azure offers multi-factor authentication and single sign-on (SSO), which enhances client security. In order to comply with stringent rules and safeguard confidential information and financial organization need to apply these requirements.

3.1.2 Analyse how this IAM solution meets specific business needs and security requirements

Azure AD's strong identity protection and access control features help financial organisations in meeting their particular business and security requirements. Organisations can regulate access according to a user's location, device state, application sensitivity, and risk level by implementing conditional access policies. As a result, companies may attain more precise access control and users can only access critical resources under certain conditions.

Azure may limit identity theft and prevent unauthorised access through the use of multi-factor authentication, which adds an additional layer of security verification. This is essential to protecting customer data and financial activities, particularly in light of the rise in attacks.

Financial organisations may more precisely regulate user access to cloud resources with Azure's RBAC (Role-Based Access Control). RBAC helps in maintaining the concept of least privilege, which reduces any internal and external security issues, by granting users the fewest rights (required permissions). Financial organisations that must set up exact access controls for various departments and team members are most suited for this kind of privilege management.

Furthermore, financial organisations may rapidly identify and respond to possible security risks by monitoring and analysing security events and trends through Azure AD's security analytics and reporting capabilities. The key to cloud environment security is real-time monitoring and reporting, which is essential for assisting organisations in defending from more complex attacks and protecting customers data and financial information.

Single sign-on (SSO) provision helps cloud users use one password to access all applications/services. It provides secure and uninterrupted service by retaining a copy of the credentials for each user. Users do not need to specify their credentials each time they access different cloud web services. Security Assertion Markup Language (SAML), Open Authentication (OAuth), and OpenID provide single sign-on (SSO) facilities by allowing identity providers (IdPs) to share authentication and authorization information with service providers (SPs).(Indu, I., Anand, P.M.R. and Bhaskar, V. (2018))

Overall, Microsoft Azure AD as an IAM solution completely satisfies the identity and access management requirements of financial organisations during cloud migration due to its strong compliance support, flexible administration capabilities, and advanced security features. In addition to offering the requisite security and compliance measures, it enhances user productivity and experience, supporting financial institutions' business growth and innovation while protecting essential assets.

Financial organisations can ensure the success of their cloud migration plans and provide their customers and workers a safe, effective, and easy cloud service environment by selecting Azure AD as their Identity and Access Management (IAM) solution. This decision not only shows the organization's commitment to security but also its flexibility and vision for upcoming technological developments.

3.2 Password policy

3.2.1 Importance of Password Policy

Data security and privacy protection are always tasks that enterprises cannot afford to ignore in their cloud initiatives. Authentication with just username and password is no longer a good method as the technology and attack methods are now evolving. Password policy can greatly improve the security of the system and is one of the most important methods to strengthen the protection of cloud resources and reduce the security risks caused by password leakage.

A good password policy can make it more difficult for users' passwords to be breached. YuHongBird needs to change passwords regularly to reduce the potential risks associated with using one password for a long period of time. A strong password policy also enhances employees' awareness of information security, allowing them to form good habits and making the cloud environment more secure.

3.2.2 Detailed Password Policy

To effectively enhance the security of cloud resources, the following is a recommended detailed password policy to be implemented, containing at least five key points:

1. **Password Complexity Requirements**: Passwords need to contain upper and lower case letters, special symbols, and so on. The length cannot be less than 12 digits. This will significantly increase the complexity of the passwords and make them difficult to break.
2. **Password Update Period**: Every user must change their password every 90 days, and it cannot be the same as the previous password (less than 4 times). This effectively reduces the risk of password theft, and even if the password is compromised, it can be stopped in advance.
3. **Password Attempts Limit**: Accounts with more than 5 failed password attempts in a short period of time will be automatically locked for 30 minutes or until manually unlocked by the administrator. This measure can effectively prevent brute-force breaking attacks.

4. **Password Leakage Detection**: Utilising current password leakage detection services, employees are checked at regular intervals to see if their passwords have been compromised. If it occurs, they are asked to change their passwords immediately.
5. **User education and training**: Regularly train users on password security so that they know how to create a strong password and understand why using weak passwords can be a hidden danger to personal and company information security. Improve overall security by increasing individual security awareness.

One of the key strategies for enhancing account security is two-factor authentication (2FA), especially in financial institutions that handle sensitive financial data. Users need two different forms of verification like 2FA provides to access an account or system. These two forms can be a mobile phone and a password (something the user knows and something the user has). This way even if an attacker gets the password, they cannot gain access without a second factor.

3.3 Importance of 2FA

In financial organisations, customers and company assets have the highest level of security. 2FA provides financial institutions with an additional layer of security that makes unauthorised access more difficult. 2FA can better stop security threats due to password compromise, phishing or keylogging. Such security measures are necessary in financial institutions. Since the main target of these attackers is financial organisations, any breach can lead to significant financial or reputational damage.

3.3.1 Recommended 2FA Approaches

For financial institutions, the following two 2FA methods are recommended:

1. **Time-based one-time password (TOTP)**:
    - Users can authenticate with a password generated in a mobile app.
    - Benefits include ease of implementation, low cost and user-friendliness.
    - This method has a low network dependency, providing users with increased flexibility and convenience, as well as improved security.
2. **Hardware tokens**:
    - Each user must have a physical device that generates a one-time secret key when a login is required. The user needs to use this secret key to perform operations.
    - This method is more costly, but it also provides greatly improved security, which is very useful for departments and management that have to deal with a large number of financial transactions.

- Hardware tokens are essentially impossible to steal or copy remotely, which is the main reason it was chosen, and provides an additional layer of protection for financial institutions.

In finance, as digitisation grows, so does the importance of protecting sensitive data and information. 2FA as a strong security measure not only provides an effective means for financial institutions, but also better enhances security, prevents unauthorised access, and better protects customer assets. By using methods such as TOTP and hardware tokens, financial institutions can simultaneously protect sensitive data and ensure security and convenience. It is clear that in the digital age, the use of 2FA has become one of the most important tools for financial institutions to ensure the security of information and safeguard customer assets, and while there are still some challenges to be faced, these can be overcome with the right strategies and measures.

3.4 Privilege Access Management

A key component of information security and data management is privileged access management (PAM). Especially for industries with extremely high security requirements, such as the financial industry, PAM monitors access to critical systems and sensitive data, especially privileged accounts that have privileges beyond those of ordinary users, such as system administrators, super users, and so on.

PAM is the use of specialised tools and techniques to identify, monitor, control and audit privileged account access. In cloud environments, it is important to manage these privileged accesses as resources scale. But without strict controls, these privileged accounts can be used by attackers as a prime target for attacks. And with PAM, organisations can mitigate these risks.

Privileged access management helps prevent unauthorised access in several ways:

1. **Least Privilege Principle**: Ensuring that users and systems have intelligent access to the resources and information they need, which limits the potential for security breaches.
2. **Session monitoring and logging**: Privileged sessions are monitored in real time and all operations are logged so that unauthorised activity can be quickly detected and the necessary auditing and tracing can be provided.
3. **Credential Management**: Automation of credential management prevents password leakage and ensures that credentials are provided only when needed and revoked as soon as they are used.

To effectively use privileged access management, you can adopt RBAC to define roles more clearly and associate access rights with them, which simplifies managing permissions and ensures that only the right roles have access to sensitive data. The activities and permission configuration of privileged users need to be reviewed periodically to ensure that they do not have unnecessary permissions. Use MFA to add an extra layer of security to ensure that

credentials are not stolen. Ensure that high-risk operations do not affect low-risk operations by isolating the environment in which sensitive information is accessed.

Organizations also need to choose a PAM solution that supports automation and integrates privileged account management capabilities to ensure compatibility with existing facilities. Employees also need professional training to enhance their safety awareness. Monitor privileged accounts and respond quickly when an account is accessed abnormally. With these measures, financial institutions are well placed to improve the security of their cloud platforms. PAM not only reduces the risk of data breaches, but also enhances protection against insider threats, and using PAM strategies can provide a good foundation for financial institutions to better control and manage sensitive data after moving to the cloud.

3.5 Single sign-on

SSO is an authentication mechanism that allows users to access multiple applications and services with a single login operation. This mechanism simplifies the user login experience and reduces password fatigue (users need to remember many passwords, which is easy to remember). Users need to implement SSO through an authentication server that authenticates the user's identity and informs other systems.

