Universiteit Leiden

ICT in Business and the Public Sector

Multi-Cloud Governance Framework for Financial Institutions

Student Name: Mohamed Atef Thabet Abdelrahim
Student-no: s2557037

Date: 30/03/2023

1st supervisor: Drs. J.B. Kruiswijk

2nd supervisor: Dr. C.J. Stettina

Multi-Cloud Governance Framework for Financial Institutions

A holistic strategic framework that will support the financial institutions in adopting and governing the migration to multi-cloud

This master thesis is submitted to Leiden University in partial fulfillment of the requirements of

Master of Science in ICT in Business

Faculty of Science

Student Name: Mohamed Atef Thabet Abdelrahim

Student Number: s2557037

Date: 30 - March - 2023

First Supervisor: Drs. J.B. Kruiswijk

Second Supervisor: Dr. C.J. Stettina

Preface & Acknowledgment

Dear Reader,

The desire for this research project came from my goal of becoming an expert in the cloud consultancy field. In 2013, I finished my Bachelor of Science in Computer Science. Then, I worked as a Software Developer and Solutions Supervisor. During my work, I decided that I wanted to study business and work in an international environment. As a result, I chose this master program at Leiden University because it is like an MBA with thesis research. After that, I took a Cloud Internship at Accenture Netherlands to conduct my thesis research.

I would like to express my deepest gratitude to my university supervisors Prof. Bas Kruiswijk and Prof. Christoph Johann Stettina, for their time, support, and insights. Their wisdom and their wealth of knowledge and experience inspired me throughout my study.

I am extremely grateful to my Accenture supervisors, Quentin Pannebakker, Madhumita Naik, and Liss Meijer, for all the guidance and support that they provided me throughout my internship.

Finally, I would like to thank Leiden University and Accenture Netherlands for providing me with all the resources that I need to conduct my thesis research.

Mohamed Thabet

Leiden, March 2023

Abstract

Most financial institutions are adopting multi-cloud to keep their on-premises mainframes and benefit from the best-of-breed of different public cloud providers. However, the financial institutions that adopted multi-cloud encountered challenges they did not encounter when they adopted a single cloud, such as managing security and risks across different cloud providers, migrating cloud workloads between different cloud providers, and managing the operations of their multi-cloud environment. Despite more than fifteen years of ongoing research on the impact of cloud computing on business, financial institutions still struggle with adopting cloud computing.

Therefore, thesis research aims to investigate the challenges that financial institutions encounter before, during, and after the migration to multi-cloud and investigate the solutions that they took to solve these challenges in order to develop a holistic strategic governance framework that will support the financial institution in adopting and governing the migration to multi-cloud.

The aim of this thesis research was achieved by taking a cloud internship at one of the largest cloud consultancy organizations in the world. Firstly, the challenges and the solutions that the financial institutions encountered were identified by conducting literature reviews of academic research and industry research and conducting interviews with 17 cloud experts from the host company because it was not allowed to interview clients due to the internship contract limitations. After conducting the literature review of the available cloud governance frameworks and analyzing the interviews, the first version of the multi-cloud governance framework was developed. After that, seventeen interviews with cloud experts from the host company were conducted to evaluate the first version of the framework. Finally, the final version of the framework was developed based on their feedback.

From the literature review and the experts' interviews, it was found that the challenges that the financial institution encounter are shortage of cloud engineering skills, shortage of mainframe engineering skills, shortage of DevSecOps skills, shortage of multi-cloud skills, complexity of the re-organization and complexity of managing the security across a multi-cloud environment, and being in a vendor-lock to their first cloud provider due to lack of cloud migration and cloud exit strategies. From all these findings, the multi-cloud governance framework was developed.

Keywords:
Multi-cloud, Hybrid-cloud, Governance Framework, Cloud Migration, Financial Institutions

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

API	Application Programming Interface
CCOC	Cloud Center of Competency
CCOE	Cloud Center of Excellence or Enablement
CCO	Chief Cloud Officer
IaC	Infrastructure-as-Code
IaaS	Infrastructure-as-a-Service
IT	Information Technology
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SLA	Service Level Agreement

Chapter 1 Research Introduction

Introduction of Chapter 1

This thesis research investigated the challenges financial institutions encounter before, during, and after migration to multi-cloud to develop a holistic governance framework that will support them in adopting and governing the migration to multi-cloud. This chapter provides an introduction to this research. Section 1.1 presents the research background and the research problem. Section 1.2 presents the research aim. Section 1.3 presents the main research question and the sub-research questions. Finally, the chapter ends with a conclusion.

1.1 Research Background and Research Problem

Defining and formulating the research problem is the most important step in any research. Kothari (2004) said, "*A researcher must find the problem and formulate it so that it becomes susceptible to research. To define a problem correctly, a researcher must know: what a problem is?*".

Since the study field and the professional expertise of the researcher are the business field and the IT field, the researcher started the literature review by searching for business and cloud computing research domains. Despite more than fifteen years of ongoing research on the impact of cloud computing on business, financial institutions still struggle with adopting cloud computing (Hon & Millard, 2016) (Hon & Millard, 2018a) (Sfondrini et al., 2018) (Kaya et al., 2020) (Parne, 2021) (Accenture, 2022).

One of the main goals of financial institutions is to utilize information technology (IT) services in order to improve, re-engineer, and automate their services and create new business models and revenue streams (Shu & Strassmann, 2005) (Abubakar & Tasmin, 2012) (Lin et al.,

2012) (Mocetti et al., 2017). During the previous century, financial institutions used to design, build, implement, manage, and maintain their own on-premises data centers in order to have complete control of all their IT infrastructure and data (Gartner, 2021).

However, during the 2000s, cloud computing emerged. Cloud computing represents a disruptive change in which IT services are designed, developed, deployed, delivered, scaled, maintained, and paid for (Marston et al., 2011). Organizations from small-medium-businesses, and enterprises, to governments across all industries and countries are adopting cloud computing due to its various benefits, such as immediate access to hardware and software services, capacity auto-scaling according to the current needs, and no-upfront capital investments (Dash & Pani, 2016) (Modisane & Jokonya, 2021). Adamuthe & Thampi (2019) conducted a trend projection and technology maturity curve of six computational technologies, including two disruptive technologies, namely mainframes and cloud computing. They concluded that all computational technologies except cloud computing had undergone upward and downward trends. The slope of the curve of cloud computing is almost vertical.

Additionally, since February 2020, the sudden COVID-19 pandemic forced the world into a global lockdown within two months. As a result, organizations had to switch fully or partially to remote online working by accelerating the digital transformation at short notice. The COVID-19 pandemic forced organizations to focus their priorities on decreasing costs and utilizing IT to support and secure a remote online workforce. Cloud computing played an essential role in ensuring the business continuity of different industries during the lockdown by addressing these priorities (Alhomdy et al., 2021) (Amankwah-Amoah et al., 2021). According to Gartner Inc (2021), the COVID-19 pandemic increased worldwide end-user spending on public cloud services from $257.5 billion in 2020 to 18.4% to $304.9 billion in 2021.

As a result, financial institutions are adopting cloud computing due to many benefits such as immediate access to IT resources and services, creating new financial services and new revenue streams, improving business agility, creating new business continuity plans and disaster

recovery plans, and reducing the carbon footprint (Nedelcu et al., 2015) (Yan, 2017) (Hon & Millard, 2018a) (Megargel et al., 2020) (Trovato et al., 2019) (Vinoth et al., 2022).

On the other hand, cloud adoption has significant challenges from the financial institutions' perspective, which are governance, security, and privacy (Nedelcu et al., 2015) (Yan, 2017) (Hon & Millard, 2018a) (Vinoth et al., 2022). Regarding governance and security, cloud computing depends on the shared responsibility model, which means the responsibility of governance and security are split between the financial institution and the cloud service provider. Regarding privacy, the data are stored in the data centers of the cloud service providers. As a result, governments are issuing new laws and regulations to protect their citizens' privacy and data, such as the European Union GDPR (Hon & Millard, 2018b). Therefore, financial institutions must consider the laws and regulations before taking any strategic cloud decision. For example, in some countries, some laws and regulations dictate data storage location. As a result, the financial institution will not be able to migrate their data to cloud service providers who do not have data centers in the locations stated by the regulators (Ghule et al., 2018).

One of the approaches that can allow financial institutions to benefit from on-premises data centers and cloud computing is adopting multi-cloud. Multi-cloud is a deployment model composed of one or more on-premises data centers or private clouds and one or more public clouds from different cloud providers. In the multi-cloud, financial institutions usually keep the critical IT services running on the on-premises data center and migrate the less-critical IT services to the public clouds (Hon & Millard, 2018a) (Accenture, 2022) (Cheng et al., 2022) (IDC, 2022).

Reference to the research background, it was evident that cloud computing is a main technological driver for organizations across different industries, and it was a survival environment for the organizations during the lockdown of the COVID-19 pandemic. Therefore, the initial literature review of cloud computing started by studying the existing research about:

- Challenges of Cloud Adoption.
- Impact of Cloud Adoption on Strategic Alignment between Business and IT.
- Impact of Cloud Adoption on Financial Institutions.

The challenges and issues of single public cloud deployment have been investigated by academia and industry. The challenges and issues were vendor-lock, service availability, and changing legal requirements and regulations regarding the location of data (Petcu, 2011) (Petcu et al., 2013) (Westerlund & Kratzke, 2018) (Truyen et al., 2020) (Ahn & Ahn, 2020) (Christiansen et al., 2022). As a result, the adoption of multi-cloud computing over the past few years is increasing due to its benefits, such as avoiding vendor-lock-in, choosing the best of breed of cloud services from different cloud providers, and strengthening business continuity and disaster recovery. However, organizations that adopt multi-cloud computing encounter new challenges that they do not encounter while adopting single-cloud computing, such as managing security across different cloud vendors, employing different development tools and APIs for each one, and automating and orchestrating the solutions across them (Petcu, 2011) (Paraiso et al., 2014) (Rosian et al., 2022).

Few research papers analyzed the impact of cloud adoption on the strategic alignment between the business and the IT of the cloud consumer. The papers found that IaaS and PaaS have different impacts on the strategic alignment between the business and the IT of the cloud consumer than the impact of SaaS. In Addition, the flexibility of SaaS allowed the business departments to bypass the IT department and request cloud applications directly from the cloud provider. This behavior led to the self-explained phenomenon The Shadow IT (Marston et al., 2011) (Avram, 2014) (Schneider & Sunyaev, 2016) (El-Gazzar et al., 2016) (Fuzes, 2018).

Research from academia and industry investigated the impact of cloud adoption on financial institutions. They found that the main drivers for adopting cloud computing are cost reduction, technical limitation of mainframes, and shortage of employees who can manage and

maintain the mainframes and their core applications (Nedelcu et al., 2015) (Yan, 2017). On the other hand, financial institutions have concerns and challenges regarding cloud computing, such as the loss of complete control of IT infrastructure and data, the continuously changing laws and regulations, and the traditional conservative organizational culture of financial institutions (Hon & Millard, 2018a). Hon & Millard (2018a) investigated how banks within the European Union approached cloud computing. They found that they approached cloud computing in three main approaches, which are: shadow cloud, mushroom cloud, and formal cloud strategy.

The three approaches are summarized in the following table:

Banks Cloud Approach	Description
Shadow Cloud	It starts with individuals or individual teams. Individual teams request cloud services directly from the cloud provider with or without consulting the IT or the procurement department.
Mushroom Cloud	It starts from multiple different shadow clouds. Individual teams request cloud services directly from the cloud provider with or without consulting the IT or the procurement department for small-scale use cases.
Formal Cloud Strategy	It starts with the IT department or top management. They establish a cloud governance strategy. They identify their use cases, needs, and expectations from cloud computing. After that, they start testing cloud computing using trials or proof of concept for the less critical services. Finally, they start editing the strategic alignment between business and IT to maximize the benefits of cloud adoption.

Table (1): How Banks approach Cloud Computing

1.2 Research Aim

In order to successfully adopt and govern a multi-cloud environment, strategic planning and alignment between business and IT are needed. In order to do so, a clear understanding of different strategic aspects of multi-cloud adoption and governance is extremely important. Therefore, this research aims to investigate multi-cloud environments within the financial industry to develop a strategic framework that will support them in adopting and governing the migration to multi-cloud based on a holistic approach. The holistic approach will consider the technological factors, the organizational factors, and the environmental factors of financial institutions and multi-cloud environments.

