A document with text and numbers

Description automatically generated with medium confidence

1. **Executive Summary**

Phoenix Capital, a dynamic financial services firm focused on personal wealth management, is poised to enhance its operational efficiency by transitioning to a cloud computing model. This move aims to resolve the firm’s challenges with IT infrastructure scalability and reliability.

Introduction to Business Challenges:

Phoenix Capital is grappling with:

·   Inflexibility of on-site servers during high trading volumes.

·   Exorbitant upkeep for the existing IT systems.

·   Subpar disaster recovery processes.

·   Increasing the necessity for remote access for staff and clientele.

Table of Contents

[2. Current limitations 4](#_Toc157364910)

[3. NEED FOR MITIGATION 5](#_Toc157364911)

[4. Cloud Implementation model 6](#_Toc157364912)

[5. Service Model 8](#_Toc157364913)

[6. Deployment Model 10](#_Toc157364914)

[7. Service Selection 11](#_Toc157364915)

[8. Cost Involvement 13](#_Toc157364916)

[9. Cost Management Considerations in Cloud Migration 13](#_Toc157364917)

[10. Security 14](#_Toc157364918)

[11. Integration of Cost Management Strategies 14](#_Toc157364919)

[12. Challenges and Mitigations 15](#_Toc157364920)

[13. Conclusion 16](#_Toc157364921)

[14. References 17](#_Toc157364922)

[Appendix 18](#_Toc157364923)

[Group Activity Report 18](#_Toc157364924)

Table of Figures

[Figure 1: Cloud Implementation Model 5](#_Toc157357172)

[Figure 2: Service Model 6](#_Toc157357173)

[Figure 3: Deployment Model 8](#_Toc157357174)

[Figure 4: Pricing Model (Part A) 9](#_Toc157357175)

[Figure 5: Service Provider (Feature Comparison) 10](#_Toc157357176)

[Figure 6: Cost Involvemnt 11](#_Toc157357177)

**1.** **Current limitations**

1.     The current on-premises infrastructure of Phoenix Capital is posing several challenges:

2.     **Limited accessibility:** The current system is highly limited as the staff are only able to work when being present at the workplace, leading to complaints and dissatisfaction among the staff due to the recent COVID phase they faced.

3.     **Limited resources:** The on-premises servers are struggling to scale with the increasing demand, leading to performance degradation during peak times

4.     **High Expenditure on maintenance:** Maintaining the current outdated servers significantly strains the company's finances. And the upgrading of the on-premises servers requires substantial financial investments. Thus, the company is looking for a way to reduce the server operation and maintenance costs while upgrading it.

5.     **Lack of adaptability:** The infrastructure of the company is an old model, leading to the need for more adaptability to adapt to the changing business requirements in the rapidly developing world. This makes it challenging for Phoenix Capital to stay competitive in the dynamic retail market.

6.     **Limited Disaster Recovery:** The current disaster recovery plan needs to be more comprehensive, posing a risk to business continuity in case of unforeseen events, and the business is still utilising only a single level of security.

7.     **No staff monitoring: The devices are not monitored when working, leading to the threat of a security breach being** more prominent.

**3.** **NEED FOR MITIGATION**

Phoenix Capital still uses old technology even when the company desperately needs higher computational power and devices. The above limitation explains the need for the changes to be made in the company. So, the only way for the company to solve their current challenge is to migrate to the cloud. Some of the advantages of making the migration are as follows:

·   The company's scale and operational power will be highly increased and available on demand.

·   The maintenance cost of the new server will be reduced.

·   There will be more available data backup in case of data corruption or security breach.

·   The staff will be able to be monitored when using the technology, reducing the risk of data theft and maintaining data confidentiality.

·   The work will be done remotely, allowing the work to be more adaptable and flexible.

Everything has advantages and disadvantages. Some of the benefits of doing the migration are:

·   The staff feels their privacy is stolen as they will be monitored when working by the system.

·   Even though after installation, the maintenance cost of the server will be highly reduced, there will be some expenditure when conducting migration to the new system.

To solve the critical issue Phoenix Capital faces, the IAAS (Infrastructure as a Service) is the best Cloud service layer applicable. The Cloud deployment model is the Hybrid model.  The major reason for that is:

· **Flexibility and Control:** One of the issues faced by the Company is being too rigid and not having much flexibility in it. So, applying this model will allow more flexibility to design personalized solutions that meet the particular needs of the company's individual.