Because users use fewer duplicate passwords, all SSO reduces the risk of password leakage. And because only one authentication is required, this also reduces the probability of being attacked during the login process. SSO allows for centralized management of user permissions, so security administrators can revoke access more quickly and update access controls more easily when there are personnel changes.

Applicability to financial institutions:

Security: Security is of the utmost importance to financial institutions. SSO can increase account security by enforcing authentication. In this way, even if the data has been compromised, it is difficult for unauthorized users to gain access to the system with a single login attempt. In addition, SSO has an advanced monitoring and alarm system, which can prevent suspicious behavior and increase security.

User experience: Both customers and employees of financial institutions need access to multiple systems. With SSO, they only need to enter information once and can access multiple service systems, greatly improving efficiency and convenience. This convenience is important in dealing with customer problems because it can enhance the customer experience.

Cost: In the early days of using SSO, the overhead can be high because of the cost of technology investment and staff training. But in the long run, reducing password resets and reducing IT support stress can significantly reduce operating expenses. SSO can also avoid financial losses due to security incidents.

Overall, SSO provides an effective test for financial institutions in all aspects. By simplifying the login process, the operation efficiency is improved and the security is enhanced. When financial institutions use SSO, they can better ensure security performance and compliance,

while also improving user satisfaction, which can also provide institutions with some competitive advantages in the financial market.

4 Networking

When it comes to network design, security is fundamental. If not properly secure network architecture in Azure network workloads, there could be a serious risk that hostile attackers could use our resources for illegal activities, access sensitive data, or damage Organisation reputation. To avoid these threats, we need to consider security best practices when we design and set up Azure virtual networks.

Azure offers robust network infrastructure services with a wide range of customized configurations, which allows planning and deployment from simple to complex network designs. These features permit cover organization's needs including private hybrid connectivity between on-prem and Azure, in this case, our proposed solution architecture.

Based on the information given, the client is a medium-sized global financial institution with 425 employees. Considering the business and security needs of the financial institution, we need to further refine the subnet configuration and IP address allocation to ensure that the network is secure, meets Australia's security and policy requirement and is easy to manage, while also ensuring good scalability and efficiency.

4.1.a Network Architecture Design Principles

Security Principle:
This principle is to ensure the data security of the financial institution and the protection capability of the network.
Methods:
1.Access control and authentication: Ensure that all network access is subject to strict authentication and authorization. Ensure that only authorized users have access to network resources by implementing multi-factor authentication and dynamic access control policies.
2.Defense Strategy: Deploy advanced firewalls and Intrusion Detection Systems (IDS) at all entry points to the network and ensure that the latest cyber threats are countered by continuously updating defenses.

Management Principle:
This principle is to simplifies the management of network architecture and improves work efficiency.
Methods:
1.Monitoring System: A centralized monitoring system is in place to monitor network performance and security events in real time, allowing for a quick response to any potential problems.
2.Automatic operation and Maintenance: The automatic deployment and configuration of network components reduces manual operation errors and improves O&M efficiency.

Expandability Principle:
This principle provides excellent network design support regarding future business growth or company expansion.
Methods:

1.Cloud and Local infrastructure: Ensure efficient synergy between cloud and local resources to provide strong network support for future business growth or institutional expansion.
2.Azure Dynamic Resource Allocation: Network resources can be dynamically adjusted according to business needs to support the rapid development of business.

Efficiency Principle:
This principle provides efficient network services to meet the needs of business operations.
Methods:
1.Virtual network configuration and management capabilities: Azure delivers powerful network infrastructure services that support simple to complex network designs to improve efficiency.
2.High-performance network equipment: High-performance network equipment is used to ensure fast data transfer, especially for high-frequency financial transaction data.

4.1.b IP address ranges and subnet configuration

In order to ensure the network security of financial institutions, we designed a comprehensive Virtual network (VNet) with the name 'GlobalFinanceNet' and the address space '10.1.0.0/16'. ', (/16 provides 65,534 available hosts, which can provide enough address space and also provides enough flexibility to divide multiple subnets, which helps simplify the design and management of the network, thus making it easier to implement security policies and access control to meet the business needs of different services and departments). The following are the subnetting configurations involved for the key services and functions of a global financial institution:

WebSubnet: '10.1.1.0/24', this subnet hosts the public-facing Web site and customer portal, where servers are responsible for handling requests from the Internet, providing Web content and user interaction.

DBSubnet: '10.1.2.0/24', this subnet hosts financial institutions' data, including customers' personal information. This subnet requires additional security measures (ACLs/IDS) to secure sensitive data from unauthorised access.

AppSubnet: '10.1.3.0/24', This subnet runs applications and processing jobs, handling database queries and corresponding client requests.

ADSubnet: '10.1.4.0/24', this subnet manages directory services and user authentication, the Active directory server handles login authentication, user and computer account management, and network service authorization.

DevSubnet:'10.1.5.0/24', This subnet provides an environment for application development and testing. A development server is used for coding and testing during the development phase.

EmailSubnet(Exchange Server): '10.1.6.0/24', This subnet handles email from financial institutions, the Email server is used to receive and store emails.

FTPSubnet: '10.1.7.0/24', this subnet is used for file transfer, FTP server supports secure uploading and downloading of files for internal file sharing, backup and transfer.

TapeStorageSubnet: '10.1.8.0/24', this subnet is used for data backup and disaster recovery. Tap Storage is responsible for storing backups of important data to ensure disaster recovery capability.

ManagementSubnet: '10.1.9.0/24', this subnet is used for network and device management. The Manage subnet provides an isolated environment for network maintenance, monitoring and management. (Because a financial institution's infrastructure includes a wide variety of servers, storage devices, and network devices that require regular maintenance, having a separate management subnet better simplifies operations and ensures high security.)

MixeduseSubnet: '10.1.10.0/24' ,this subnet provides wired and wireless device connections.

FinanceSubnet: IP range: '10.1.11.0/24', this subnet is used for a dedicated network for the finance department to handle sensitive financial transactions and data.

CustomerCareSubnet: IP range: '10.1.12.0/24', this subnet is used for customer service department for customer relationship management and support services.

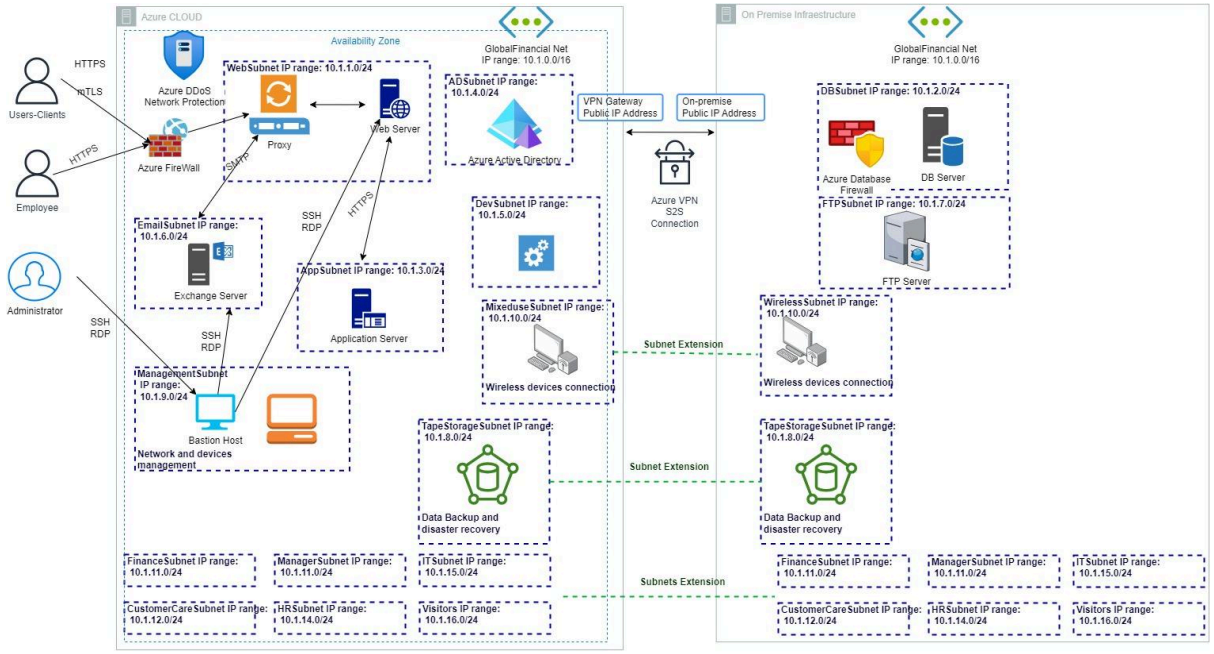
ManagerSubnet: IP range: '10.1.13.0/24', this subnet is used for management staff to ensure adequate privacy and security.