1.3 Research Questions

Reference to the aim of the research, the following research questions were defined.

The Main Research Question

How can a financial institution govern the challenges of migrating to a multi-cloud environment?

To answer the main research question, the following sub-research questions were defined.

Sub-Research Question 1 (SRQ1)

What is cloud computing?

This sub-research question aims to build the base foundation of the research by investigating the following points in order to understand cloud computing in-depth:

- Cloud Computing.
- Cloud Actors and their responsibilities.
- Cloud Computing Characteristics.
- Cloud Computing Service Models.
- Cloud Computing Deployment Models.
- Multi-Cloud Delivery Models.
- Cloud-enabling Technologies.
- Cloud Services Lifecycle.
- Cloud Applications Maturity Level.
- Cloud Migration Strategies.

This sub-research question was answered by conducting a literature review.

Sub-Research Question 2 (SRQ2)

What are the cloud adoption drivers and cloud adoption challenges of financial institutions?

This sub-research question aims to identify and categorize financial institutions' challenges when they migrate to a multi-cloud environment.

After answering this question, a list of challenges was identified that supported interviewing the experts by asking them about challenges they did not mention. This sub-research question was answered by conducting a literature review.

Sub-Research Question 3 (SRQ3)

What are the available cloud governance and management frameworks?

This sub-research question aims to identify the current cloud governance and management frameworks used by organizations to identify the components of the governance framework.

After answering this question, the research understood the difference between cloud governance and cloud management and their components. This sub-research question was answered by conducting a literature review.

Sub-Research Question 4 (SRQ4)

What are the challenges that a financial institution encounters before, during, and after the migration to a multi-cloud environment?

This research question aims to identify a financial institution's challenges before, during, and after migrating to a multi-cloud by conducting semi-structured interviews with experts. This sub-research question was answered by semi-structured interviews.

Sub-Research Question 5 (SRQ5)

What are the governance strategies that a financial institution can use for governing the challenges of migrating to a multi-cloud environment?

This research question aims to identify the governance strategies that financial institutions use to govern the challenges identified in the SR5. This sub-research question was answered during the same semi-structured interviews.

Sub-Research Question 6 (SRQ6)

What are the requirements of a holistic strategic framework for governing the challenges of migrating to a multi-cloud environment for financial institutions?

This research question aims to develop a strategic framework that will support adopting and governing the migration to a multi-cloud environment based on a holistic view. The holistic approach will consider the technological factors, the organizational factors, and the environmental factors of financial institutions and multi-cloud environments. This final sub-research question was answered by analyzing the answers to the previous sub-research questions. Finally, conducting evaluation interviews with experts to evaluate the framework and develop the final version of it.

Conclusion of Chapter 1

Chapter 1 introduced the thesis by presenting the research background, research problem, and research questions. From the initial literature review, it was concluded that cloud computing allowed organizations to innovate, create new business models, create a remote workforce, and strengthen their business continuity and disaster recovery. However, single cloud computing comes with challenges, such as vendor lock-in. As a result, organizations adopt multi-cloud computing to avoid vendor lock-in and choose the best of breed of cloud services. On the other hand, multi-cloud computing comes with new challenges, such as managing security across different cloud vendors. In addition, the data is stored in the data centers of the different cloud service providers in different geographic regions. As a result, governments are issuing new laws and regulations to protect their citizens' privacy and data. As a result, financial institutions struggle with adopting multi-cloud due to many challenges, such as the security complexity of the multi-cloud environment. Therefore, this thesis research aims to investigate multi-cloud environments within the financial industry to develop a strategic framework that will support adopting and governing the migration to multi-cloud based on a holistic approach. The holistic approach will consider the technical factors, the organizational factors, and the environmental factors of financial institutions and multi-cloud environments.

Chapter 2 Research Methodology

Introduction of Chapter 2

This chapter presents the research methodology. Section 2.1 presents the chosen research method and the data analysis method. Section 2.2 presents the approach of the literature review. Section 2.3 presents the approach of the interviews. Section 2.4 presents the research plan. Section 2.5 presents the research outline of this document. Finally, the chapter ends with a conclusion.

2.1 Research Methodology

Reference to the research questions mentioned in section 1.3, this research will need to capture the perspective and insights of the business and IT employees regarding their work status and challenges. A qualitative research approach is suitable for this study because it aims to understand the participant's view of a phenomenon in a specific context. In addition, qualitative research seeks to answer what and how rather than how much or how many questions. Hence, the choice of qualitative research is most appropriate for this study. The chosen qualitative technique is semi-structured interviews because it will allow the interview to flow into a natural conversation and allow the interviewee to add more information and new insights.

There are several data analysis methods that are used in analyzing qualitative data, such as thematic analysis, grounded theory, and phenomenology (Thorne, 2000). Thematic Analysis is used in analyzing qualitative data, where the primary purpose of the research is to identify some trend or highlight particular behavior among the sample population (Braun & Clarke, 2006). Thematic Analysis is suitable for this research because it will allow capturing, understanding, and analyzing the answers of each interviewee and then analyzing all the answers to find insights

and patterns. Thematic analysis is mainly done on data gathered through interviews and questionnaires. Bruan and Clark (2006) identified six phases for thematic analysis: familiarization with the data, initial code generation, searching for themes, reviewing themes, defining and naming themes, and producing the report.

One of the methods for conducting thematic analysis of the data from semi-structured interviews is the Framework Method. The Framework Method was developed in the 1980s by Jane Ritchie and Liz Spencer for analyzing qualitative data of social science research (Ritchie et al., 2013). It provides a systematic model for managing and categorizing data. Its output is a matrix of rows and columns. The rows can be cases, organizations, or interviews. The columns can be codes, themes, or dimensions.

The Framework method uses the Constant Comparative Method used in Grounded Theory, where researchers sort the raw data into groups or codes according to their attributes to define the themes and then create a new theory. However, the Framework Method does not need to create a new theory. Data coding aims to categorize the data to compare them systematically and then identify or discover the themes. The Framework Method can be used in the deductive approach and inductive approach. The difference between them is how the themes are identified. In deductive research, the themes are pre-identified based on previous literature or research questions. While in inductive research, the themes are identified based on coding the data without following a restricted set of codes. In much research, the combined approach is suitable when the research has pre-identified dimensions or themes to explore and aims to discover undiscovered themes. As a result, it became popular in multi-disciplinary qualitative research to get a holistic descriptive overview of the entire data (Gale et al., 2013). Therefore, the Framework Method will be used in this research to conduct the interviews' thematic analysis. The following table summarizes the stages of the Framework Method (Gale et al., 2013):

Stage no.	Stage Name	Stage Tasks
1	**Transcribing Interviews**	Listen carefully to interviews. Transcript interviews.
2	**Familiarization with Interviews**	Re-listen to the interviews. Re-read the transcripts.
3	**Coding Transcripts**	Carefully read the transcriptions line by line. Identify and apply a code (label) that describes what the interviewee emphasized that is very important.
4	**Developing Analytical Framework**	Compare codes. Identify the needed codes. Group codes into categories in a tree-like diagram or hierarchy. Develop analytical framework from the previous diagram.
5	**Applying Analytical Framework**	Indexing transcripts under codes.
6	**Charting Data into Framework Matrix**	Summarize the data by category for each transcript. Map reduced data to a matrix.
7	**Interpreting Data**	Analyze reduced data in the matrix in order to find relations between them.

Table (2): Stages of Framework Approach

2.2 Literature Review Approach

The aim of the literature review is to answer the SRQ1 and the SRQ2. The published academic research and industrial research are analyzed as primary literature, while the industrial whitepapers and reports are analyzed as secondary literature. The review protocol is as the following:

- **Search Strategy:**

  The used search engines are Google, Google Scholar, ScienceDirect, SpringLink ,EmeraldInsight and ResearchGate.

- **Search Terms:**

  The used search terms are “multi cloud governance”, “multi cloud challenges”, “multi cloud migration”, “multi cloud bank”, “multi cloud financial institution”, “cloud adoption framework”, and “cloud governance framework”. In order to refine the results, the operators “OR” or “+” are used.

2.3 Interview Approach

The researcher got a cloud internship at Accenture Netherlands in order to get access to multi-cloud projects, Accenture employees, Accenture clients and Accenture knowledge base documents. However, due to the limitation of the internship contract, it was not allowed to interview Accenture clients. Therefore, Accenture experts were interviewed. All the interviewees work at Accenture Netherlands, Accenture UK, Accenture Ireland, and Accenture USA. Their positions are from Associate Managers until Leaderships. All of them worked on multi-cloud projects within the financial industry and other industries. Their roles are cloud consultants, cloud engineers, cybersecurity, and enterprise architects. The interview starts by explaining to the interviewee the purpose of the interview. Then, the interviewee was asked about his or her role within Accenture. Then, the interviewee was about his or her experience with multi-cloud projects within the financial sectors. After that, the interviewee was asked to choose a multi-

cloud project of a financial institution that he or she believes is suitable for the research. 17 interviewees were interviewed. The interview durations were between 30 minutes and 45 minutes. All the interviews were conducted online. The interview questions can be found in Appendix A.

2.4 Research Plan

This research will be conducted at Accenture Netherlands. The internship started from 01-September-2022 and ended on 01-March-2023. During September, October, and November, the literature review was conducted in order to find knowledge gap, develop research questions and write the research proposal. The research plan was as the following:

December 2022:

1. Conduct literature review to define:

- Cloud Computing.
- Cloud Actors and their responsibilities.
- Cloud Computing Characteristics.
- Cloud Computing Service Models.
- Cloud Computing Deployment Models.
- Multi-Cloud Delivery Models.
- Cloud-enabling Technologies.
- Cloud Services Lifecycle.
- Cloud Applications Maturity Level.
- Cloud Migration Strategies.
- Cloud Governance.
- Cloud Management.

2. Conduct literature review to identify:

- Drivers for multi-cloud adoption of financial institutions.
- Challenges of multi-cloud adoption of financial institutions.

3. Develop holistic conceptual framework for interviews

- Conduct literature review in order to find the strategic frameworks and technology adoption frameworks that are commonly used in IS research and cloud-related research.
- Identity the frameworks that cover the dimensions of cloud adoptions.
- Integrate the frameworks in order to develop a holistic framework that determine the dimensions and the scope of required data from the interviews.

4. Develop interview questions based on the holistic conceptual framework.

January 2023

1. Conduct expert interviews to answer SRQ4 and SRQ5.

February and March 2023

1. **Analyze the interview data.**
2. **Develop a holistic governance framework.**
3. **Conduct evaluation interviews to evaluate the findings and the framework.**
4. **Write the thesis document.**
5. **Defend the thesis.**

2.5 Research Paper Outline

This research paper is structured as the following:

Chapter 1: Introduced the research problem and the research questions.

Chapter 2: Presented the research methodology and the research plan.

Chapter 3: Presented the literature review for cloud computing and cloud migration strategies.

Chapter 4: Presented the history of technology with the financial institutions.

Chapter 5: Presented the IT governance, the strategic flexibility, and the digital transformation.

Chapter 6: Presented the available cloud governance frameworks from research and industry.

Chapter 7: Presented the research model that was used for developing the interview questions.

Chapter 8: Presented the results of the expert interviews.

Chapter 9: Presented the first version of multi-cloud framework.

Chapter 10: Presented the results of the validation interviews and the final version of multi-cloud governance framework.

Chapter 11: Presented the discussion and conclusion of the research results.

References: Presented the list of references using APA 7th Edition.

Appendix A: Presented the questions of the expert interviews.

Appendix B: Presented the questions of the validation interviews.

Appendix C: Presented the final version of Multi-Cloud Governance Framework.

Appendix D: Presented the most important citations from the expert interviews.

Conclusion of Chapter 2

Chapter 2 introduced the research methodology by explaining the reasons for the chosen research method. The chosen research method is qualitative analysis in order to understand the participant's view of a phenomenon in a specific context. The chosen qualitative technique is semi-structured interviews because it will allow the interview to flow into natural conversation and it will allow the interviewee to add more information and new insights. Due to the internship contract limitation, interviewing Accenture clients. As a result, only Accenture employees were interviewed.

Chapter 3 Cloud Computing

Introduction of Chapter 3

This chapter presents the results of the literature review. The literature review aims to find and analyze the literature on cloud computing, starting from cloud computing history until cloud migration strategies, to build a strong foundation for the thesis. This chapter is structured as the following. Section 3.1 until section 3.8 presents the history of cloud computing, the definition of cloud computing, the characteristics of cloud computing, the cloud actors and their responsibilities, the cloud service models, the cloud deployment models, the multi-cloud delivery models, and the cloud-enabling technologies. Sections 3.9 until section 3.11 present cloud services lifecycle, cloud applications maturity level, and cloud migration strategies to understand cloud migration.