·   **Cost:** The company does not wish to spend much money implementing the new model. This makes this model the best one as it provides scalability in terms of cost. The company will only have to pay for any extra capacity if required.

·   **Security:** The company is still using only the basic level of security and is not even using two-factor authorisation. However, with the application of this model, the chances of attacks like data theft by attackers are considerably reduced.

**4.** **Cloud Implementation model**

To solve the critical issue Phoenix Capital faces, the IAAS (Infrastructure as a Service) is the best Cloud service layer applicable. The Cloud deployment model is the Hybrid model.

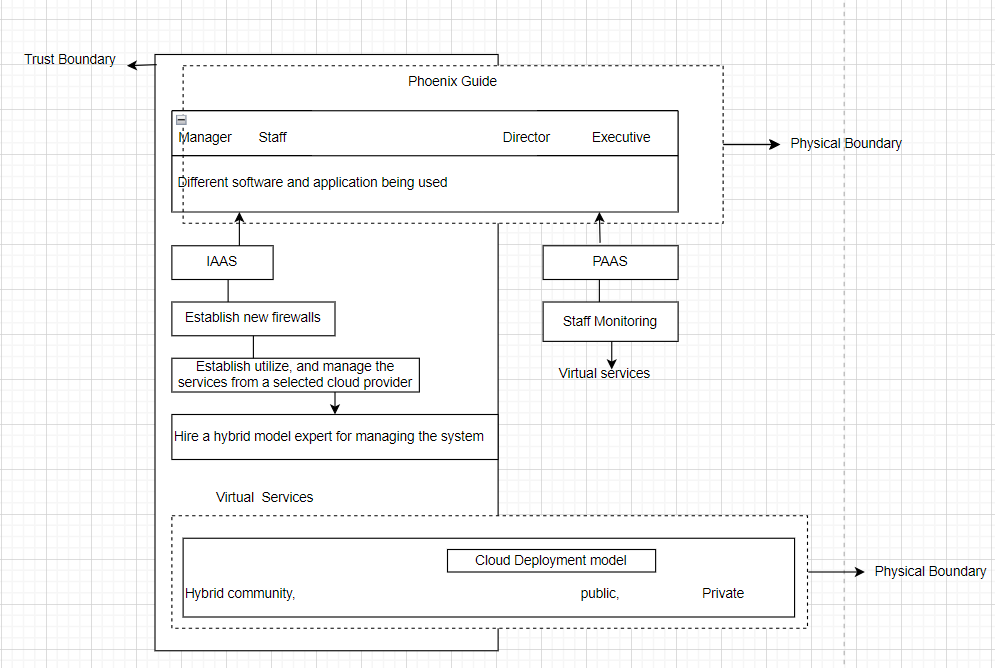


Figure 1: Cloud Implementation Model

The primary reason for implementing this model is as follows:

* **Flexibility and Control:** One of the issues faced by the Company is being too rigid and not having much flexibility in it. So, applying this model will allow more flexibility to design personalized solutions that meet the needs of the company's individual.
* **Cost:** The company does not wish to spend much money implementing the new model. This makes this model the best one as it provides scalability in terms of cost. The company will only have to pay for any extra capacity in case it is required.
* **Security:** The company is still using only the basic level of security and is not even using two-factor authorisation. However, with the application of this model, the chances of attacks like data theft by attackers are considerably reduced.