HRSubnet: IP range: '10.1.14.0/24', this subnet is used for HR department to provide employee information and other HR services.

ITSubnet: IP range: '10.1.15.0/24', this subnet is used for IT support team to system maintenance, monitoring and administration.

VisitorSubnet: IP range: '10.1.16.0/24', this subnet is used for visitor to use, provides limited network access for Internet and basic services.

4.2 Topology



Since this is a global financial institution, we chose an advanced Hybrid-Cloud network architecture for the financial institution in order to face the growing volume of data and transactions in the global financial market (VeritisAdmin, 2023). This architecture combines Azure Cloud with On-Premise Infrastructure, Azure Cloud for cost savings, scalability, flexibility, and security. On-Premise Infrastructure with highly customizable policies and configurations to meet the specific needs of physical control, which is critical for financial institution regulatory compliance and data governance. This two ways combine to maximize operational efficiency and data protection.

Azure Cloud Environment:
WebSubnet (10.1.1.0/24): Core portal for web services for employees and customers. Protects against network attacks with Azure Firewall and Azure DDoS protection, and further enhances security and anonymity with proxy servers.
AppSubnet (10.1.3.0/24): Hosts key application servers that handle incoming requests from WebSubnet and interact with database servers.
ADSubnet (10.1.4.0/24): Used for Azure Active Directory services, it provides user authentication and authorization management and is the cornerstone of overall network security.
DevSubnet (10.1.5.0/24): An environment that supports software development and testing, isolating development work to avoid impacting the production environment.
EmailSubnet (10.1.6.0/24): Centralizes all email communication for the organization, with a dedicated Exchange server.
ManagementSubnet (10.1.9.0/24): Includes Bastion Host, providing a secure entry point for network and device management.
FinanceSubnet, HRSubnet, ITSubnet, etc.: Multiple subnets divided by function to support the business operations and data protection needs of specific departments.

MixedUseSubnet (10.1.10.0/24): Provides wired and wireless device connectivity services for employees and visitors, maintaining network flexibility.

On-Premise Infrastructure：
DBSubnet (10.1.2.0/24): Stores sensitive financial data, protected by Azure database firewalls.
FTPSubnet (10.1.7.0/24): Used for file transfer services to ensure secure uploading and downloading of data.
TapeStorageSubnet (10.1.8.0/24): Provides backup and disaster recovery services for critical data.
Cross-environment interconnection.
Azure VPN Gateway: Builds a secure connection from your local infrastructure to your Azure environment, supporting bi-directional data synchronization and service continuity.
Subnet Extensions: Allows subnets within a VNet to extend locally, providing flexible service distribution and enhanced data access.

Security and Compliance:
Azure Firewall: Provides defenses at the network border to ensure compliance and security for all incoming and outgoing traffic.
Azure Active Directory: Provides consistent identity and access management across hybrid cloud environments.

The Hybrid-Cloud architecture we utilize is designed to meet the needs of financial institutions that demand efficiency and the most stringent security standards. This structure provides business agility, continuity and data security. It ensures that any challenges from different attackers can be met in the time to come.

4.3 FW, IPS and IDS

In today's society, financial institutions handle large amounts of money and sensitive data, so that making them attractive targets for cybercriminals (Murray,2024). These growing cybersecurity threats are not only complex and frequent, and attacks on sensitive data and services of financial institutions can lead to catastrophic consequences, so design the security network is key to preventing financial loss, maintaining customer trust and business continuity in the financial industry. Therefore, it is necessary to choose appropriate security measures to protect these resources. As cybersecurity threats continue to advance due to technological developments, the deployment of more advanced firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) has become necessary to secure sensitive data. Azure Firewall Premium, an advanced firewall service, is designed to provide more advanced, robust protection for high sensitive environments to ensure that financial institutions can respond to highly sophisticated security threats and stringent compliance requirements.

Azure Firewall Premium is a cloud firewall service provided by Microsoft Azure, it is an enhancement package to Azure Firewall. This Premium Edition includes all of the features of the Basic Firewall Edition, with the addition of TLS inspection (decrypting, inspecting, and re-encrypting traffic), IDPS (Intrusion Detection and Prevention System), URL Filtering (expanded from FQDN), Web Category Filtering, and Signature-Based IDPS Advanced. It allows financial institutions to more effectively monitor and block malicious traffic in encrypted traffic, real-time monitoring and prevention of network attacks. Sophisticated logging and reporting capabilities, thus providing stronger protection and traceability for financial institutions' cloud resources and meeting financial institutions' operational and regulatory compliance. With Azure Firewall Advanced, we can protect the environment from a wide range of cyber threats and ensure the confidentiality, integrity and availability of your data and applications (Vhorne, 2024).

The recommendation for FireWall is: Azure Firewall Premium. Azure firewall Premium is a hosted, cloud-based cybersecurity service that not only reduces labor costs and provides more advanced threat protection, it also protects highly sensitive resources in Azure virtual networks, which meets the financial institution's data security and availability for future business growth and expansion.

Azure Firewall Premium, in order to meet the increasing performance demands of highly sensitive environments, uses more powerful virtual machine named SKU(Vhorne, 2024). Azure Firewall Premium provides Transport Layer Security (TLS) check, which allows Azure Firewall Premium to encrypt traffic for potential security threats, hide illegal user activity and malicious traffic, and check outgoing traffic established to the Internet. To ensure that the traffic is travelling over a secure TLS connection. This helps prevent malicious parties from attempting to exploit unsecured connections to carry out cyber attacks and steal sensitive data. TLS checks in Azure Firewall Premium can help financial institutions ensure the security of their network communications. Azure Firewall Premium also provides comprehensive network layer and application layer protection. It not only supports condition monitoring, application layer and network layer filtering (alerting users to malicious traffic). It is worth noting that Azure Firewall Premium's virtual machine SKU can auto-scale to a maximum of 100Gbps as traffic grows(Vhorne,2024b), which can ensure that financial institutions can maintain normal function and operation in high-traffic environments. It is very suitable for financial institutions to process large amounts of transaction data on a daily basis.

A recommendation for Intrusion prevention systems (IPS) is the IDPS feature in Azure Firewall Premium. Azure Firewall Premium provides signature-based IDPS that allow rapid detection of attacks by looking for specific patterns. At the same time it is fully managed and constantly updated. It provides real-time threat detection and blocking capabilities to financial institutions utilizing advanced security intelligence analytics and new rules published daily. Azure Firewall Premium is able to monitor traffic and detect possible threats, including malware, cyber attacks, and other security threats. Once a potential threat is detected, IDPS takes automatic blocking action to prevent the threat from causing damage to the network and system. This capability enables financial institution to maintain a high level of security in a cloud environment and respond quickly to a variety of real-time security threats. IDPS also uses a dedicated IP range to identify inbound, outbound, or internal traffic. Each signature is applied to a specific traffic direction based on the provided

signature rules, and each signature has an internal ID, which is also displayed in the Azure firewall logs to prevent untraceable security attacks.
The recommended intrusion detection systems (IDS) are: IDPS and Azure Security Center's Defender for Cloud(threat protection feature), IDPS we have described in the previous paragraph that we will not go into more details. Let us talk about Defender for Cloud(TerryLanfear, 2023), an extended security management service, provides advanced threat protection to improve the security of resources in the Azure cloud environment. In Defender for Cloud, IDS uses behavioural analytics and machine learning techniques (Microsoft has access to data on large amounts of cloud network activity) to detect possible intrusions. Defender for Cloud also uses anomalies to detect and identify threats, which is more personalised than "behaviour analytics" and can be detected based on a baseline deployed by the user. Defender for Cloud will also continuously and automatically detect cloud resource configuration issues, this service can provide recommendations to improve security, and help financial institutions comply with industry standards and regulatory requirements through compliance scores. For financial institutions, the threat identification, security and compliance capabilities provided by Defender of Cloud are extremely valuable. It helps financial institutions not only protect sensitive financial data, but also ensure that financial institutions can meet stringent regulatory requirements can enable financial institutions to achieve a higher level of security and operational efficiency.