3.1 Cloud Computing History

The concept of provisioning computing services as a public utility was proposed in 1961 by John McCarthy "*computing may someday be organized as a public utility just as the telephone system is a public utility… The computer utility could become the basis of a new and important industry*" (Ivanov, 2008). The evolution of computing delivery models is classified into six phases (Voas & Zhang, 2009) (Furht, 2010). The following table summarizes the phases.

Phase Name	Phase Description
Mainframe Computing **1960s**	Users use terminals for using shared powerful computers on premises. The terminal is just a monitor and keyboard. The mainframe is shared by many users.

Stand-alone Computing **1980s**	Users use computers that have their own processing and storage capabilities.
Network Computing **1980s**	Users form local network to connect their computers and servers. Users access extra computing by communicating with servers.
Internet Computing **1990s**	Users connect their local networks to form global network. Users access extra computing by communicating with servers in remote locations.
Grid Computing **2000s**	Users connect servers in different locations to run services.
Cloud Computing **2007s**	Users get instant access to scalable computing services through the internet.

Table (3): History of Cloud Computing

3.2 Cloud Computing Definition

In order to build a strong foundation for this thesis, a standard definition of cloud computing is needed. In 2011, the National Institute of Standards and Technology of USA (NIST) was designated to accelerate the US government's adoption of cloud computing by developing standards and guidelines about cloud computing after consulting and collaborating with standard bodies and the private sector. The NIST definition of cloud computing (Hogan et al., 2011) (Mell & Grance, 2011):

"*A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

3.3 Cloud Computing Characteristics

Reference to the definition of the NIST, the NIST identified five main characteristics of cloud computing as the following (Hogan et al., 2011) (Mell & Grance, 2011):

- **On-demand Self-service**

The cloud consumer can request and access computing services instantly without interaction from the cloud provider.

- **Broad Network Access**

Cloud services are available over the internet and can be accessed through standard mechanisms through command line interface, web browsers, or mobile apps.

- **Resource Pooling**

The cloud services of the cloud provider are pooled to serve multiple different cloud consumers using a multi-tenant model.

- **Rapid Elasticity**

Cloud services can be scaled up and down automatically to cope with the current demand.

- **Measured Services**

The usage of cloud services is measured by units of time or by the number of requests, so the cloud consumer pays per usage.

3.4 Cloud Actors

The NIST identified five major actors who perform different tasks in a cloud environment. The five major actors are (Hogan et al., 2011) (Mell & Grance, 2011):

1. Cloud Consumer

An entity that requests cloud services from a cloud provider directly or via a cloud broker.

2. Cloud Provider

An entity is responsible for creating and maintaining cloud services for cloud consumers. The activities of cloud providers fall into five categories:

a. Service Deployment

It includes all the activities of creating, managing, and maintaining cloud deployment models. The deployment models are private cloud, public cloud, community cloud, and hybrid or multi-cloud. The cloud deployment models are explained in section 3.6.

b. Service Orchestration

It includes all the activities of designing, arranging, coordinating, and managing cloud infrastructure in order to create different cloud services. These activities can be classified into three layers as the following:

i. Service Layer:

It is the top layer in which the cloud consumer uses cloud services. It has cloud service models, which are Infrastructure-as-as-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The cloud service models are explained in section 3.5.

ii. Resource Abstraction and Control Layer

It is the middle layer that has all the software components that the cloud provider needs to access and manage the hardware in the Physical Resource Layer. It includes software components such as virtual machine hypervisors and virtual data storage.

iii. Physical Resource Layer

It is the lowest layer that has the hardware resources. It includes hardware resources such as servers, networks, and storage systems.

c. Cloud Service Management

It includes all the activities that are necessary for the management and operation of cloud services. The activities can be required or proposed by the cloud consumer or cloud broker. The activities can be classified under three categories as the following:

i. Business Support

It includes all the activities related to managing a business with cloud consumers, such as Customer Management, Contract Management, Pricing, Billing, and Auditing.

ii. Provisioning and Configuration

It includes all the activities that are related to running and maintaining cloud services, such as Service Provisioning, Metering, and Reporting.

iii. Portability and Interoperability

It includes all the activities that are related to supporting cloud consumers in migrating to the cloud and integrating their services with the cloud services, such as Data Portability, Service Portability, and System Interoperability.

d. Security

The cloud providers are responsible for the physical security of the data center. However, regarding the security of the cloud services, the security is defined based on the shared responsibility model in which the responsibility is shared between the cloud provider and the cloud consumer depending on the cloud service model, the cloud deployment model, and the SLAs.

e. Privacy

The cloud providers are responsible for adhering to the laws and regulations of the countries where their data centers are located. The governments and cloud auditors conduct assessments for cloud providers to verify their compliance with laws and regulations.

3. **Cloud Broker**

An intermediary entity is responsible for managing the delivery of cloud services and the negotiation between cloud providers and cloud consumers. As cloud computing evolves, the integration of cloud services becomes very complex for a cloud consumer to manage alone. The services of cloud brokers fall into three categories.

a. Service Intermediation

The cloud broker provides value-added services to cloud consumers by enhancing a given service from a cloud provider.

b. Service Aggregation

The cloud broker integrates multiple services from cloud providers to create one or more new services.

c. Service Arbitrage

It is similar to service aggregation, except the cloud broker can replace individual services from different cloud providers.

4. Cloud Auditor

An independent entity that conducts independent assessments of cloud services in order to evaluate the security, privacy, and performance of cloud services. They evaluate the cloud services to verify their compliance with laws and regulations.

5. Cloud Carrier

An intermediary entity that provides connectivity between cloud providers and cloud consumers. Some cloud consumers and cloud providers require cloud carriers to make dedicated direct connections between their locations for performance or security reasons.

3.5 Cloud Service Models

In the industry, cloud computing is usually classified according to a service model and deployment model. The service model defines the type of services that the cloud consumer can request and the amount of control over them. The most common classification of service models is Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Hogan et al., 2011) (Mell & Grance, 2011).

- **Infrastructure as a Service (IaaS)**

It is the most flexible service model, because it allows the cloud consumer to determine the specification of the requested services. However, it requires the most effort from the cloud consumer because they are responsible for installing, managing, and updating the operating systems and the applications that run these services (Hogan et al., 2011) (Mell & Grance, 2011).

- **Platform as a Service (PaaS)**

It is something in between IaaS and SaaS because it offers a managed deployment platform that allows the cloud consumer to deploy their applications immediately while the cloud provider will provision and manage the required hardware, virtual machines, and operating systems (Hogan et al., 2011) (Mell & Grance, 2011).

- **Software as a Service (SaaS)**

It provides the cloud consumer with ready-made apps from cloud providers. The cloud customer is responsible for migrating their data and managing the identity and access management, while the cloud provider is responsible for managing and updating the cloud apps (Hogan et al., 2011) (Mell & Grance, 2011).

It is worth noting that some cloud providers use other classifications for marketing purposes, such as Database-as-a-Service or Desktop-as-a-Service. However, such specific service models can be classified as a PaaS or SaaS depending on the level of control that the cloud consumer has over them.

3.6 Cloud Deployment Models

The cloud deployment model is defined based on the owners, the operators, and the locations of the cloud data centers in a cloud environment. The most common classification of deployment models is Private Cloud, Public Cloud, Community Cloud, and Hybrid Cloud or Multi-Cloud (Hogan et al., 2011) (Mell & Grance, 2011).

- **Private Cloud**

The cloud infrastructure is provided exclusively for a specific cloud consumer and may be owned or managed by the cloud consumer or a cloud provider. It may be located on-premises or off-premises (Hogan et al., 2011) (Mell & Grance, 2011).

- **Public Cloud**

The cloud infrastructure is owned and managed by a cloud provider and is available for public usage (Hogan et al., 2011) (Mell & Grance, 2011).

- **Community Cloud**

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., security requirements). It may be managed by the organizations or a third party and may exist on-premises or off-premises (Hogan et al., 2011) (Mell & Grance, 2011).

- **Hybrid Cloud or Multi-Cloud**

The cloud infrastructure is a composition of two or more (on-premises data center, private, public, community) clouds that are still unique independent entities, but the provisioned services are connected by standardized technologies or proprietary technologies that enable the integration of data and applications. There are other less common names for Hybrid Cloud or

Multi-Cloud deployment models such as Inter-Cloud, Aggregated Cloud, Federated Clouds, Cloud of Clouds or Hybrid-Multi-Cloud. For simplicity, this thesis will use the term Multi-Cloud for the rest of the paper (Petcu, 2013).

3.7 Multi-Cloud Delivery Models

Research analyzed the taxonomy of multi-cloud and identified two delivery models within the multi-cloud, which are the Volunteer Federated Multi-Cloud Model and the Independent Multi-Cloud model (Petcu, 2013) (Grozev & Buyya, 2014) (Samreen et al., 2014). The difference between the two models is the degree of collaboration between the involved cloud providers.

In the Volunteer Federated Multi-Cloud Model, there is a prior agreement between the cloud providers to share the resources, while in the Independent Multi-Cloud model, there is no agreement. In the Independent Multi-Cloud model, the cloud customer builds a multi-cloud environment based on multiple independent cloud providers.

As a result, the integration and the portability are the responsibility of the cloud consumer. From an architectural perspective, Grozev and Buyya (2014) classified the Federated Multi-Cloud Model into Centralized Model and Peer-to-Peer Model, while the Independent Multi-Cloud Model into the Service-based Model and Library-based Model. The table and the diagrams explain and summarize them.

3.8 Cloud-enabling Technologies

Cloud computing is neither a stand-alone technology nor a new IT service delivery model. It is the result of utilizing other technologies together with IT outsourcing which are (Böhm et al., 2011):

1. Virtualization

It is the key technology of cloud computing because it allows (Scarfone et al., 2011):

- **Service Portability** by running any services on any underlying hardware.
- **Elasticity** by scaling up or down the hardware resources during the run-time of the services.
- **Multi-tenancy** by isolating the service instances running on the same hardware from each other.
- **Cost Effective** by utilizing any hardware resource to its peak performance capacity.

2. Cluster Computing

It is the utilization of a group of the same hardware resources connected by a local network in the exact location to run the same service. The nodes in the clusters act as virtual computer. Once a node fails in the cluster, another standby node will take over. Therefore, cluster computing is used for high availability and load balancing (Sadashiv & Kumar, 2011) (Kumar & Charu, 2015).

3. Grid Computing

It is the utilization of a group of different hardware resources that are in different locations to run the same service. The nodes of the grid communicate using standard protocols. Therefore, grid computing aggregates geographically distributed hardware resources (Sadashiv & Kumar, 2011) (Kumar & Charu, 2015).

4. Service Oriented Architecture (SOA)

Cloud computing is an example of an IT provisioning model. However, it represents a shift from the traditional-based IT provisioning model to the service-based IT provisioning model and outsourcing. Therefore, a comparison between cloud computing and SOA and between cloud computing and outsourcing is needed. SOA is an architectural paradigm allowing enterprises to use their software effectively and efficiently. In SOA, each business function is executed by a stand-alone software component. The software components communicate through protocols in order to execute a service. The SOA allows the enterprise to update its services by updating or replacing individual software components instead of updating or replacing the entire service or software. However, SOA focuses on software, and cloud computing applies similar principles to software and hardware (Feuerlicht, 2010) (Böhm et al., 2011).

5. IT Outsourcing:

It is the delegating of some or all of an organization's IT services to a third party based on a Service Level Agreement (SLA) in order to reduce cost and focus on core business (Dhar & Balakrishnan, 2006) (Böhm et al., 2011). Cloud computing is considered the next level of IT outsourcing because it allows instant provisioning of IT services and pay-per-usage payment model (Böhm et al., 2011).

3.9 Cloud Services Lifecycle

Cloud computing changed the way IT services are designed, implemented, delivered, consumed, and retired. As a result, the lifecycle of cloud services is different from the lifecycle of on-premises IT services. Joshi et al. (2014) defined 5 phases of the lifecycle of cloud services.

These phases are as the following:

1. Cloud Service Requirements Phase:

The cloud consumer identifies the functional requirements and the non-functional requirements that a service must fulfill. The functional requirements entail the functions that services must fulfill. While non-functional requirements entail the properties of the services, such as performance, platform, certifications, and standards that it must fulfill.