1. Service Model

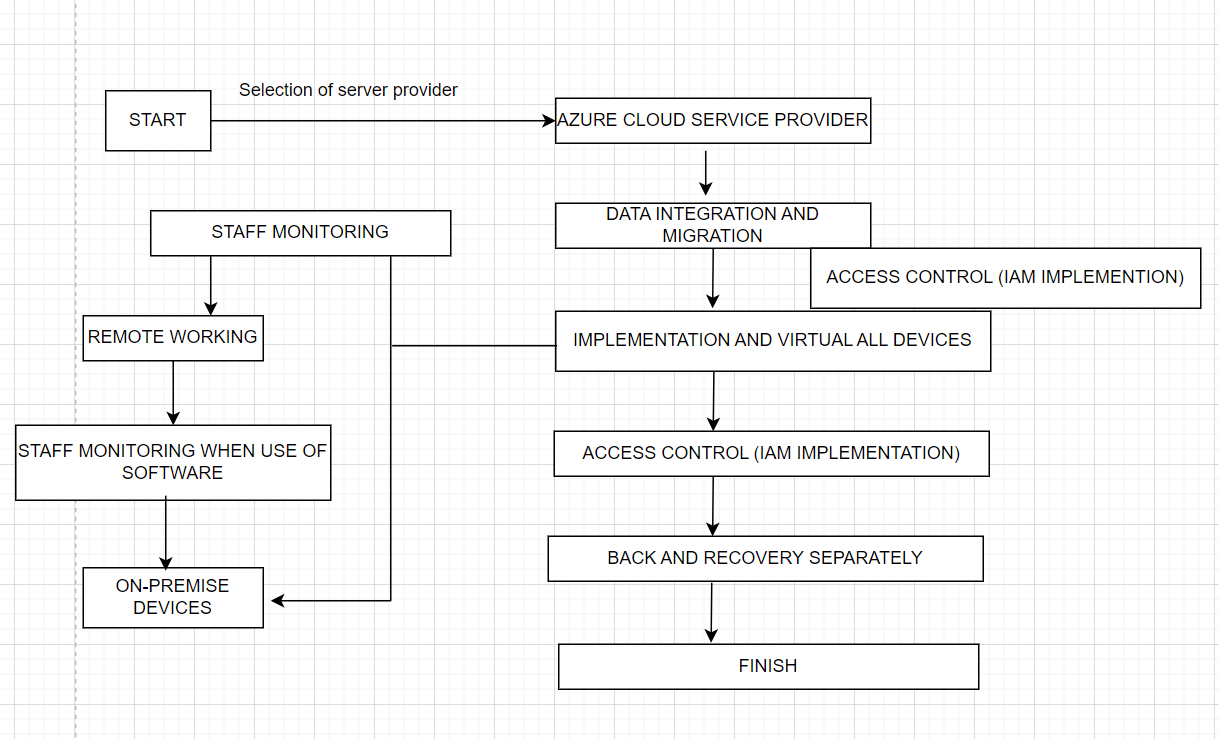


Figure 2: Service Model

**Description of workflow:**

The above workflow chart is all about the detailed cloud implementation and migration process, especially while using the Azure cloud service provider. This is an essential financial institution like Phoenix Capital, which is trying to enhance IT infrastructure and operating capabilities.

Phoenix Capital launches its cloud migration strategy by picking Azure Cloud Service Provider, indicating a critical step towards boosting infrastructure flexibility and operational efficiency. Phoenix Capital selected Microsoft Azure, suggesting a strategic partnership with a supplier recognised for its broad cloud capabilities, which include robust security measures, financial compliance, and a diverse range of services that promote scalability and flexibility.

Staff monitoring is an essential component of the process. Monitoring is vital for compliance and security at financial institutions like Phoenix Capital, which handles sensitive financial transactions and personal client information. Implementing such strategies also aids in monitoring productivity and making better use of corporate resources.    The rise in remote working possibilities represents the modern workplace's growing need for flexibility. It enables employees to access systems and data from remote places, enhancing productivity and employee satisfaction, particularly in the post-pandemic era, when remote work is becoming increasingly common.

Specific software monitoring reveals that Phoenix Capital intends to maintain high security to prevent data breaches and unauthorised access. This stage may include monitoring access logs and user behaviour inside company software to ensure that any abnormal behaviour is quickly identified and rectified.  Staff monitoring during software use suggests that Phoenix Capital intends to maintain high security to prevent data breaches and unauthorised access. Involvement of On-Premises Devices is specific monitoring during software use, which indicates that Phoenix Capital wants to maintain high security to avoid data breaches and unauthorised access.  Data integration and migration is moving existing data to the Azure cloud platform. It requires combining data from many sources and formats, ensuring it is correctly mapped and stored in the new context. Implementing Identity and Access Management (IAM) allows for control over cloud access. IAM is integral to cloud security since it guarantees that only authorised users may access sensitive financial data and services. The method seeks to virtualise all devices by abstracting real hardware. Virtual devices are easier to manage, update, and protect since they can quickly adjust to suit new business requirements or address security problems. Backup and recovery arrangements demonstrate the company's dedication to protecting data and ensuring business continuity. The mitigating process is completed. The last step signals the end of the first migration procedure. However, it is critical to understand that cloud migration is a continuous process of optimisation, security monitoring, and adaptation to new technologies and business requirements.