4.4 Network Security Rules and Firewall policies

4.4.1 Network Security Group

One of Azure's features to control network traffic is through Azure Security Group as known as NSG. This option enables setting security rules in a NSG to permit or deny network traffic entering or leaving different Azure resources. It is possible to determine the protocol, port, source and destination per resource, and each rule individually.
The table below shows the proposed Security Groups and detailed rules to deploy on the Cloud proposed topology.

Name	Priority	Source	Source Port	Destination	Dest. Port	Protocol	Access	Direction
BastionHostSSH	100	Any	*	BH IP address	22, 3389	TCP	Allow	Inbound
BastionHostDenyAll	110	Any	*	BH IP address	*	TCP	Deny	Inbound
WebSunetAllowHTTPS	100	Any	*	10.1.1.0/24	443	TCP	Allow	Inbound
WebSunetBastionHostAllowSSH	110	BH IP address	*	10.1.1.0/24	22	TCP	Allow	Inbound

ExchangeWebSubnetAllowSMTP	130	10.1.1.0/24	*	10.1.5.0/24	25	TCP	Allow	Inbound
DatabaseTraffic	100	10.1.0.0/16	*	10.1.2.0/24	1433	TCP	Allow	Inbound
FTPLimitedTraf	110	10.1.0.0/16	*	10.1.7.0/24	21	TCP	Allow	Inbound

Details of NSG Rules

BastionHostSSH: This rule applies to control that the Bastion Host could only be accessible via SSH(Secure Shell protocol) and RDP. Bastion Host allows the Administrator to access Cloud Infrastructure and resources without directly exposing it to the internet. We deploy this rule in the bastion host NIC level.

BastionHostDenyAll: with this rule, we limited other inbound traffic to Bastion Host. We deploy this rule in the bastion host NIC level.

WebSubnetAllowHTTPS: Access to Corporation Systems will be via HTTPS protocol(TLS latest version, mTLS for sensitive client's data transaction) using default port 443.

WebSubnetBastionHostAllowSSH: Only SSH traffic is allowed from Bastion Host to connect to WebSubnet, any other traffic port is prohibited.

ExchangeWebSubnetAllowSMTP: this allows SMTP traffic that is handled via the Proxy server.

DatabaseTraffic: to allow traffic to/from database using default port and limiting to only VNet range. By default, access to Databases from Public IP are disabled.

FTPLimitedTraf: this rule allows ftp traffic requested from ip range Vnet, any other source will be blocked.

NSG rules are subject to changes(add, modify current, deletion) according to Organisation Security needs.

4.4.2 Azure Firewall

On the other hand, Azures provides a stateful Firewall protection services to manage in a centralised way the network traffic that comes and goes from outside to the Organization. Azure FW includes Intrusion Detection and Prevention System(IDPS), a Transport Layer Security Inspection, URL filters and
Microsoft threat intelligence feeds managed by Microsoft to alert and deny network destinations that are identified as malicious (Magušić, n.d.-b).

Azure Firewall policy rules could be set according to 3 main categories: Network, Application and Destination Network Address Translation(DNAT).
A set of firewall rules for the Financial Organization cloud scenario is proposed. Also, we will define a tableRoute on Azure firewall configuration to manage all internet traffic that goes to the VNet to pass to the Firewall first.
Network collection rule will be create to filter inbound/outbound IP Public traffic used to access the Vnet
DNAT collection rule will be created to translate the public IP to private IP to reach Virtual Servers on the Vnet.
Finally, WAF rule collection will be created and changed to *Prevention* mode. In this mode Azure-managed OWASP rules are enabled by default (vhorne, 2023)

4.5 Network protection recommendations for data security and privacy

4.5.1 DDoS Network Protection

As part of Control: ISM-1431 of the Australia ISM, to assure availability, DDoS protection should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP (*Guidelines for Networking | Cyber.gov.au*, 2023).

This service is applied to the entire virtual network and provides DDoS protection for all public IP addresses that are associated with resources in the virtual network (*Chapter 8: Designing and Implementing Network Security - Designing and Implementing Microsoft Azure Networking Solutions [Book]*, n.d.).

4.5.2 Client-Servers communication

TLS nowadays is the most talked-about technology when it comes to network security. Is a session layer protocol. TLS protocol.

For very sensitive information it will be used mutual TLS (mTLS). It establishes trust in both directions between the client and the server. Both the client and the server have their own certificates, and each certificate is authenticated with their public or private key pair.

4.5.3 Databases data traffic

For securing data in transit in and out the databases, Azure SQL Database supports the Tabular Data Stream (TDS) protocol, which integrates a TLS handshake.

4.5.4 Cloud-On premises communication

To connect Cloud Infrastructure with our On-premises one, it will be used VPN Site to Site Azure Services. It uses IPsec/IKE (IKEv2) VPN tunnel protocol. IPS is a suite of network protocols and technologies to ensure data in transit confidentiality and integrity.

IKE (Internet Key Exchange) is a protocol responsible for the origin authentication, the creation and management of keys for subsequent communications. IKE is responsible for session establishment between two entities. Key management is implemented to accommodate the creation and maintenance of keys that are used in the encryption

processes to provide the security services of IPSec (Chapter 9: Key Management - a Technical Guide to IPSec Virtual Private Networks [Book], n.d.).

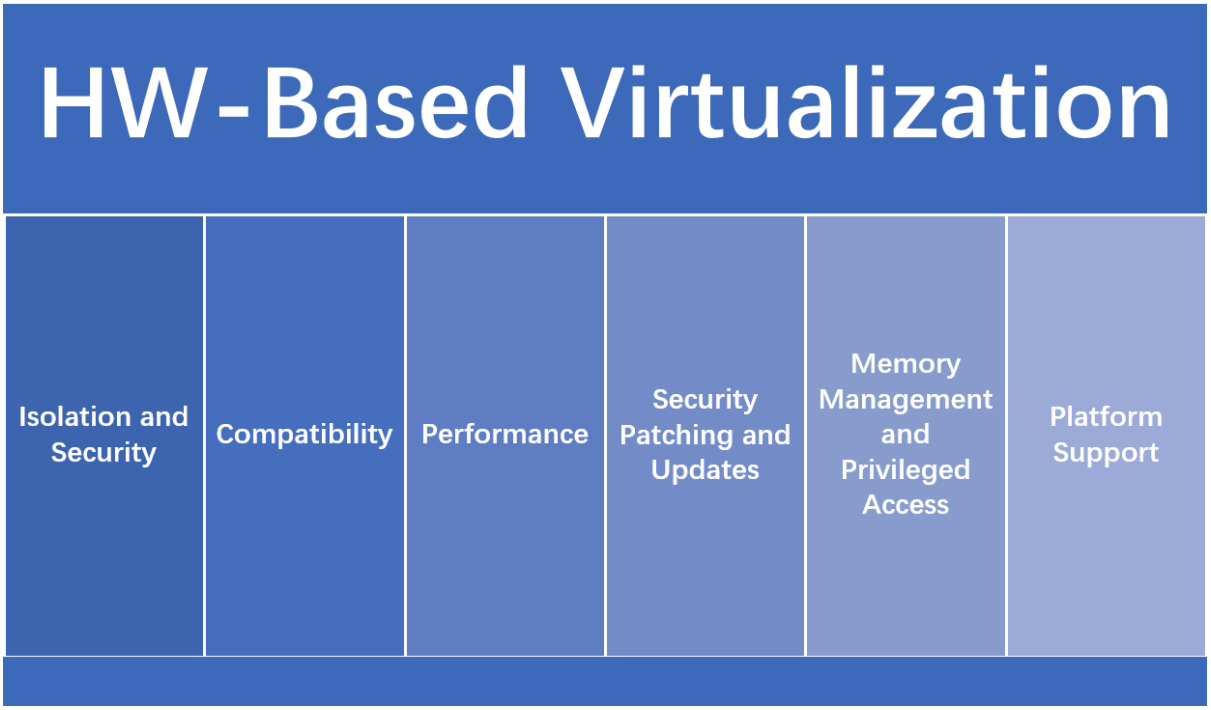
5. Infrastructure Security

In this section, the choice of virtualization, hardening measures for the infrastructure security, patch management process and VM isolation strategies will be discussed.