2. Cloud Service Discovery Phase:

The cloud consumer identifies the cloud providers that fulfill the requirements of the requirements phase. According to the NIST reference architecture document in section 3.2, the cloud consumer can identify the provider themselves or consult a cloud broker. Then, the cloud consumer can consult the cloud auditor to check the compliance of cloud providers' services with the required laws and regulations.

3. Cloud Service Negotiation Phase:

The cloud consumer discusses and negotiates the SLAs with cloud providers.

4. Cloud Service Composition Phase:

The cloud consumer and the cloud service provider or providers design the composition and the orchestrating of the cloud services if needed.

5. Cloud Service Consumption Phase:

The cloud services are delivered to the cloud consumer based on the Negotiation Phase. Then, the cloud consumer starts consuming the cloud services, and the payment is made based on the

agreed-upon pricing model in the SLAs. In the public cloud deployment model, the cloud services reside in the datacenters of the cloud provider. Hence, the cloud services administrating, managing, and monitoring are in the hands of public cloud providers. Therefore, the cloud consumer needs tools that monitor the cloud services and compare them with the SLAs.

3.10 Cloud Applications Maturity Levels

Before an organization migrates an application to the cloud, it needs to determine the maturity level of the application in relation to the cloud. In academia and industry, cloud applications maturity levels are categorized into four levels of maturity as the following (Spillner et al., 2018):

Level 0: Legacy Applications (Non-Cloud-enabled application)

The applications were originally designed for running on-premises data centers, and they are tightly coupled to the hardware that it is impossible or extremely expensive to migrate to a cloud environment.

Level 1: Cloud-enabled Applications

The applications were also originally designed for running on-premises data centers, but they can be adapted to run in a cloud environment. The developers usually need to create a virtual environment on the cloud similar to the on-premises data center. However, these applications cannot interact with cloud native services.

Level 2: Cloud-aware Applications

They are the next level of cloud-enabled applications. These applications can integrate with cloud-native services.

Level 3: Cloud-native Applications

These applications are designed for cloud environments. They can either be cloud-vendor dependent or cloud-neutral dependent (cloud agnostic). These applications are usually designed based on a microservice architecture or serverless architecture as the following:

- The microservice architecture is a development approach that is based on service-oriented architecture in which the application is divided into independent modules (microservices) that interact with messages (Dragoni et al., 2017) (Kratzke, 2018).

- The serverless architecture is a development approach that is based on event-based architecture. Each service is a function executed when an event occurs (Kratzke, 2018).

3.11 Cloud Migration Strategies

In the past, enterprises built on-premises data centers to run their applications. Their monolithic applications were developed by old programming languages and installed on outdated hardware. Hence, they are called legacy applications. Holland and Light (1999) defined legacy applications "*Legacy systems encapsulate the existing business processes, organization structure, culture, and information technology*".

The characteristics of legacy applications are inflexible to change and expensive to maintain. In previous years, enterprises started migrating to cloud computing due to its benefits such as auto-scaling and pay-per-usage model. Cloud migration is defined as the process of re-engineering legacy applications to become cloud-enabled (Chauhan & Babar, 2012). Pahl et al. (2013) created a more detailed definition of cloud migration: "*Cloud migration is the process of partially or completely deploying an organization's digital assets, services, IT resources or applications to the cloud. The cloud migration process may involve retaining some IT infrastructure on-site. In such a scenario, the existing system may be fused with a partial cloud solution that can be hosted by a third party over the Internet for a fee. The cloud component of*

this hybridized system can transition between several cloud providers allowing businesses to choose the most cost-effective solution". Cloud migration can be classified into five types (Andrikopoulos et al., 2012) (Gholami et al., 2016) as the following:

Migration Type	**Migration Definition**
Type I	Deploy the business logic tier of legacy applications to cloud IaaS or PaaS. Keep the data tier on the on-premises datacenter.
Type II	Replace some components or the entire business logic tier of legacy applications with SaaS. Keep the data tier on the on-premises datacenter.
Type III	Keep the business logic tier of legacy applications on the on-premises datacenter. Deploy the data tier to cloud IaaS.
Type IV	Keep the business logic tier of legacy applications on the on-premises datacenter. Replace legacy database with cloud native database.
Type V	Replace the entire business logic tier of legacy applications with cloud native services. Replace legacy database with cloud native database.

Table (5): Cloud Migration Strategies

Another classification of cloud migration strategies that is common in industry is summarized in the following table (Accenture Cloud Migration Strategies, 2021) (Pohl et al., 2022).

Cloud Migration Strategies	Description
Rehost	Applications are migrated to cloud 'as-is'. Also called Lift and Shift.
Replatform	Applications are migrated to cloud after applying changes that may include operating systems, containers, and middleware.
Replace	Applications are replaced with SaaS alternatives.
Rearchitect	Applications are re-architected in order to be cloud-native.
Reimagine	Business services are refined by considering all the current capabilities of cloud offering.
Retain	Applications will not be migrated to cloud due to technical limitation or financial reasons or legal restrictions.
Retire	Applications will be retired because they no longer add value.

Table (6): Another Cloud Migration Strategies

Conclusion of Chapter 3

This chapter answered the SRQ1. It investigated cloud computing from the history of cloud computing until cloud migration strategies. It was found that cloud computing is not a standalone computing technology, but it resulted from integrating and leveraging other

technologies such as virtualization, cluster computing, and grid computing. In addition, IT outsourcing is also part of cloud computing because the cloud consumer uses the IT infrastructure of cloud providers. The level of responsibility between the cloud consumer and the cloud provider depends on the deployment model and the service model of the cloud.

There are many strategies to migrate applications to the cloud, such as rehost, replatform, and rearchitect. Each migration strategy has its value and effort. Adding to that, not all the strategies apply to all applications. Sometimes applications are tightly coupled to the hardware, so rehosting or replatforming it to a cloud environment is impossible or extremely expensive.

Chapter 4 Cloud Transformation within Financial Industry

Introduction of Chapter 4

Since this thesis research focuses on adopting multi-cloud by financial institutions, understanding the digital transformation within the financial industry is needed. Section 5.1 presents a short history of technology in the financial industry. Section 5.2 presents digital transformation within the financial industry to understand its influencing factors. Section 5.3 and section 5.4 presents the cloud adoption drivers and cloud adoption barriers from the perspective of financial institutions. Finally, this chapter ends with a conclusion.

4.1 Financial Industry and Technology

The financial industry is a very old industry that started with the first bank that was established in 1397. In the past, financial institutions relied on physical media to store data, such as papers. Since transferring physical media relied on physical transportations, the business of the financial institutions at that time was limited to small geographic areas around their branches. However, this was changed with IT. IT allowed financial institutions to separate data from the physical media and to transfer them anywhere in the world. As a result, financial institutions became largely dependent on IT. Since the 1960s, financial institutions have established large IT departments responsible for purchasing, developing, operating, and maintaining the mainframes and the core applications. Since the 2000s, the continuous evolution of IT created new disruptive technologies that allowed for the emergence of new disruptive competitors, such as FinTech, that offer digital services to their customers.

On the other hand, as people and organizations become more dependent on IT for their daily lives and daily businesses, this dependency on IT is changing their behavior toward online

and mobile services. As a result, financial institutions continuously compete to create new digital services (Omarini, 2017) (Alt et al., 2018). Consequently, governments are issuing new laws and regulations to protect their citizens' privacy, such as the European Union GDPR (Hon & Millard, 2018b). Therefore, financial institutions must consider the laws and regulations before making strategic IT decisions. For example, in some countries, some laws and regulations dictate data storage location. As a result, the financial institutions in those countries will not be able to migrate their data to cloud service providers who do not have data centers in the locations stated by the regulators (Ghule et al., 2018).

4.2 Digital Transformation within Financial Industry

From the previous section, it was concluded that financial institutions are not born-digital organizations such as tech organizations and telecom organizations. This means that they were not initially structured as IT organizations. Therefore, an understanding of digital transformation for pre-digital organizations is needed.

Digital transformation has become a critical key concern for pre-digital organizations because digital transformation impacts the inner aspects of an organization, such as the products, services, processes, and structure, and the organization's outer aspects, such as customer behavior, partners and suppliers. Therefore, in order to build a successful digital transformation strategy, the organizations must consider the business strategy and the technology strategy at the same time because digital transformation is a business-centric and technology-inspired strategy (Bharadwaj et al., 2013) (Diener & Špaček, 2021). Researchers identified and analyzed the factors that influence the digital transformation of a financial institution (Werth et al., 2020). They created a model by combining Porter’s Five Forces with PEST Analysis, as shown in figure (2).

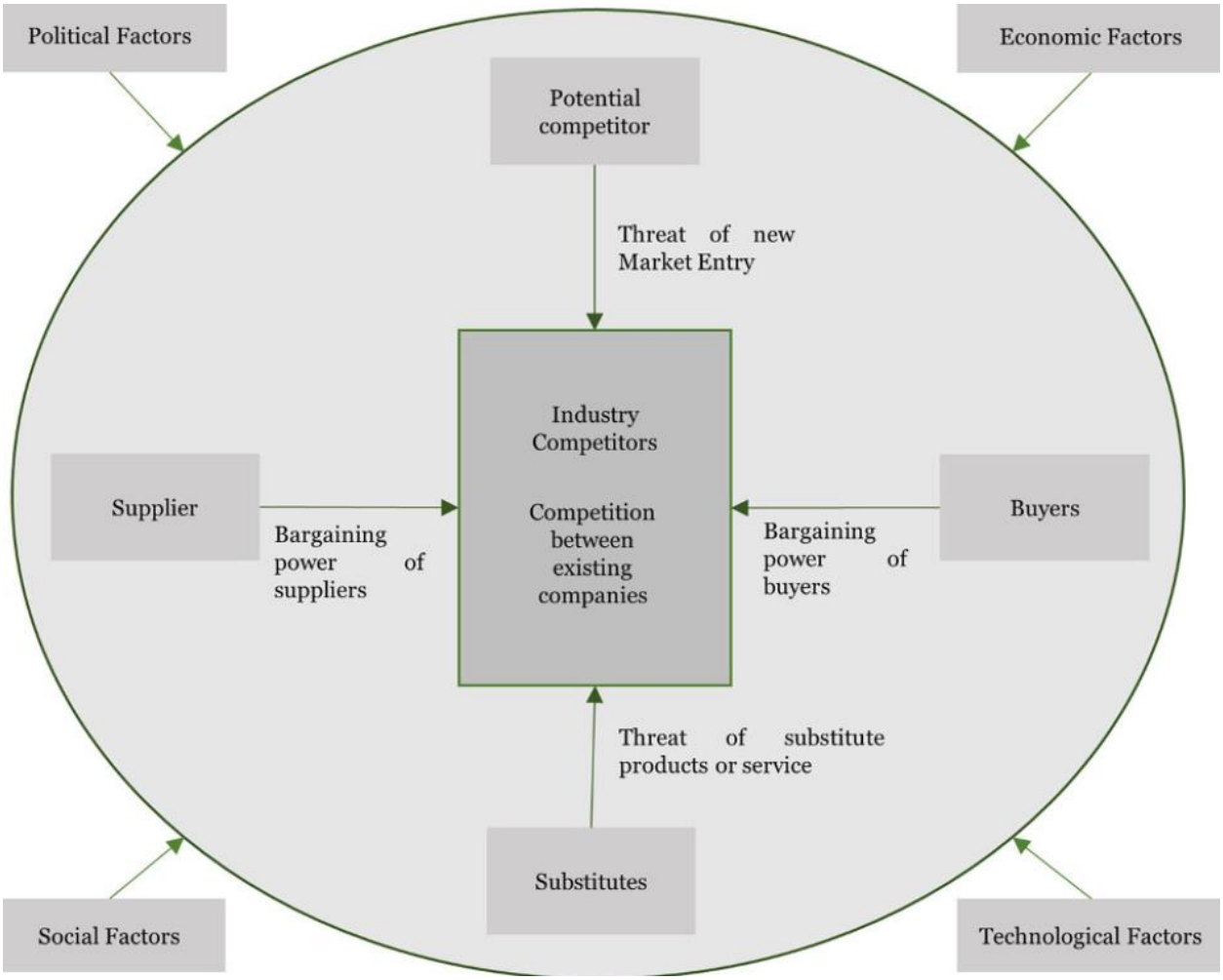


Figure (1): Digital Transformation factors within the Financial Industry.