Throughout this workflow, Phoenix Capital is committed to using cloud technology to increase operational resilience, data security, and workforce flexibility, all while preserving regulatory oversight and control over its digital transformation.

1. Deployment Model

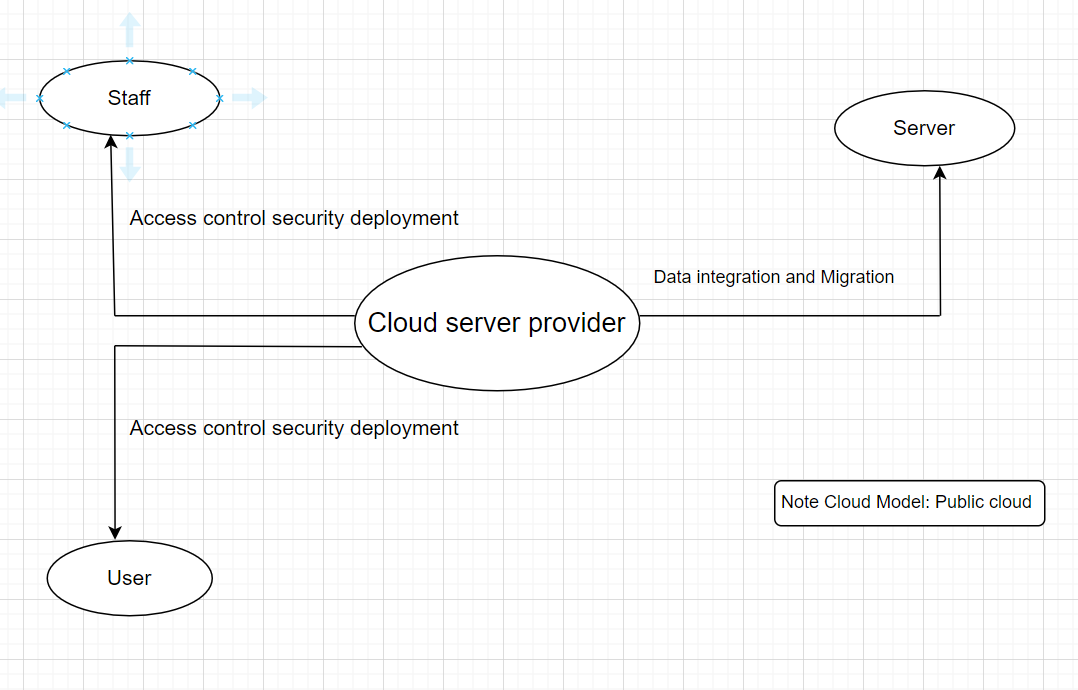


Figure 3: Deployment Model

The deployment model presented in the image is a cloud architecture intended to help data and application management, with a focus on security and user access.

Staff and Server Interaction: The diagram consists of two main entities: 'Staff' and 'Server'. The ‘Staff' refers to the employees of the organisation who require server access for operational purposes. The 'Server' represents the on-premises or original state of the company's data and applications.

Data Integration and Migration: A one-way interaction between the 'Server' and the 'Cloud server provider' represents the movement of data and applications from on-premises servers to the cloud. This is a vital step in which current systems move to the cloud, ensuring that data is transferred securely and without loss.

This oval represents Azure, a cloud service company mentioned before. The model's primary control centre oversees Phoenix Capital's operations, storage, and services. Given the 'Public cloud' annotation, this supplier provides services via the public internet, making them open to anybody who wants to buy or lease them.

Implementing Access Control Security for Staff and Users: Arrows marked 'Access control security deployment' point to the 'Staff' and 'User' entities of the 'Cloud server provider'. This demonstrates that access control measures are in place to monitor and restrict access to cloud resources. These measures are required to secure sensitive financial data and comply with various regulatory requirements.

IAM systems will be used to guarantee that only approved professionals and users may access certain cloud resources. This is frequently performed by authentication approaches such as passwords, two-factor authentication, biometrics, and authorization systems that describe which resources users may access once confirmed.