5.1 Virtualization of Infrastructure

As specified above, the PaaS and hybrid storage are recommended, the security of infrastructures in the local data centre and cloud data centre should both be discussed here. As the data centres store sensitive data, a high security level should be applied. Also, migration of local physic servers should also be considered. Therefore, HW-based virtualization is highly recommended.

If HW-based virtualization is chosen, following impacts should be considered:



Isolation and Security

The foundational principle of strong isolation between virtual machines (VMs) in a hardware-based virtualization environment significantly mitigates the risks associated with unauthorised access and data leakage between VMs(Microsoft, 2024). Therefore in order to ensure overall system security and data integrity, this isolation enforces that each VM operates independently from others.

In hardware-based virtualization, VMs are encapsulated within their own virtualized environments, isolated from each other and from the underlying physical hardware. This physical level isolation is achieved by hypervisor. Hypervisor manages and arbitrates access to hardware resources such as CPU, memory and storage.Each VM operates as if it were running on dedicated hardware, oblivious to the presence of other VMs on the same physical host. Attack surfaces are greatly reduced by this structure., making it challenging for attackers to conduct boundary breach which will lead to unauthorised access or data compromising.

Compatibility and Versatility

The ability of hardware-based virtualization to support unmodified guest operating systems (OSs) facilitates seamless migration of existing servers into virtualized environments (Geekforgeeks, 2023). Deployment of different OSs and applications are allowed by this feature without modification of OSs, which enables compatibility with former systems and applications.

By leveraging hardware virtualization technologies such as Intel VT-x or AMD-V, the hypervisor can present a consistent and standardised virtual hardware platform to guest OSs. This abstraction layer shields guest OSs from the underlying physical hardware specifics, enabling them to run without modifications. Therefore, the organisation can move all their workload to cloud environments with minimal disruption.

Performance

While hardware-based virtualization provides robust isolation and flexibility, it introduces overhead due to the emulation of hardware resources. This overhead can become more pronounced under conditions of high computational demand or resource contention among multiple VMs sharing the same physical hardware (Schlosser, D., Duelli, M., Goll, S., 2011).

The supervisor's role in managing virtualization introduces a layer of indirection between the guest OS and physical hardware. . The critical achievement of the virtualization can influence the performance especially during rushing hours. However, advancements in virtualization technologies, coupled with hardware enhancements like nested paging and extended page tables, have significantly minimised performance overheads, enabling near-native performance for most workloads.

Security Patching and Updates

Maintaining the security of a virtualized environment involves regular patching and updating of both the hypervisor and guest OSs. While patching the hypervisor can be relatively straightforward, applying updates to guest OSs can be complex and time-consuming, especially in large-scale deployments with diverse operating environments.

In a virtualized/cloud environment, patching strategies are critical as they can mitigate potential vulnerabilities and eliminate attack surfaces. Basically, automated patch management tools can be used to streamline the process of update deploying on multiple and variable VMs remotely and consistently. On the basis of that, leverage virtualisation-ware security solutions should be established to enhance identifying and remediating vulnerabilities specific to cloud environments.

Memory Management and Privileged Access

In the virtualized & cloud environments, in order to prevent unauthorised access and data leakage, effective and secure memory management is required. To achieve this, the hypervisor enforces strict memory isolation policies.

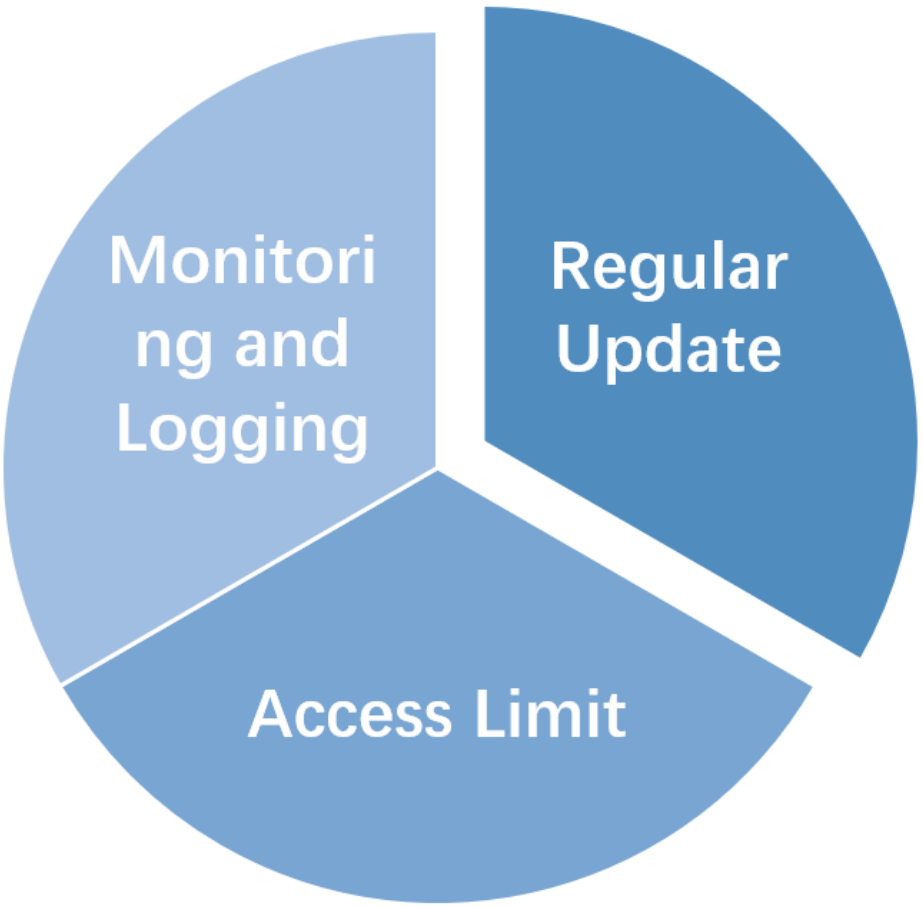
However, despite robust isolation mechanisms, the presence of a privileged super admin for the hypervisor introduces a potential insider threat. This kind of malicious manager has privileged access to hypervisor and guest VMs, which compromise the integrity of resources. Therefore, strict access controls with least privilege principle are necessary in this structure to minimise risks of insider threats and other unauthorised access.

Platform Support

Azure provides the company with a reliable and clearly defined security policy framework supported by technologies like Hyper-V (Microsoft, 2021). Besides, Azure offers other integrated security tools such as Azure Security Center and Azure Sentinel to enhance the security of the system by actively monitoring , detecting and responding. With the support of these tools, the company can build a robust security stance under the guidance of CIS benchmarks and NIST guidelines.

5.2 Hardening Measures for Hypervisors and Host OSs

After the implementation and deployment of infrastructure, these measures should be carefully considered to enhance the security of hypervisors and host OSs (Openstack, 2022):



Regularly Update Hypervisor Software and Firmware

Ensure that the hypervisors and host OSs are regularly updated with the latest patches to address any known vulnerabilities, which is one of the foundational pillars in securing hypervisors and host OSs. With this critical practice, vulnerabilities and threats are prevented. Regular updates not only ensure the security of hypervisors & host OSs but also the security of underlying firmware.

To implement this measure effectively, the company should establish a structured patch management process. This process should consist of regular vulnerability assessments, testing of patches in non-production environments and scheduled deployment of updates during maintenance windows to minimise disruption to important operations. Moreover, for a large cloud services structure, to ensure

timely and comprehensive coverage across all hypervisor and host instances, automation tools can be used.

Limit Hypervisor Access

Access control is a fundamental aspect of hypervisor and host OS security, aimed at restricting administrative privileges and user access to essential functions only. Use popular access control mechanisms such as Identity and Access Management or Role-Based Access Control to enforce the conduct of least privilege principle, which can reduce the attack surface and minimise the damage of potential security breaches.