4.3 Financial Institutions Cloud Adoption Drivers

Historically, financial institutions used to build and manage their mainframes in order to have complete control over the applications and data. The hardware of these mainframes was developed in the 1970s or earlier, and the core applications were developed by old programming languages, and they are tightly coupled with the hardware. Since the early 2000s, cloud computing has allowed new players, such as neo-banks and FinTech institutions, to compete with traditional financial institutions and gain market share by developing innovative solutions. Consequently, traditional financial institutions adopted cloud computing to develop new business models and innovative applications, control costs, adopt the agile methodology and DevOps, and reduce time-to-market (Hon & Millard, 2018a). The following subsection summarizes their cloud adoption drivers.

a. Creating Data-driven Services

The amount of data that financial institutions generate is growing annually at an extraordinary rate. Organizations across all industries utilize data analytics and AI to gain more value from their data. As a result, they are considering their data as an enterprise asset and adopting data governance structures to protect their data. However, the limited capacity of legacy data centers does not allow financial institutions to leverage the value of their data. Therefore, financial Institutions are adopting cloud computing due to its unlimited auto-scaling data storage. Adding to that, the cloud service providers are competing by improving their AI capabilities (Hon & Millard, 2018a) (Accenture, 2021) (The Economist, 2021a) (The Economist, 2021b) (Abbott, 2022) (Lanza, 2022).

b. Adopting Agility and Decreasing Time to Market

The instant provisioning of cloud services allowed financial institutions to adopt agile methodologies and hence, become able to provide new services quickly and respond to any market disruptions (Hon & Millard, 2018a) (Accenture, 2021) (The Economist, 2021a) (The Economist, 2021b) (Abbott, 2022) (Lanza, 2022).

c. Improving Sustainability and Green IT

Financial institutions now have environmental, social, and governance targets. They can achieve these targets quickly by migrating to public cloud providers and minimizing the usage or closing their legacy data centers (Hon & Millard, 2018a) (Accenture, 2021) (The Economist, 2021a) (The Economist, 2021b) (Abbott, 2022) (Lanza, 2022).

d. Strengthening Business Continuity and Disaster Recovery

When financial institutions keep all their applications and data on their on-premises data center, they become entirely responsible for them. In order to have business continuity plans and disaster recovery plans, they will have to buy and maintain backup data centers. Hence, higher

costs. Fortunately, most public cloud providers have multiple data centers in different geographic regions with direct private connections. They offer many business continuity and disaster recovery plans allowing redundant applications and data in different regions. Therefore, financial institutions can keep running with up-to-date data in case a disaster impacts the primary cloud data center (Hon & Millard, 2018a) (Accenture, 2021) (The Economist, 2021a) (The Economist, 2021b) (Abbott, 2022) (Lanza, 2022).

4.4 Financial Institutions Cloud Adoption Barriers

Financial institutions are security-driven organizations because they deal with very sensitive data, such as financial data and personal data. Therefore, their top priorities are always security and stability, more than innovation. As a result, they prefer to use their own on-premises data centers and old mainframes to keep the infrastructure and the data under control. The following subsection summarizes their cloud adoption barriers.

a. Security, Compliance, and Privacy Risks

Historically, the culture of financial institutions is very conservative in that they want to own, build, manage, and maintain their IT infrastructure because the financial industry is heavily regulated. Therefore, they used to run all the applications and save the data on their on-premises data centers. Additionally, a lack of understanding of cloud computing from business leaders of financial institutions and regulators contributes to these security and trust concerns (ENISA, 2014) (Hon & Millard, 2018a) (Abbott, 2021) (Abbott, 2022) (Lanza, 2022).

The European Union Agency for Network and Information Security ENISA (2014) conducted surveys and interviews with financial institutions and regulators within the European Union. They found they have the following concerns regarding the public cloud: Level of Availability, Data Breach, Data Loss, Data Secure Deletion, and Lack of Auditing Features. The ENISA found that in countries with effective communication and collaboration between the financial

institutions, regulators, and cloud service providers, the cloud market is more mature and evolving. As a result, they prefer to migrate critical IT services to the private cloud and less critical IT services to the public cloud. Therefore, the preferred cloud deployment model by them is a multi-cloud environment.

b. Limitation of Mainframe and Core Applications

Most core banking applications were developed by legacy programming languages and are tightly coupled to the legacy mainframes. Migrating legacy applications to the cloud might require rearchitecting or reimagining the entire applications, which may be too expensive and time-consuming. Additionally, the legacy applications are ready tested, and they have been running from many years (Hon & Millard, 2018a) (Abbott, 2021) (Abbott, 2022) (Lanza, 2022).

c. Shortage of Skills

The lack of understanding of cloud computing is one of the main barriers to cloud adoption. Financial institutions need employees who understand their core applications, cloud engineering, and their core business to build innovative cloud solutions instead of rehosting the same applications on the cloud. Additionally, to migrate legacy applications to the cloud, financial institutions will need employees who understand the architecture of legacy applications and cloud computing to migrate them to the cloud. Unfortunately, the shortage of skills prevents organizations from migrating to the cloud or fully realizing the full benefits of their cloud environment (Hon & Millard, 2018a) (Abbott, 2021) (Abbott, 2022) (Lanza, 2022).

Conclusion of Chapter 4

From this chapter, it was concluded that financial institutions always need to identify and analyze all the factors that influence their digital transformation in order to improve their digital transformation strategy and hence their cloud transformation by considering the following

factors: Political or Regulation Factors, Economical Factors, Technological Factors, Changing Behavior of Consumers, Suppliers, and Partners, and the emergence of competitors and substitutes.

The chapter also presented the cloud adoption drivers and cloud adoption barriers from the perspective of financial institutions. The most important drivers are agility, shorter time to market, and strengthening business continuity and disaster recovery. On the other hand, financial institutions are security-driven organizations, so security, privacy, and compliance are their topmost challenges. Adding to that the shortage of skills. They need employees who understand their core business, mainframe, core application, and cloud engineering to maximize the benefits of their cloud migration.

Chapter 5 Cloud Governance

Introduction of Chapter 5

This chapter presents cloud governance. Section 4.1 presents IT governance, IT governance decision-making models, and IT governance flexibility in order to understand IT governance in depth and its impact on strategic flexibility and digital transformation. Section 4.2 presents strategic flexibility and its components to understand how organizations can build a flexible strategy to cope and adapt to continuously evolving technologies. Section 4.3 presents digital transformation because it includes cloud transformation. So, an understanding of digital transformation is needed to understand cloud transformation. Finally, the chapter ends with a conclusion.

5.1 IT Governance

Since organizations start to depend on IT in order to conduct business, they start implementing IT governance in order to obtain the needed involvement from business leaders and to achieve a strategic alignment between business and IT because it is the key to leveraging the business value from IT (Peterson, 2004). Gartner (2020) found that the executives listed IT governance as the top risk for 2021 due to the COVID-19 pandemic. There are many different definitions of IT governance. However, all of them have one common purpose: achieving strategic alignment between business and IT. This research will use the definition of Van Grembergen (2004) because he included IT management in the definition because the failure of an organization to leverage the strategic benefits of its IT investment is due to poor IT management because IT management and IT governance are interrelated on multiple levels (Sohal & Fitzpatrick, 2002). IT governance is defined as: "*IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that*

ensure that the organization's IT sustains and extends the organization's strategy and objectives. IT governance is the organizational capacity exercised by the Board, executive management, and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT." Van Grembergen (2004). Since, IT governance and IT management are related, a clear comparison between them is needed. The following table summarizes the differences between them (Peterson, 2004):

IT Governance	IT Management
Focuses on the set of IT decisions about who can make which IT decisions.	Focuses on how to maximize the efficiency and effectiveness of daily IT operations.
Support the strategic demands of the current business needs and the future business needs.	Support the daily demands of the current business needs.
Flexible to cope with any disruption or innovations.	Strict to force operations to stay in order.
Internally oriented and externally oriented.	Internally oriented.

Table (7): IT Governance VS IT Management

5.1.1 IT Governance Decision-Making Models

Since financial institutions are hierarchical and conservative organizations, understanding IT governance decision-making models is essential to understand each model's impact on IT governance. IT governance can be classified according to the position of decision-makers and the level of decision-making into Centralized Model, Decentralized Model, and Federal Model. In the centralized model, the executives make all the decisions. The centralized model leads to standardized controls, consistency, and economies of scale. In contrast, the decentralized model may work well in organizations in which the IT decision-makers are allocated to different business divisions that are located in globally different locations. The decentralized model enables a sense of business ownership and more flexibility to respond to local business needs.

However, excessive standardization under the centralized model may lead to inflexibility in responding to disruption and innovation. In contrast, excessive flexibility under the decentralized model may lead to different standards that may lead to inflexibility. Regarding the federal model, the executives are responsible for IT infrastructure development decisions, while the divisional executives are responsible for business application decisions (Peterson, 2004). From this subsection, it was concluded that the centralized model and the federal model are more suitable for financial institutions than the decentralized model in order to enforce standardization across their IT infrastructure and decision-making.

5.1.2 IT Governance Flexibility

Nowadays, IT governance needs to meet the demands of standardization, efficiency, and cost control. On the other hand, it needs to meet the demands of flexibility and speed to market. One of the reasons organizations fail to realize the maximum value of technology, including cloud adoption, is that their existing strategies do not consider the dynamics of the modern business environment, which are innovation, disruption, and uncertainty (Bughin et al., 2018). Additionally, the COVID-19 pandemic forced the world into global lockdown within two months. As a result, organizations had to switch fully or partially to remote online working by accelerating the digital transformation at short notice because digital transformation opened new communications channels that allowed organizations to find, reach and interact with customers. Digital transformation is not only about adopting technology, but it is also about changing the strategizing because it differs from traditional forms of strategic change because technologies accelerated the speed and the rate of change, which led to more innovation, disruption, uncertainty, and complexity. Therefore, digital transformation changes business models, business processes, and organizational structure. So, digital transformation focuses on three strategic areas: enhancing digital maturity, redesigning organizational structure, and promoting collaboration and innovation (Warner & Wäger, 2019). From this section, it was concluded that the flexibility of IT governance of an organization could allow it to maximize the benefits of its cloud adoption because the organization can take into account the dynamics of modern business environments, such as innovation, and quickly respond and adapt in order to create more value.

As a result, financial institutions, especially the traditional ones, need to have IT governance flexibility in order to be able to take advantage of disruptive technologies and compete with disruptive competitors.

5.2 Strategic Flexibility

The COVID-19 pandemic forced organizations to focus their priorities on decreasing costs and utilizing IT to support and secure a remote online workforce. As a result, organizations need to consider four strategic areas: rethink the organization, re-engineer business processes, control costs, and accelerate the adoption of digital solutions (Sneader & Sternfels, 2020). The degree to which an organization can achieve these strategic goals is a measure of the organization's strategic flexibility. Strategic flexibility is the ability of an organization to identify significant changes in the external environment and to utilize resources to respond to changes in a short time with due regard to the competitive forces in the environment (Peterson, 2004) (Shimizu & Hitt, 2004) (Sony et al., 2022). The components of strategic flexibility are summarized as the following (MacKinnon et al., 2008):

- **Organizational Flexibility:**

Organizations that adopted a more flat organizational structure and culture of commitment to flexibility, agility, knowledge sharing, cross-functional training, outsourcing, and non-traditional work arrangements.

- **Information Flexibility:**

The flexibility of an organization's information systems to provide the required information quickly. The information flexibility is classified into:

  - **Reporting Flexibility:**

  It is the ability of an organization to obtain data from its transactional information systems.

  - **Analytical Flexibility:**

  It is the ability of an organization to extract insights from its historical information systems.

- **Operational Flexibility:**

It is the flexibility of an organization to adjust its business processes.

- **Supply Chain Flexibility:**

It is the ability of an organization to quickly exchange data with its customers and supply chain partners.

Strategic flexibility is essential in any industry that depends heavily on technology due to rapid innovation, disruption, and changing customer needs. Strategic flexibility depends on IT infrastructure flexibility which is the ability to quickly provision scalable IT infrastructure, applications, and skills within a short time. Many organizations seek competitive advantage through technology, but their legacy IT infrastructure may limit flexibility (Byrd & Turner, 2000). The components of IT infrastructure flexibility are (MacKinnon et al., 2008):

- **Enterprise Systems:**

The organization establishes enterprise-wide information systems that will allow standardization across the organization and avoid organizational silos.