The 'User' at the bottom of the illustration symbolises the end user of cloud services. This might comprise internal users (employees using company applications) and external users (customers visiting web portals). The implementation of access control security from 'Cloud server provider' to 'User' ensures that users may only access data and apps that are relevant to them, resulting in a more personalised and safe experience.

The cloud model is a hybrid cloud', which means that Azure's cloud services that will be adopted in the business is the hybrid model which is the combination of both public and private cloud services. As the Phoenix capital is operated while providing connection to both public and within the organization.

This deployment approach focuses on a secure migration from on-premises servers to a public cloud environment, emphasising access control to safeguard resources and data. Phoenix Capital's usage of a public cloud architecture implies that it is using the scalability and cost-effectiveness of cloud resources while prioritising security and compliance, both of which are crucial in the financial services business.

1. Service Selection

When it comes to the cloud service provider that are available on the market; there are many of them. For the Phoenix Capital, three major cloud service providers have been taken into consideration; and have been compared among one another to find the best cloud service provider for the company. The three of them are AWS, Azure, and Google. All of them are among the most popular cloud service provider platforms. The table shows the comparison of some of the features.

|  |  |  |
| --- | --- | --- |
| AWS | Azure | Google |
| 29,000 | 27,500 | 31,000 |

Figure 4: Pricing Model

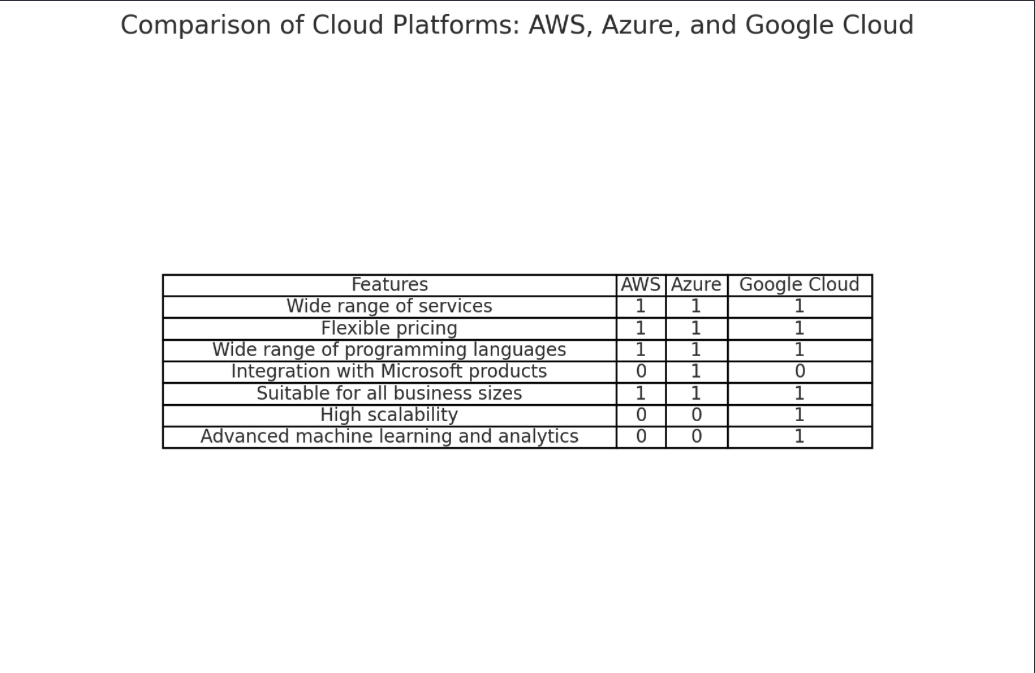
****

Figure 5: Service Provider (Feature Comparison)

The Phoenix Capital is a financial institution which has a limited budget. The scalable pricing that all the service model provides makes all of them appear to be usable as it creates the possibility of conducting the migration to the cloud while spending under the budget. The company also needs the Microsoft related services from the Office 365 to Dynamic 365 and more Microsoft related services as it is a financial organization. Which leads to the Azure Cloud service provider turning out to be the most applicable for it as it fulfills all of it needs. Therefore, the Azure Cloud Service provider has been decided to be used for this business.