The IAM system enables the company to define role-based access policies and make sure that users can only acquire necessary privileges to perform their tasks. For example, administrators may have full control over hypervisor configurations and virtual machines, while users with limited roles can access specific resources for their designated purposes. RBAC complements IAM by structuring access around job responsibilities, further refining permissions based on organisational hierarchy and operational needs.

Besides, multi-factor authentication and privileged access management solutions should also be applied to the access control procedure. The application of this technique will add an extra layer of security by requiring users to authenticate with multiple factors such as passwords, biometrics or hardware tokens, which will bring much more strength and robustness to the access control. While MFA ensures that the authentication is secure, PAM solutions will enforce strict protocols for accessing critical systems and conducting audits to track administrative activities by monitoring and managing privileged accounts.

Monitoring and Logging

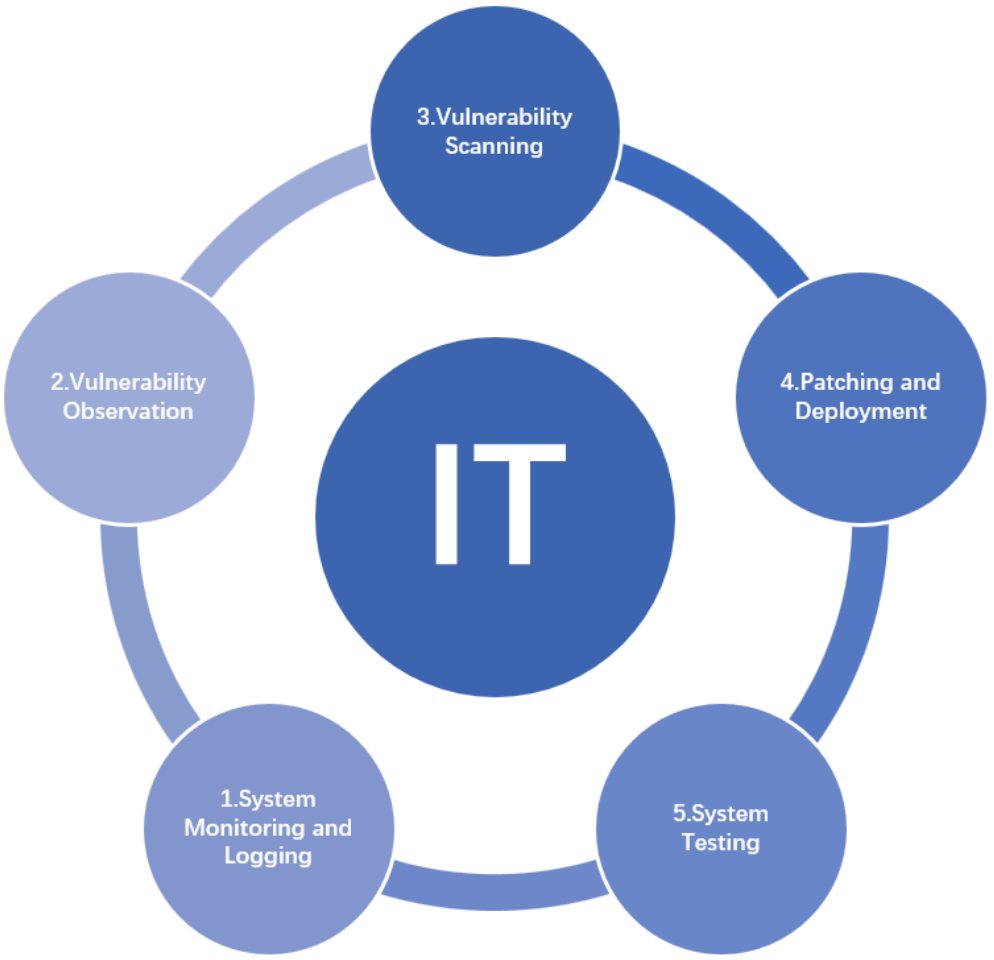
It is critical to involve monitoring and logging systems in the infrastructure framework for the purpose of effective detection and response to incidents happening inside/outside hypervisors and host operating systems. These subsystems provide administrators ability to dive into system activities, which makes it much easier for them to identify unusual behaviours, activities or traffic.

To achieve effective monitoring, deploy intrusion detection systems (IDS) or intrusion prevention systems (IPS) tailored for virtualized environments. All the network traffic, system logs and behaviour patterns will be analysed by these systems to detect and identify suspicious activities.

Comprehensive logging is essential, capturing detailed records of system events, user activities, and administrative operations within hypervisors and host operating systems (OSs). Logs should include timestamps, event types, originating IP addresses, and relevant metadata for forensic analysis and auditing.

5.3 Patch Management Process

According to the case of the company and decisions made above, the following process should be established by the IT department to maximise the security of the system (TechTarget, 2022).



In the patch management process, there are five key phases that organisations should follow to ensure the security and stability of their IT systems.

Phase 1: Continuous Monitoring and Information Gathering

The first phase involves ongoing monitoring of IT systems and gathering relevant information. The IT department should systematically monitor device types, operating system (OS) versions, software versions, and other pertinent details. While these data are gathered regularly, the data will be used to assess the robustness, security level and parching priority. Besides, the data will also play a crucial role in vulnerability tracking, allowing the company to identify potential vulnerabilities that may be exploited by malicious attackers in the system.

Phase 2: Vulnerability Tracking and Assessment

Next, organisations must track the latest vulnerability information from device, service, and application providers. The term track means that the IT team should constantly monitor security forums, threat intelligence feeds, and other reputable sources to stay informed about emerging vulnerabilities relevant to their IT environment. By tracking these developments, the company can effectively assess potential risks and prioritise actions to mitigate them.

Phase 3: Vulnerability Scanning and Tagging

After gathering vulnerability information, conduct comprehensive scans across the IT infrastructure. Identify and tag all devices, operating systems, applications, and resources susceptible to identified vulnerabilities. Based on the reports of scanning, related devices, OSs, applications and other resources can be tagged for further patch up. In this phase, not only the IT team should be involved in the testing, third-party testers can also be introduced in order to enhance the professionality and coverage of the test. In the test, the domain of the penetration and scanning should be strictly restricted to avoid unauthorised access, data leakage and other potential security risks.

Phase 4: Patch Acquisition and Deployment

Once vulnerabilities are identified and tagged, obtain or implement appropriate patches from vendors or reliable sources. The IT team should take the responsibility to acquire, identify and verify the reliability and timeliness of patches. After obtaining trustful patch resources and before deployment, ensure patches are thoroughly tested for compatibility and effectiveness. In the deployment process, techniques supported by Azure such as Hyper-V should be used to ensure the deployment is effective and across multiple devices & applications.

Phase 5: Post-Deployment Testing and Validation

Following patch deployment, conduct thorough testing to validate the effectiveness of applied patches in mitigating vulnerabilities. Perform system-wide tests to confirm that identified vulnerabilities have been successfully addressed without introducing new issues. Besides, the performance should also be tested and compared to ensure that all the services are running as intended.