- **Enterprise Integration:**

The organization establishes integration between enterprise systems to establish inter-organizational information systems.

Therefore, in order for IT governance to be strategically flexible, it must be able to meet the following needs (Peterson et al., 2000) (Peterson, 2004):

● **Service Infrastructure:**

Provisioning cost-effective, scalable IT infrastructures with maximum reliability and availability quickly.

● **Solution Integration:**

Developing and delivering integrated IT solutions that allow the organization to respond to any disruption, innovation, or customer demands in a short time.

● **Strategic Innovation:**

Realizing the value of IT investments in terms of operational efficiency, customer excellence, and sustainable financial growth.

5.3 Digital Transformation

Since cloud computing is an example of digital transformation, understanding digital transformation is essential in order to understand the triggers and requirements of digital transformation. Organizations are considering digital transformation to create new business models, services, and products, re-engineer and automate business processes, improve customer experience, and control costs. Digital transformation is using new digital technologies to achieve these goals, such as cloud computing, blockchain, the Internet of Things, and artificial intelligence. Therefore, digital transformation must be investigated to understand cloud transformation (Fitzgerald et al., 2014). However, Rogers (2016) argued that digital transformation is not only about technology but also about strategy because it is about the organizational transformation that integrates and aligns technology with business. Warner and Wäger (2019) analyzed the digital transformation journey by interviewing traditional enterprises in traditional industries, such as the financial industry, and then they developed a framework that can guide organizations through the journey, as shown in figure (1). Firstly, the journey starts

with digital sensing, in which the organization scans for technological trends in the industries, competitors, partners, and customers. Then, the organization promotes digital mindsets and formulates digital strategies. Secondly, the organization adopts lean start-up methodologies and creates minimum viable products. Then, the organization establishes and tests new business models and allocates resources. Thirdly, the organization measures its digital workforce maturity. Then, it interacts with different digital partners and joins new digital ecosystems. After that, it digitizes its business models and builds a team-based structure. Finally, organizations must always keep an eye on external triggers such as disruptive digital technologies, internal enablers such as executive support, and internal barriers such as rigid strategic planning and high hierarchy level.

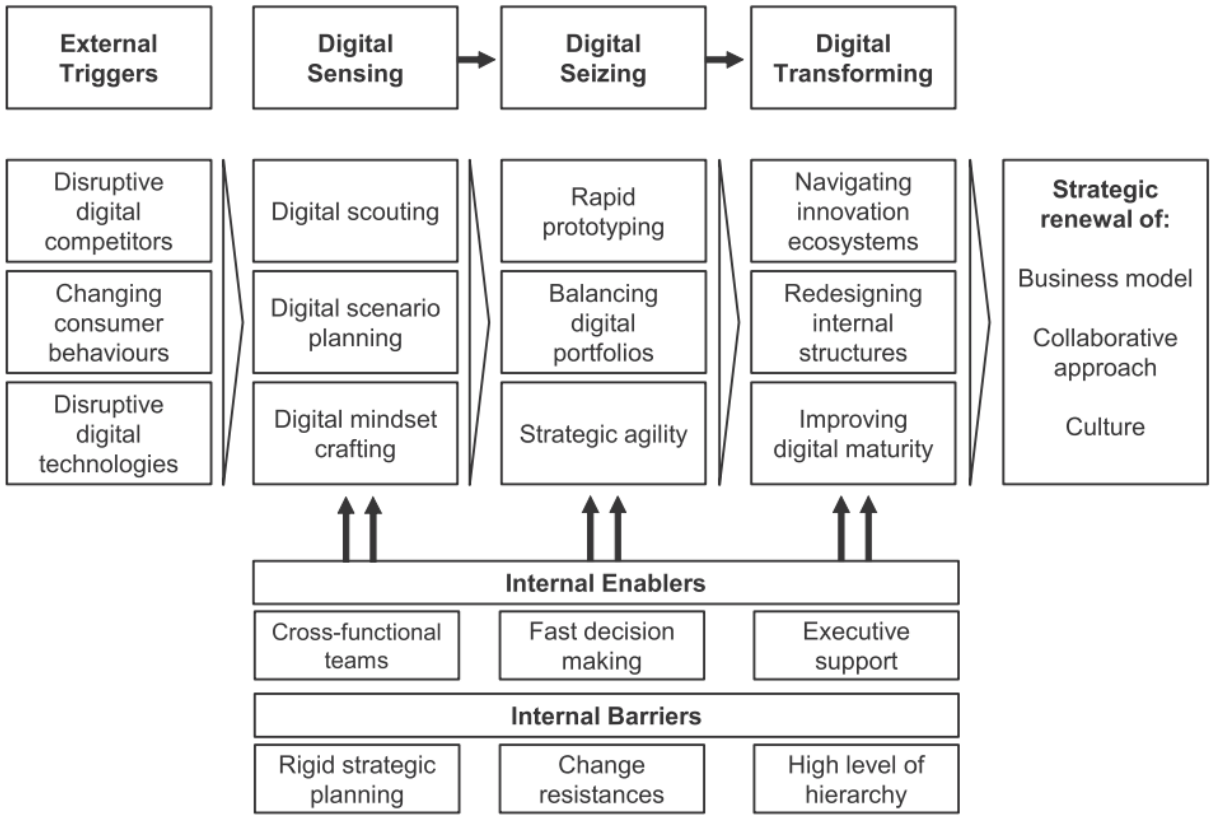


Figure (2): Warner and Wäger (2019) Digital Transformation Framework

Strategic flexibility has a significant role in the success of the digital transformation journey (Fachrunnisa et al., 2020). One of the important factors of strategic flexibility of an organization that plays a significant role in the success of the digital transformation journey is the

technological capability of the organization (Sony et al., 2022). Technological capability is the ability of an organization to be effective and efficient in utilizing technology during transformation compared with its competitors. There are four components of technological capability which are (Al-Mamary et al., 2020):

1. Technology-acquiring capability:

It is the ability of an organization to acquire new technology through formal or informal channels.

2. Technology-operation capability:

It is the ability of an organization to operate the technology effectively and efficiently.

3. Technology-shifting capability:

It is the ability of an organization to adjust the parameters of its technologies to improve processes, services, and products.

4. Technology-upgrading capability:

It is the ability of an organization to upgrade its technology to meet the changing market demands.

Sony et al. (2022) analyzed the impact of the four technological capability components on strategic flexibility. They found that the four components have a positive impact on improving strategic flexibility and improving competitive advantage.

From the previous sections, it was concluded that IT Governance Flexibility improves IT Flexibility which improves Strategic Flexibility which improves Digital Transformation. Hence,

improve the benefits of cloud adoption because cloud adoption is a form of digital transformation.

Conclusion of Chapter 5

From this chapter, it was concluded that organizations, including financial institutions, need to improve their strategic flexibility in order to be able to monitor changes in the market and technology and respond quickly and create competitive advantages. In order to improve their strategic flexibility, they need to adopt a more flat and agile organizational culture. They need to have a flexible IT infrastructure to be able to adjust their IT infrastructure in a short duration of time. They also need to be able to exchange data quickly with their customers and supply chain partners. One of the best IT technologies that can satisfy the requirements of IT flexibility is cloud computing due to its characteristics and benefits, which are mentioned in section 3.3 and section 3.12.

Chapter 6 Cloud Governance & Management Framework

Introduction of Chapter 6

In order to build a strategic, holistic multi-cloud governance frame, an in-depth understanding of the available cloud governance frameworks, lifecycles, and structures is needed. Section 6.1 presents two of the most common IT governance frameworks ITIL framework and COBIT framework. Section 6.2 presents the lifecycle of cloud governance. Section 6.3 presents the organizational structures within cloud governance. Finally, this chapter ends with a conclusion.

6.1 Cloud Governance Frameworks

Researchers analyzed the available IT governance framework to test its suitability for cloud governance. They found that they are not much suitable for cloud governance. As a result, they adapted it to cloud computing. The following sections summarize the findings of their research.

6.1.1 ITIL Framework

The Information Technology Infrastructure Library (ITIL) Framework is a widely adopted framework that is used to govern IT services. However, the ITIL Framework is initially developed for on-premises data centers. Many researchers adjusted this model to make it suitable for cloud computing (Mourad & Hussain, 2014). Karkošková (2018) proposed a cloud governance framework based on ITIL Framework as the following:

1. Cloud Service Strategy

The goal of this phase is to plan a cloud migration journey. This phase includes seven processes.

a. Cloud Provider Portfolio Management:

This process evaluates the cloud providers available on the market.

b. Cloud Service Portfolio Management:

This process evaluates the available cloud services from cloud providers.

c. Cloud Service Risk Management:

This process analyzes the potential risks of migrating to the cloud.

d. **Cloud Services Financial Management:**

This process performs a cost-benefit analysis of migrating to the cloud.

e. Cloud Service Compliance Management:

This process evaluates the legislative and regulatory requirements of cloud services.

f. Cloud Service Agreement Management:

This process ensures that the cloud services can be monitored against SLAs.

g. Cloud Exit Strategy Management:

This process involves preparing plans for ending the contract with the cloud provider and migrating to an on-premises data center, private cloud, or another public cloud.

2. Cloud Service Selection:

This phase ensures that the selected cloud services meet the functional and non- functional requirements and are provided by the optimal cloud provider.

3. Cloud Service Transition:

This phase is the base for planning, testing, and migrating to the cloud. This phase has four processes.

a. Cloud Service Transition Planning:

This process plans and coordinates the activities and resources needed to migrate to the cloud.

b. Cloud Service Validation and Testing:

This process validates that the provided cloud services fulfill the functional requirements and non-functional requirements.

c. Cloud Service Access Management:

This process plans and implements identity and access management plans.

e. Cloud Service Migration Management:

This process plans and coordinates the activities needed to migrate to the cloud.

4. Cloud Service Operation

This phase ensures that the cloud services meet the SLAs and the acceptable level of performance by monitoring the cloud events and logs and responding to incidents and requests from the cloud users.

a. Cloud Service Event Management Process

This process provides up-to-date data logs about the cloud services.

b. Cloud Service Incident Management Process

This process performs activities that will restore the cloud services after an incident.

c. Cloud Service Problem Management Process

This process minimizes the impact of incidents and prevents their recurrence.

d. Cloud Service Request Fulfillment Process

This process receives and manages the handling and fulfillment of a request from a cloud user to adjust a cloud service.

e. Cloud Service Request for Access Management Process

This process receives and manages the request from a cloud user to access a cloud service.

f. Cloud Service Monitoring Process

This process utilizes monitoring tools that monitor the parameters of cloud services and compare them with SLAs. If any deviation from SLAs occurs, the process generates and sends reports to cloud consumers and cloud providers.

5. Cloud Continual Service Improvement

This phase ensures the continuous improvement of cloud services in terms of effectiveness, efficiency, acceptable level of risks, and cost reduction. If the cloud consumer is unsatisfied with cloud services, they can request a change to cloud service or SLAs.

6.1.2 COBIT

Control Objectives for Information and Related Technology (COBIT) is one of the most popular industry frameworks that allows an organization to govern and manage the technology and the data of an organization. The first version of COBIT was released in 1996 by Information Systems Audit and Control Association (ISACA) to help the financial audit community better govern IT environments (De Haes et al., 2013). Every few years, ISACA releases a new version of COBIT. With each new version, COBIT is transitioning toward an IT governance and management framework with tools, including maturity models. The latest version is COBIT 2019 (ISACA, 2018). The COBIT frameworks are commonly adopted by financial institutions (De Haes et al., 2016) (Vugec et al., 2017) (Al-Fatlawi et al., 2021).

The definition of control in COBIT is "*The policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.*"

The COBIT defines six principles for governance system (ISACA, 2018):

1. Meeting Stakeholder Needs

Each organization needs a governance system to identify the stakeholders' needs and balance the needs, risks, and resources.

2. Holistic Approach

The governance system is built from different components that affect each other. In order to build a holistic governance system, the organization must consider its environmental factors, organizational factors, and technological factors.

3. End-to-End Governance System

The governance system should consider not only the IT functions but the entire data estate and the IT infrastructure, including endpoint devices, regardless of their location.

4. Separating Governance from Management

COBIT differentiates between governance and management as the following:

The Purpose of Governance ensures:

a. Identifying the stakeholders' needs to determine the organization's objectives.

b. Setting the directions for achieving the organization's objectives.

c. Monitoring performance and compliance against the direction and the objective.

The purpose of Management ensures:

Planning, running, and monitoring activities to ensure that the organization's objectives are in alignment with the direction that was set by the governance entity.