1. Cost Involvement

During the migration of the data to the cloud and the deployment of it; there are multiple instances where the budget needs to be spent. There are factors which are going to cost more money than others. The table below explains those factors in detail while also providing an estimated expense price that is expected to be spent during this process.

| **Category** | **Annual Cost (USD)** |
| --- | --- |
| Virtual Machines | 18,000 |
| Storage | 2,400 |
| Database Services | 3,600 |
| Networking | 1,200 |
| Security and Compliance | 2,400 |

Figure 6: Cost Involvemnt

The estimated cost is of 28,000 dollars. This is an estimated cost so the overall expense when the action is carried out might differ. The organization is still lacking in the terms of the machines and infrastructures so the estimated cost for that is 18,000. And the storage price is for around 10 TB Of data storage from the Azure cloud service provider. For the networking, the cost is estimated due to the cost of establishing the bandwidth for data transfer. And lastly, now the security of the Phoenix Capital is highly vulnerable, so advance threat protection needs to be established when data migration in-between the cloud service provider and the organization; and among the staffs is conducted. And the cost for the staff monitoring also comes int o the security and compliance category.

1. Cost Management Considerations in Cloud Migration

a. Comparison and Selection of Service Providers

Single Service Provider Strategy: By combining billing and support, choosing a single cloud service provider can simplify operations and possibly save costs.

Comparative Analysis: Determining which provider (such as AWS, Azure, and Google Cloud) best suits Phoenix Capital's needs by evaluating them according to their costs, services provided, and adherence to industry standards.

b. Classifying Data for Security Purposes

Rank-Order Security Approach: Applying varying degrees of protection according to the data's sensitivity. To optimize costs, less sensitive client data may have fewer security measures and be stored in less secure environments, whereas highly sensitive client data may be encrypted.

Policies for Data Management: defining precise data management guidelines to guarantee that information is handled and stored in a way that balances cost and security.

c. Infrastructure-Related Issues

Infrastructure-Related Issues: Establishing a server room for intranet use in accordance with business needs is known as intranet server room setup. This entails weighing the expense of using cloud capabilities for internal data flow against maintaining an on-premises server room.

Hybrid Infrastructure: Determining whether a hybrid cloud strategy that combines cloud services and on-premises infrastructure could be a financially viable way to address some internal processes while still utilising the advantages of the cloud for other operations.

1. Security

For the security, two factor authentication will be utilized irrespective of whether the user is the public or a member of the Phoenix Capital. Two factor authentication for logging into the system.

The data will be divided into various categories which will be allowed access based on the authority. Moreover, confidential data will require the access from multiple devices to ensure the confidentiality and integrity of the data. For this access controls is going to be incorporated int he company data and the data on the cloud. Any activity carried out by the staff after logging into the system on the system is monitored in detail after asking for access from the staff.

And all the important data will be backed up separately too as being overdependent on the cloud can lead to a disaster. So, the back-up of important is done for recovery and to check the integrity of the data for future reference.

1. Integration of Cost Management Strategies

Balanced Service Selection: Selecting just one cloud provider can simplify things and possibly save costs, but it's important to make sure the provider can handle all the requirements of the company, including compliance, scalability, and reliability.

Security Cost Improvement: In the financial industry, security is crucial, but costs must be taken into consideration as well. This entails making necessary security measure investments without going overboard on extra features.

Control of information and storage: By categorising data according to its value and sensitivity, more effective and economical security and storage solutions can be developed. With a focus on high-priority areas, this approach guarantees that resources are allocated appropriately.

1. Challenges and Mitigations

1. Technical Challenges

Complexities of Data Migration: It can be difficult to ensure secure and efficient data transfer to the cloud.

Mitigation: To reduce disruptions, use robust data migration tools and services, as well as a phased migration.

2. Security concerns.

Data Security and Compliance: Protecting sensitive data and meeting regulatory requirements in the cloud.

Mitigation: Implement strong security measures such as encryption and access controls and select cloud providers that meet financial industry standards.

3.Human Resource Challenges

Skill Gaps: Existing employees may lack the skills required for effective cloud management and utilisation.

Mitigation: Implement comprehensive training programmes and consider hiring or consulting with cloud experts.

4. Cultural and Organisational Change

Adjusting to new workflows: Resistance to new processes and workflows can pose a significant challenge.