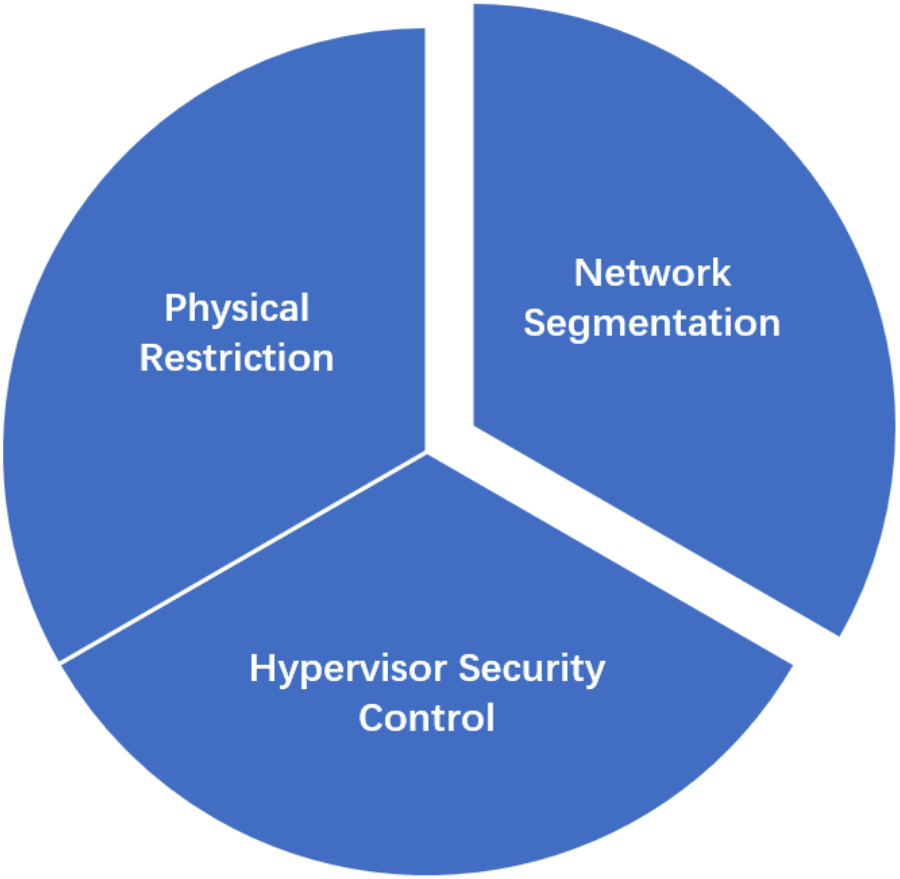
Continuous Improvement: Iterative Monitoring and Logging

After completing the initial patch management cycle, return to continuous monitoring and logging. Regularly monitor the system for new vulnerabilities, changes in device configurations, and emerging threats.

Following these phases diligently helps organisations maintain a structured and effective approach to patch management, ultimately enhancing the security and resilience of their IT infrastructure.

5.4 Strategies for VM Isolation and Segmentation

To minimise the risk of lateral movement within the structure, it is essential to have strong and robust strategies for VM isolation and segmentation. To address the issue of lateral movement, following three strategies are recommended:



Network Segmentation and Micro-segmentation.

According to the sensitive levels and trust levels to separate VMs into different subnets. This kind of technique limits communication interfaces between VMs and reduces the scope of lateral movement if there is a compromise.

Within the VNets, using Azure Firewall or NSGs to split data centres into separate security pieces down to the application level and then implement security controls and provide services for each unique segment. With this technique, security rules can be defined and enforced at VM and application level and control the traffic flows (Hewitt, 2023).

Network segmentation and micro-segmentation offer significant benefits, including limiting the lateral movement of attackers within the network in the event of an attack on a virtual machine, thereby minimising the overall impact. In addition, compliance with regulatory standards often requires robust network segmentation, which helps organisations demonstrate compliance and reduces

risks such as data leakage and unauthorised access. Moreover, these technologies are scalable, adapting to changes in infrastructure by easily incorporating new virtual machines or applications into existing network segments with appropriate security controls. Centralised management of security policies through tools such as Azure Firewall or Network Security Groups (NSG) simplifies administration while ensuring consistent security across the infrastructure.

For this case, it is recommended to create separate subnets for different departments and functional areas.

Hypervisor-Level Security Controls

Deploy firewalls at the hypervisor level to provide an additional layer of defence. This security level enforces policies on VM-to-VM communication, allowing admins to control and restrict traffic based on policies and criteria.

Besides, virtual switch access controls are also recommended. This technique enables admins to define rules that control the traffic between VMs and external networks. Based on this, the network can achieve network segmentation and traffic monitoring easily (yosharm, 2022).

The use of firewalls at the hypervisor level allows for the creation of different network segments within the virtual infrastructure. This segmentation of network segments is key to containing potential security breaches and minimising the impact of compromised VMs. Administrators can precisely control VM-to-VM communication through hypervisor-level firewalls, thereby defining specific policies and standards for traffic and ensuring that only authorised communication takes place between VMs. In addition, leveraging virtualisation platforms such as Hyper-V for policy management and access control optimises performance by allowing security-related tasks to be handled efficiently at the hypervisor level without significant impact on VM performance. Meanwhile, the combination of hypervisor-level firewalls and virtual switch access control provides a comprehensive security policy for virtualized environments, complementing traditional perimeter defences and host-based security measures to strengthen the overall network security posture.

For this case, it is recommended to use virtualization platforms such as Hyper-V to achieve policy management and performance optimization on the hypervisor level. And for virtual switch access control, port-level access controls are recommended as there may be servers running multiple services.

Applying hypervisor-level security controls, efficient resource management is provided by allocation and monitoring resources among VMs, which prevent resource contention and ensure fair resource allocation for guest OSs. Besides, hypervisor-level security controls offer secure boot mechanisms and integrity verification of VMs. This feature ensures that only trusted VMs are allowed to run

on the hypervisor and protect the system against malicious malware and attackers.

Physical Restricting

As the network is running on a hybrid method, the physical connection between physical devices and external internet should be carefully restricted. Only necessary connection should be applied to the devices. If unnecessary connections are applied to the system, there will be risks of unauthorised access and data leakage, which can cause large damage to the business and performance of the system.

For this case, it is recommended to separate different departments into different physical subnets and use router & firewall to filter all the traffic inbound and outbound. Besides, inside each subnet, only necessary connections should be applied. For example, an ad server for a department should not connect to DB servers as this is not necessary.

After applying physical restrictions, different parts of the network are isolated from each other and malicious breaches and attacks are limited to minor domains. Also, fault isolation is introduced to the system as failure of a certain part can not affect the entire environment and troubleshooting & maintenance will be easier. Last but not the least, traffic management is much easier as directing and prioritising network traffic within specific segments is facilitated.

Reference

Alzakholi, O., Shukur, H., Zebari, R., Abas, S., & Sadeeq, M. (2020). Comparison among cloud technologies and cloud performance. *Journal of Applied Science and Technology Trends*, *1*(1), 40-47.

AUSTRAC. (2022). *Record-keeping | AUSTRAC*. Austrac.gov.au. https://www.austrac.gov.au/business/core-guidance/record-keeping

Australian Home Affairs. (2019). *Data retention obligations*. Homeaffairs.gov.au. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations

Ayuya, C. (2023, February 3). *The importance of data retention policies*. TechRepublic. https://www.techrepublic.com/article/the-importance-of-data-retention-policies/

Basatwa, G. (2023, March 7). *AES-256 Encryption - Everything You Need to Know*. AppSealing. https://www.appsealing.com/aes-256-encryption/

Belmansour, T. (2021, March 26). *Manage your data retention policies with Azure Storage Lifecycle Management*. DEV Community. https://dev.to/tidjani/manage-your-data-retention-policies-with-azure-storage-lifecycle-management-39nh

Brook, C. (2022, November 23). *5 Common Data Classification Types*. Digital Guardian. https://www.digitalguardian.com/blog/5-common-data-classification-types

Brook, C. (2023, December 19). *Everything You Need to Know About Microsoft DLP*. Www.digitalguardian.com. https://www.digitalguardian.com/blog/everything-you-need-know-about-microsoft-dlp

BuffALO. (2023, November 17). *What Is 256-bit AES Encryption and Why Do You Need It*. Www.buffalotech.com. https://www.buffalotech.com/blog/what-is-256-bit-aes-encryption-and-why-do-you-need-it

Chapter 8: Designing and Implementing Network Security - Designing and Implementing Microsoft Azure Networking Solutions [Book]. (n.d.). Www.oreilly.com. Retrieved April 12, 2024, from https://learning.oreilly.com/library/view/designing-and-implementing/9781803242033/

Chapter 9: Key Management - A Technical Guide to IPSec Virtual Private Networks [Book]. (n.d.). Www.oreilly.com. Retrieved April 12, 2024, from https://learning.oreilly.com/library/view/a-technical-guide/9780203997499/Part09.html#a157

Cherylmc. (n.d.). Azure VPN Gateway topologies and design. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/vpn-gateway/design

CLOUDFLARE. (2024). *What is the difference between HTTP and HTTPS?* Why Use HTTPS?; CLOUDFLARE. https://www.cloudflare.com/en-gb/learning/ssl/why-use-https/

Cocoara, Z. (2024, January 31). *DLP Security: Essentials for Business Data Protection*. Endpoint Protector Blog. https://www.endpointprotector.com/blog/dlp-security/

Crook, H., Raza, S., Nowell, J., Young, M., & Edison, P. (2021). Long covid—mechanisms, risk factors, and management. *bmj*, *374*.