5. Dynamic Governance System

The governance system should be dynamic so that when a factor changes, the impact of the change can be considered in the governance system.

6. Tailor to Enterprise Needs

Any governance system must be tailored to the organization's needs using a set of principles and guidelines.

COBIT defined three principles for a governance framework (ISACA, 2018):

1. A governance framework should be based on a conceptual model, identifying the key components and relationships among components to maximize consistency and allow automation.

2. A governance framework should be open and flexible. It should allow adding new content and the ability to address new issues in the most flexible way while maintaining integrity and consistency.

3. A governance framework should align with relevant related standards, frameworks, and regulations.

COBIT identified 12 design factors that influence the governance system as the following:

1. Enterprise Strategy:

Each organization has an enterprise strategy that defines its goals. Examples of enterprise strategies are cost leadership, and innovation differentiation.

2. Enterprise Goals:

The enterprise strategy is realized by achieving the enterprise goals. Examples of enterprise goals are customer-oriented service culture and compliance with laws and regulations.

3. Risk Profile:

The enterprise must define its risk profile to assess the cloud provider and its cloud services based on it. Then, create a catalog of the approved cloud provider and their cloud services that the business users can use.

4. Information and Technology related Issues:

Information and Technology related issues that the organization must solve in order to achieve enterprise goals. Examples are Service delivery issues by IT outsources and Failure to meet IT-related regulatory requirements.

5. Threat Landscape:

The level of threat landscape under which the organization operates. The levels are low, normal, or high.

6. Compliance Requirements:

The level of compliance requirements under which the organization operates. They are classified into low, normal, or high.

7. Role of IT:

The role of the IT department within the organization. It is categorized into Support, Factory, Turnaround, or Strategic.

8. Sourcing Model of IT:

The sourcing model of IT functions. It is classified into insourcing, Outsourcing, Cloud, or Hybrid.

9. IT Implementation Methods:

Agile, DevOps, Traditional, or Hybrid.

10. Technology Adoption Strategy:

First Mover, Follower, Slow Adopter.

12. Enterprise Size:

Large Enterprise.

Small and Medium Enterprise.

6.2 Cloud Governance Lifecycle

Karkošková and Feuerlicht (2017) found that the widely accepted IT governance frameworks do not fully address the requirements of cloud computing. They proposed a cloud governance lifecycle model that guides the implementation and continuous improvement of cloud governance activities. They proposed their model based on SOA governance because they share some similarities, which were already discussed in section 3.8.

Their model consists of four main phases:

1. Planning phase:

The activities of this phase involve the analysis of existing governance models and processes. Then, developing a cloud governance strategy. Finally, developing a cloud governance roadmap.

2. Definition phase:

The activities of this phase involve the definition of organizational structure and assigning roles and responsibilities. Then, defining cloud governance artifacts and governance processes. Finally, creating transition plans.

3. Implementation phase:

This phase involves the implementation of transition plans.

4. Monitoring phase:

The activity of this phase involves the collection of data on cloud governance processes. Then, evaluating the cloud governance process in order to improve cloud governance in the next cycle.

6.3 Cloud Governance Structure

Prasad et al. (2014) conducted research in order to identify what IT governance structures are appropriate for governing cloud computing. They found that the governance of cloud computing will need to govern three layers:

1. **Business Governance Layer:**

   It governs the management of cloud services.

2. **Service Governance Layer:**

   It governs the monitoring, tracking, and enforcement of cloud services.

3. **Technical Governance Layer:**

   It governs the designing, the implementation, the deployment, and the maintaining of cloud services.

Then, a cloud consumer must form 4 entities that will govern different roles within the three cloud governance layers. The four entities are (1) Chief Cloud Officer, (2) Cloud Management Committee, (3) Cloud Service Facilitation, and (4) Cloud Relationship Center.

1. Chief Cloud Officer:

The Chief Cloud Officer (CCO) is a role that is similar to Chief Technology Officer, but he or she is a very expert in cloud computing. The Chief Cloud Officer monitors the cloud market and assists the organization, the cloud providers, and the cloud brokers in designing more and better cloud services.

2. Cloud Management Committee

It is a management entity within the cloud consumer that manages the migration to cloud computing. Its members are cloud decision-makers and cloud service users. As cloud computing evolves, cloud adoption increases and becomes more complicated. The organization needs to add more stakeholders to the Cloud Management Committee to keep its cloud environment under control and fulfill its business needs.

3. Cloud Service Facilitation

It is a management entity within the cloud consumer that manages the operations of the cloud environment. Within this entity, there is a role called Cloud Service Manager. The Cloud Service Manager monitors cloud performance, manages change facilitation, and resolves issues. The Cloud Service Facilitation should develop a cloud services requisition system allowing business users to request cloud services. The Cloud Service Facilitation will execute the decisions of the Cloud Management Committee. The Cloud Management Committee will decide what must be done through the cloud, while the Cloud Service Facilitation will decide how it will be done.

4. Cloud Relationship Center

It is a management entity within the cloud consumer that manages the communications between the cloud consumer and the cloud providers and solves the conflicts between them.

Conclusion of Chapter 6

From this chapter, it was concluded that any organization should consider establishing these entities to govern better and manage their cloud environment.

1**. Establish Chief Cloud Executive role:**

i. Define any organizational changes, roles, and responsibilities with the board members.

ii. Manage the following entities.

2. Establish Cloud Center of Competency or Excellency (CCOC) or (CCOE).

They will be responsible for the cloud management governance layer.

i. Analyze any digital transformation triggers within the organization or outside the organization.

ii. Analyze any business needs.

ii. Analyze the cloud market for the available cloud capabilities and industry trends.

iii. Identify the best-of-breed cloud services at different cloud providers.

iv. Conduct a risk assessment for the selected cloud services.

v. Create a catalog for the services that passed the risk assessment.

vi. Provide cloud guidance for the organization.

vii. Manage the communication and the partnerships with cloud providers.

3. Establish Cloud Migration Team:

They will be responsible for the cloud technical governance layer.

i. Execute the decisions of CCOC or CCOE.

ii. Evaluate the workloads and their dependencies.

iii. Identify the best possible migration strategies for each workload.

iv. Design the migration roadmap.

v. Execute the migration.

4. Establish Cloud Operation Team:

They will be responsible for the cloud service governance layer.

i. Monitor the operations of the cloud environment.

ii. Maintain and solve any issues.

iii. Control identity and access management to the cloud.

iii. Receive tickets from the cloud users.

iv. Measure cloud performance against SLAs.

Then, the organizations should define cloud adoption and migration strategy as the following:

1. They need to evaluate the cloud providers and their cloud services.
2. They need to perform risk analysis for their cloud services.
3. They need to evaluate the regulatory requirements of cloud services.
4. They need to define a cloud exit strategy before migrating to the selected cloud provider to minimize the cost and the effort of the cloud exit plan.

Chapter 7 Research Model for Expert Interviews

Introduction of Chapter 7

Frameworks are commonly used in research to narrow the research scope and identify relevant data, theories, and variables (Green, 2014). There are two types of frameworks that are used in research: Theoretical Frameworks and Conceptual Frameworks. Theoretical Frameworks are frameworks that are developed based on one theory or various theories, while Conceptual Frameworks are frameworks that are developed based on various concepts (Fain, 2004) (Parahop, 2006). The concepts of a conceptual framework are linked to the components of research questions. These concepts allow a researcher to narrow the scope of the needed data to get the correct answers. The following points summarize conceptual frameworks' role (Pauwels, 2011).

- Providing the overall structure in which a researcher can articulate and examine the objective of a research.
- Serving as a compass for identifying the relevant literature and theories.
- Provide context for the research.
- Help to develop, refine, and delimit research questions, interview questions, and questionnaire questions.
- Help to develop a framework for collecting data.
- Serving as a mechanism to reflect on the value of the research once it is completed and to suggest future research questions.

This chapter is organized as follows. Section 7.1 defines strategic frameworks. Section 7.2 defines the holistic approach. Section 7.3 presents two technology adoption theories and frameworks as the following. Section 7.3.1 presents the Diffusion of Innovation technology

adoption theory. Section 7.3.2 presents the Technology-Organization-Environment model. Section 7.4 presents the research model developed from the previous theory and model. The research model allowed the development of the questions for the expert interviews.

7.1 Strategic Frameworks

The implementation of an organizational strategy directly affects or indirectly affects all the dimensions of an organization (Okumus, 2003). Okumus (2003) conducted a literature review and identified eight strategic frameworks in industry and academia. He analyzed the frameworks, identified 11 key factors, and finally grouped these factors into four categories. The following table summarizes them.

Category	Factor	Definition
Strategic Content	**Strategic Development**	Why and how the strategy is initiated
	Issues that must be considered	
	The new strategy must be consistent with the overall strategic direction of the organization.	
	The aim of the new strategy should be clearly identified.	
	The level of participation from all levels of management is recommended.	
	The potential impact of ongoing projects and future projects on the new strategy must be considered.	
Category	**Factors**	**Definition**
External Context	**Environmental Uncertainty**	The degree of uncertainty and changes in the environment.
	Issues that must be considered	
	The changes in environments require new strategy	
	The new strategy should be appropriate to the market condition	

Category	**Factors**	**Definition**
Internal Context	**Organizational Structure**	Job duties and responsibilities
		Decision-making approaches
		Distribution of power
		Labor skills and knowledge
	Issues that must be considered	
	The impact of new strategy on job duties, roles, and decision-making.	
	The role of organizational structure on the free flow of information, coordination, and cooperation between different levels of management and functional areas.	
	Factors	**Definition**
	Organizational Culture	The shared understanding of employees about how they do thing within an organization.
	Issues that must be considered	
	The impact of organizational culture on communication, coordination and cooperation between different management and functional levels.	
	The impact of the new strategy on the organizational culture and subculture.	
	The needed efforts and activities to change organizational culture and subculture.	
	Factors	**Definition**
	Leadership	The support of the top management.
	Issues that must be considered	
	The actual involvement of top management.	
	The level of support and backing from top management	

Category	Factors	Definition
Organizational Process	**Operational Planning**	The process of initiating the project and the operational planning of the implementation of activities.
	Issues that must be considered	
	The Preparing and planning of the implementation of activities.	
	The participation and feedback from different levels of management.	
	Factors	**Definition**
	Resource Allocation	The process of ensuring all the necessary time, financial resources, skills, and knowledge is made available. It is linked to operational planning.
	Issues that must be considered	
	Securing all the required resources	
	Time scale of making resources available and using them.	
	Factors	**Definition**
	People	Recruiting new staff, providing training and incentive for relevant employees. Operational planning and resource allocation have a direct impact on this factor.
	Issues that must be considered	
	Train current staff.	
	Hire staff who have the new skills and knowledge.	
	The impact on organization Human Resource Management policies and practices.	
	Factors	**Definition**
	Control and Feedback	The formal and informal mechanism that allows the efforts and results of implementation to be

		monitored and compared against predetermined objectives.
	Issues that must be considered	
	The monitoring activities carried out during and after implementation.	
	The Communication and operational plans are key to monitoring the process and provide feedback on the progress.	
	Factors	**Definition**
	Outcome	The intended and the unintended results of the implementation process.
	Issues that must be considered	
	Was the strategy implemented according to the plan?	
	Were the outcomes satisfactory?	
	What did the organization learn?	

Table (8): Okumus Framework for implementing Organizational Strategies

From the previous sections, it was concluded that to implement a new organizational strategy. A holistic framework is needed to identify all the relevant factors or dimensions so that all the stakeholders can consider the impact, requirements, and expected outcome of the new strategy. In addition, prepare all the required operational activities, resource planning, communication mechanisms, and feedback process to govern the new strategy's implementation. Therefore, the next section will investigate the role of a holistic framework in IS research.

7.2 Holistic Approach

The concept of holistic is defined as "a *belief that the parts of something are intimately interconnected and explicable only by reference to the whole*." (Oxford, 2019). Another definition "*analysis and evaluation of a system as a complex entity, whereby its individual components are in constant relation with each other." (Högler, 2012)*. From this definition, the

relevant components of a holistic framework are needed to be identified. In order to do so, a literature review is conducted to identify and analyze the used frameworks and theories in the IS research. The literature review started by identifying the technology adoption theories and frameworks, and then the commonly used ones in cloud-related research were chosen.

7.3 Theories and Frameworks of Technology Adoption

This section presents the most common theories and frameworks used in technology adoption research. Subsection 7.3.1 presents the Diffusion of Innovation theory. Subsection 7.3.2 presents the Technological-Organizational-Environmental model.