Mitigation: Implement effective change management strategies such as clear communication, stakeholder engagement, and support structures.

5. Financial Management

Cost Control and Budgeting: Managing and optimising cloud spending can be difficult, particularly with variable pricing models.

Some of the ways to mitigate the challenge and the problems are as follows:

Mitigation: Conduct regular reviews of cloud usage and spending and use cost-management tools provided by cloud providers.

**Focus on Data and Personnel Classification for Access Control.**

Data classification involves categorising data based on its sensitivity and value. Highly sensitive or confidential data (such as client financial records) necessitates stricter access controls and security safeguards than less sensitive data.

Role-Based Access Control (RBAC): Use RBAC to ensure that employees only have access to data and resources that are required for their roles. This reduces the likelihood of data breaches and ensures adherence to data privacy regulations.

Access controls and data classifications should be audited and reviewed on a regular basis to ensure they remain relevant and effective as the company and its data evolve.

Training and Awareness: Ensure that employees are properly trained and understand the importance of data security and access control principles.

1. Conclusion

In this paper, one of the issues of lack of security and the need for change in the Phoenix Capital has been discussed. Virtualization of the company via the cloud migration is the most optimum solution to solve all the worries of the company. For these three service providers have been compared and azure service provider has been decided to be used. As the features of this service provider is the most inclined with this company needs. The paper also mentions challenges and ways to solve the challenges in the paper along with various other materials. In short, from this report it can be concluded that by migrating the data to the Azure cloud and incorporating the Azure cloud service provider into the business; the business can grow more and perform better while also increasing the security of the data.

# References

1. A. S. Muhammed and D. Ucuz, "Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users’ Perspectives," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116254.  
   keywords: {Cloud computing;Web services;Digital forensics;Companies;Internet of Things;Security;the Internet of Things;IoT platform;Microsoft Azure;Amazon AWS;Google Cloud}, [Accessed 27/01/2024]
2. ieeexplore.ieee.org. (n.d.). *Cloud computing challenges and implementations | IEEE Conference Publication | IEEE Xplore*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7755159> [Accessed 28 Jan. 2024].

‌

# Appendix

# Group Activity Report

This is the three major meetings that happened for the completion of this project. This has been named as Meeting Minutes 1, 2, and 3.

|  |  |
| --- | --- |
| **Section** | **Details to be Included** |
|  |  |
| Documentation | Meeting Minutes: 1st  Date and Time of Interaction: 7 December 2023 at 3:00 PM  Topic of Discussion: Cloud Implementation Model  Team Members Present:  At college, all present |
| Level of Interaction in Meetings | All of the members were extremely attentive and gave their time for the report.  Everyone completed their tasks in allocated time, did the formatting; discuss about what to do next and left. |
| Task Distribution | Bibhuti – Necessity and challenges, formatting  Saraswati – Executive summary and the reasons for implementing the model.  Amit – Cloud implementation model; Current limitations |

|  |  |
| --- | --- |
| **Section** | **Details to be Included** |
|  |  |
| Documentation | Meeting Minutes: 2nd  Date and Time of Interaction: 3 January, 2024at 3:00 PM  Topic of Discussion: Service, Deployment, Security.  Team Members Present:  Physical at college, all present |
| Level of Interaction in Meetings | All of the members were extremely attentive and gave their time for the report.  All the members left together after completing submitting and compiling the task in the same report.  Everyone completed their tasks in allocated time. |
| Task Distribution | Bibhuti – Service Model  Saraswati – Deployment Model  Amit – Service Selection |

|  |  |
| --- | --- |
| **Section** | **Details to be Included** |
|  |  |
| Documentation | Meeting Minutes: 3rd  Date and Time of Interaction: 24 January, 2024 at 3:00 PM.  Topic of Discussion: Cloud Implementation Model  Team Members Present  Physical at college, all present |
| Level of Interaction in Meetings | All of the members were extremely attentive and gave their time for the report.  All of the members were extremely attentive and gave their time for the report.  All the members left together after completing submitting and compiling the task in the same report.  Everyone completed their tasks in allocated time. |
| Task Distribution | Bibhuti – Integration of Cost Management Strategies, Challenges  Saraswati – Deployment Model, Description of Workflow  Amit – Security, Conclusion, Cost Management in Migration |

# 