De Rojas, I., Moreno-Grau, S., Tesi, N., Grenier-Boley, B., Andrade, V., Jansen, I. E., ... & Sleegers, K. (2021). Common variants in Alzheimer's disease and risk stratification by polygenic risk scores. *Nature communications*, *12*(1), 3417.

ElazarK. (2023, December 10). *Microsoft Defender for Storage - the benefits and features - Microsoft Defender for Cloud*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction

Fisk, J. (2023, December 11). *Data retention and the GDPR: Best practices for compliance*. Outsourced Data Protection Officers GDPR and Data Protection Compliance. https://www.dpocentre.com/data-retention-and-the-gdpr-best-practices-for-compliance/

Franklin, R. (2020, March 13). *AES vs. RSA Encryption: What Are the Differences?* Precisely. https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences

GDPR. (2018). *General data protection regulation (GDPR)*. General Data Protection Regulation (GDPR); Intersoft Consulting. https://gdpr-info.eu/

Geeksforgeeks. (2023, March 15). *Hardware Based Virtualization*. https://www.geeksforgeeks.org/hardware-based-virtualization/

Guidelines for Networking | Cyber.gov.au. (2023). Cyber.gov.au.

Hashemi-Pour, C. (2023, July). *What is public data? - Definition from WhatIs.com*. SearchCIO. https://www.techtarget.com/searchcio/definition/public-data

Hewitt, N. (2023, June 26). *Demystifying Microsegmentation vs. Network Segmentation • TrueFort*. TrueFort. https://truefort.com/microsegmentation-vs-network-segmentation

Herzberg, B. (2023, October 16). *4 Benefits of Role-Based Access Control (RBAC) and How to Implement It*. DATAVERSITY. https://www.dataversity.net/4-benefits-of-role-based-access-control-rbac-and-how-to-implement-it/

Housing and Digital Economy Communities. (2016, July 1). *Confidential information*. Www.business.qld.gov.au. https://www.business.qld.gov.au/running-business/risk/ip/types/trade-secrets https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-networking

Indu, I., Anand, P.M.R. and Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal, [online] 21(4), pp.574–588. doi:https://doi.org/10.1016/j.jestch.2018.05.010.

Jena, B. K. (2023, February 9). *What Is AES Encryption and How Does It Work? - Simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

khdownie. (2023, January 20). *Introduction to Azure Files*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction#why-azure-files-is-useful

Kranz, G. (2022, July). *What is Data Classification and Why is it Important?* SearchDataManagement. https://www.techtarget.com/searchdatamanagement/definition/data-classification

Lekatis, G. (2002). *Sarbanes-Oxley Act*. Sarbanes-Oxley-Act.com. https://sarbanes-oxley-act.com/

León-Castillo, A., De Boer, S. M., Powell, M. E., Mileshkin, L. R., Mackay, H. J., Leary, A., ... & Bosse, T. (2020). Molecular classification of the PORTEC-3 trial for high-risk endometrial cancer: impact on prognosis and benefit from adjuvant therapy. *Journal of Clinical Oncology*, *38*(29), 3388.

Lutkevich, B. (2020). *What is HIPAA (Health Insurance Portability and Accountability Act)?* SearchHealthIT. https://www.techtarget.com/searchhealthit/definition/HIPAA

Magušić, B. (n.d.-b). Azure Security. O'Reilly Online Learning. https://learning.oreilly.com/library/view/azure-security/9781633438811/OEBPS/Text/03.htm#heading_id_9

Microsoft. (2021, July 30). *Hyper-V Technology Overview*. https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview

Microsoft. (2022, August 11). *Introduction to Blob (object) storage - Azure Storage*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

Microsoft. (2024, August 11). *What is a virtual machine(VM)*. https://azure.microsoft.com/en-au/resources/cloud-computing-dictionary/what-is-a-virtual-machine

Microsoft (2024). What is Identity Access Management (IAM)? | Microsoft Security. [online] www.microsoft.com. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam.

Microsoft (2024). What is two-factor authentication (2FA)? | Microsoft Security. [online] www.microsoft.com. Available at: https://www.microsoft.com/en-au/security/business/security-101/what-is-two-factor-authentication-2fa.

msmbaldwin. (2024, January 30). *Azure Key Vault Overview - Azure Key Vault*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/key-vault/general/overview

Murray, L. (2024b, January 8). *Financial Services Cybersecurity | Threats & Solutions | Imperva*. Learning Center. https://www.imperva.com/learn/data-security/financial-services-cybersecurity/

Openstack. (2022, Jan 8). *Hardening the virtualization layers*. https://docs.openstack.org/security-guide/compute/hardening-the-virtualization-layers.html

Puneet. (2020, September 23). *What is Key Management? | How does Key Management work? | Encryption Consulting*. Encryption Consulting. https://www.encryptionconsulting.com/education-center/what-is-key-management/

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

Schlosser, D., Duelli, M., Goll, S. (2011). *Performance Comparison of Hardware Virtualization Platforms*. In: Domingo-Pascual, J., Manzoni, P., Palazzo, S., Pont, A., Scoglio, C. (eds) NETWORKING 2011. NETWORKING 2011. Lecture Notes in Computer Science, vol 6640. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20757-0_31

Slagle, R. (2023, August 15). *Data Classifications in Small Business: Navigating Information Sensibly*. Www.linkedin.com. https://www.linkedin.com/pulse/data-classifications-small-business-navigating-sensibly-ryan-slagle/

SnapLogic. (2024). *Azure Blob Storage*. SnapLogic. https://www.snaplogic.com/glossary/azure-blob-storage

Squirrel, S. the S. (2023, July 23). *AES256 Encrypt: Is AES-256 Secure?* Kiteworks | Your Private Content Network. https://www.kiteworks.com/secure-file-sharing/unlocking-the-security-of-aes-256-a-comprehensive-guide/

TechTarget. (2022, May 24). *6 best practices for VM patch management*. https://www.techtarget.com/searchitoperations/tip/5-best-practices-for-VM-patch-management

TerryLanfear. (2023, October 20). *Azure Threat Protection*. Microsoft Learn. https://learn.microsoft.com/zh-cn/azure/security/fundamentals/threat-detection#microsoft-defender-for-cloud

The Security Company Limited. (2023, October 17). *Why is it important to support my staff with security awareness training?* Www.linkedin.com. https://www.linkedin.com/pulse/why-important-support-my-staff-security-awareness-training-kzyke/

VeritisAdmin. (2023). Cloud vs On-Premise: IT infrastructure model of your choice? *Veritis*.https://www.veritis.com/blog/cloud-vs-on-premise-it-infrastructure-model-of-your-choice/

Vhorne. (2023, August 24). Create Web Application Firewall (WAF) policies for Application Gateway. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag?source=recommendations

Vhorne. (2024, January 30). *Azure Firewall Premium Features*. Microsoft Learn. https://learn.microsoft.com/zh-cn/azure/firewall/premium-features

Vhorne. (2024b, April 9). *Choose the right Azure Firewall version for your needs*. Microsoft Learn. https://learn.microsoft.com/zh-cn/azure/firewall/choose-firewall-sku

Viswanath, K. (2023, May 24). *General Availability: Introducing Azure AD Support for Azure Files SMB shares REST API*. TECHCOMMUNITY.MICROSOFT.COM. https://techcommunity.microsoft.com/t5/azure-storage-blog/general-availability-introducing-azure-ad-support-for-azure/ba-p/3826733#:~:text=With%20Azure%20AD%20support%2C%20applications

Wright, C. (2008). Chapter 20 - risk management, security compliance, and audit controls. In C. Wright (Ed.), *The IT Regulatory and Standards Compliance Handbook* (pp. 577–607). Syngress. https://doi.org/10.1016/B978-1-59749-266-9.00020-5

yosharm. (2022, November 11). *Hypervisor security on the Azure fleet - Azure Security*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/security/fundamentals/hypervisor

Zhang, X. X., Tian, Y., Wang, Z. T., Ma, Y. H., Tan, L., & Yu, J. T. (2021). The epidemiology of Alzheimer’s disease modifiable risk factors and prevention. *The journal of prevention of Alzheimer's disease*, *8*, 313-321.