7.3.1 Diffusion of Innovation (DOI)

The Diffusion of Innovation (DOI) is a theory that seeks to explain how, why, and at what rate new ideas are spread across society and adopted. The theory was developed by Professor Everett Rogers in his book Diffusion of Innovations in 1962. The theory has five elements that influence the spread and adoption of new ideas: innovation, adopters, communication channels, time, and social system. The following table summarizes the theory.

Diffusion of Innovation (DOI)	
Description	
Explain how, why, and at what rate new ideas and technology spread.	
Dimensions	**Definition**
Innovation	Any idea, innovation or technology that is new to an organization.
Adopters	The unit of people who want to adopt a new innovation. Examples: (Individual, team, organization).

Communication Channels	The diffusion or transfer of information between the adopters about innovation over time
Time	The duration of time that is needed to adopt a new innovation
Social System	A combination of external factors (ex: Regulations) and internal factors (ex: Organizational structures) that has an impact on an organization's decision for adopting a new innovation.
Adoption Stages	Definition
Awareness and Knowledge	The potential adopters find out about an innovation.
Persuasion	The potential adopters are interested in an innovation and actively seek more details.
Decision	The potential adopters evaluate the advantages and the disadvantages of the innovation, and then they decide whether to adopt or reject the innovation.
Implementation	The adopters implement the innovation and then they evaluate the usefulness of it.
Continuation	The adopters decide whether they continue to use the innovation or not.
Limitation	
It focuses on the behavior of the adopters. It does not consider the characteristics of technological factors.	

Table (9): Diffusion of Innovation (DOI)

Although the DOI is used in many IS research, some researchers argue that it does not consider all the relevant dimensions, such as technological factors. As a result, some researchers combined DOI theory with other theories or frameworks, such as Technology-Organization-Environment (TOE) framework and Human-Organization-Technology fit (HOT-fit) framework (Lian et al., 2014) (Oliveira et al., 2014) (Gangwar et al., 2015) (Alkhalil et al., 2017) (Lynn et al., 2018) (Hiran & Henten, 2019) (Chatterjee et al., 2021).

7.3.2 Technology-Organization-Environment (TOE) framework

The Technology-Organization-Environment (TOE) framework was developed in 1990 by Tornatzky and Fleische (Tornatzky et al., 1990). They developed the model to facilitate innovation adoption by organizations. A literature review has been conducted to investigate this framework's usage in IS research. It was found that this framework is used a lot in IS research because it considers three dimensions of an organization that impact the adoption of innovation: Technology dimension, Organization dimension, and Environmental dimension. The following table explains the three dimensions and identifies the commonly used factors in cloud-related research.

Dimension	**Dimension Definition**	
Technology	Describes the characteristics of a technology and identifies the factors that affect an organization's decision to adopt this technology	
Factors	**Factor Definition**	**References**
Relative Advantage	The degree to which a technology is believed to provide more benefits for an organization.	(Zhu et al., 2006) (Ramdani et al., 2009) (Low et al., 2011) (Alshamaila et al., 2013) (Chang et al., 2013) (Gangwar et al., 2015) (Safari et al., 2015) (Wahsh & Dhillon, 2015) (Ali et al., 2020)

Compatibility	The degree to which a technology is perceived as consistent with the organization's technological infrastructure. Example of Sub-factors are: - Interoperability - Portability	(Zhu et al., 2006) (Ramdani et al., 2009) (Low et al., 2011) (Alshamaila et al., 2013) (Gangwar et al., 2015) (Wahsh & Dhillon, 2015) (Rahimah & Aziati, 2017) (Ali et al., 2020) (Qasem et al., 2020)
Complexity	The degree of difficulties that an organization encounters when it will adopt new technology.	(Ramdani et al., 2009) (Alshamaila et al., 2013) (Gangwar et al., 2015) (Safari et al., 2015) (Wahsh & Dhillon, 2015) (Rahimah & Aziati, 2017) (Ali et al., 2020) (Qasem et al., 2020)
Security Concerns	The degree of an organization's trust in a technology.	(Zhu et al., 2006) (Alshamaila et al., 2013) (Gangwar et al., 2015)

		(Wahsh & Dhillon, 2015) (Ali et al., 2020) (Qasem et al., 2020)
Dimension	**Definition**	
Organization	Describes the characteristics of an organization that might have a significant impact on their decision.	
Factors	**Factors Definition**	**References**
Organizational Readiness	The degree to which an organization has the resources, awareness, and governance to adopt a technology	(Low et al., 2011) (Zhu et al., 2006) (Alshamaila et al., 2013) (Chang et al., 2013)
Top Management Support	The degree to which top management supports and backs the adoption of a technology.	(Zhu et al., 2006) (Ramdani et al., 2009) (Low et al., 2011) (Alshamaila et al., 2013) (Chang et al., 2013) (Gangwar et al., 2015) (Wahsh & Dhillon, 2015) (Rahimah & Aziati, 2017) (Ali et al., 2020) (Qasem et al., 2020)

Dimension	Definition	
Environment	Determines the environmental elements that might affect an organization's intention to adopt a technology	
Factors	**Factors Definition**	**References**
Regulations	The impact of laws and regulations on an organization's decision to adopt a technology	(Ramdani et al., 2009) (Low et al., 2011) (Alshamaila et al., 2013) (Chang et al., 2013) (Gangwar et al., 2015) (Safari et al., 2015) (Rahimah & Aziati, 2017)
Industry Pressure	The impact of customer, suppliers, partners and competitors on an organization' decision to adopt a technology	(Qasem et al., 2020) (Zhu et al., 2006) (Low et al., 2011) (Alshamaila et al., 2013) (Chang et al., 2013)

Table (10): Technology-Organization-Environment (TOE)

7.4 Research Model for Expert Interviews

Reference to the previously mentioned frameworks:

- Okumus Framework for implementing Organizational Strategies
- Diffusion of Innovation (DOI) theory
- Technology Organization Environment (TOE) framework

The research model shown in table (11) allowed the creation of the interview questions. The research model is divided into three dimensions: Organizational Dimension, Technological Dimension, and Environmental Dimension. For each dimension, the factors that will be considered during the interviews are identified. Moreover, for each dimension, there are a set of tasks that can be performed to improve these factors. From this research model, the interview questions were developed. The interview questions asked the interviewee about the organizational challenges, the technological challenges, and the environmental challenges. If the interviewee did not understand the question, then the interviewee was guided by mentioning the factors related to each dimension. After asking for each dimension of the challenges, the interviewee was asked for the solutions. Moreover, again, if the interviewee did not understand the question, then the interviewee was guided by mentioning the tasks related to the dimension. The questions from the expert interviews can be found in Appendix A.

Organizational Dimension	**Technological Dimension**	**Environmental Dimension**
Organizational Factors	**Technological Factors**	**Environmental Factors**
Awareness (DOI) Organizational Readiness (TOE) Organizational Culture (Okumus) Organizational Structure (Okumus) Knowledge (DOI) Skills (DOI) Top Management Support (TOE)	Technological Compatibility (TOE) Technological Complexity (TOE) Security Concerns (TOE)	Laws and Regulations (TOE) Customers Expectations (TOE) Suppliers Requirements (TOE) Partners Requirements (TOE) Sustainability Requirements (TOE) Environmental Uncertainty (Okumus)
Tasks	**Tasks**	**Tasks**
Identify the relevant knowledge and skills of the current staff.	Identify the current cloud technologies.	Identify the laws and the regulations that govern and restrict any decision related to cloud adoption.

Identify the needed knowledge and skills.	Analyze the dependency between the cloud workloads.	Identify the expectations of the customers.
Train current staff.	Identify the impact of the new cloud workloads (Interoperability – Portability – Integration)	Identify the requirements of suppliers and partners.
Hire new employees if needed.	Analyze the impact of new cloud workloads that are deployed on the security posture of the new multi-cloud environment.	Identify the impact of new multi-cloud environment on sustainability
Monitor the communication and the feedback process of employees.	Prepare and plan the migration activities.	Measure the impact on sustainability score.

Table (11): Research Model for Expert Interviews

Chapter 8 Expert Interviews Results

Introduction of Chapter 8

This chapter presents the results of the semi-structured interviews with the experts. The chapter is organized as the following. Section 8.1 presents an overview of the interviews. Section 8.2 presents the analysis of the interviews as the following: section 8.2.1 presents the organizational challenges and their solutions, section 8.2.2 presents the technical challenges and their solutions, and section 8.2.3 presents the environmental challenges. Section 8.3 presents the benefits of migrating to multi-cloud by financial institutions.

8.1 Interviews Overview

As mentioned in section 2.3, Accenture does not allow the interns to interview clients. Therefore, Accenture experts were interviewed only. Accenture experts were chosen using this process:

1. Accenture Knowledge Base was checked to identify case studies or success stories for multi-cloud projects within the financial industry from different regions.
2. Accenture experts that were mentioned in these projects were sent interview invitations.

To diversify the results of the interviews, Accenture employees from Accenture Netherlands, Accenture Ireland, Accenture UK, and Accenture USA were interviewed. They were interviewed in order to identify the following:

- The reasons that made the financial institutions adopt and migrate to multi-cloud.
- The benefits that the financial institutions realized after migrating to multi-cloud.

- The organizational, technological, and environmental challenges that the financial institutions encounter before, during, and after the migration to multi-cloud.

- The solutions that the financial institution took to solve the previous challenges.

The number of the interviews was seventeen. All the interviews were conducted and recorded through Microsoft Teams.

The details of the interviewees are summarized in the following table.

ID	Region	Level	Title	Domain
Int-01	Netherlands	Manager	Technical Architect	**Enterprise Architecture** **Technical Architecture** **Multi-cloud Integration**
Int-02	Ireland	Senior Manager	Technical Architect	**Technical Architecture** **Cloud Infrastructure**
Int-03	UK & Ireland	Associate Director	Technology Delivery Lead	**Technology Delivery**
Int-04	USA & Canada	Managing Director	Technology Strategy	**Strategy for Banking**
Int-05	Netherlands	Senior Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-06	Netherlands	Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-07	UK	Senior Manager	Technology Consulting	**Technology Consulting for Banking**
Int-08	Netherlands	Senior Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-09	USA & Canada	Managing Director	Data & AI Value Strategy	**Data and AI**

Int-10	Netherlands	Associate Director	Technology Delivery Lead	**Cloud Consultancy**
Int-11	Netherlands	Senior Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-12	UK	Senior Manager	Technology Consulting	**Technology Consulting for Banking**
Int-13	USA	Associate Director	Alliance Insights & Management	**Financial Services Ecosystem**
Int-14	USA	Senior Manager	Cloud Security	**Cybersecurity**
Int-15	Netherlands	Associate Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-16	Netherlands	Associate Manager	Cloud Migration & Implementation	**Cloud Consultancy**
Int-17	Netherlands	Associate Manager	Cloud Migration & Implementation	**Cloud Consultancy**

Table (12): Details of Expert Interviewees

In order to focus on the results of each interview, the interview questions were sent to the interviewee one day before the interviewer. During the interview, the purpose of the interview was explained to the interviewee. Then, the interviewee was asked to choose a multi-cloud project of a financial institution that he or she knows well to discuss during the rest of the interview. The purpose of the interview is to interview the interviewee as if he or she was the client. Due to the confidentiality of the clients, the interviewees provided only the type and the location of their clients, as shown in the following table.

Interviewee	**Project**	**Location**
Int-01	Bank	Netherlands
Int-02	Bank	Ireland
Int-03	Bank	UK
Int-04	Different Banks	USA & Canada

Int-05	Insurance	Netherlands
Int-06	Insurance	Netherlands
Int-07	Bank	UK
Int-08	Bank	Netherlands
Int-09	Different Bank	USA
Int-10	Bank	Netherlands
Int-11	Bank	Netherlands
Int-12	Bank	UK
Int-13	Bank	USA
Int-14	Bank	USA
Int-15	Bank	Netherlands
Int-16	Insurance	Netherlands
Int-17	Insurance	Netherlands

Table (13): Project Details of Expert Interviewees

8.2 Interviews Results

The interviews were analyzed qualitatively using the process that was mentioned in the research methodology section 2.1 as the following:

1. The interviews were recorded using Microsoft Teams.

2. Each interview was transcribed by listening to the recording, playing it slowly, and writing the dialogue to Microsoft OneNote.

3. The transcripts were added to a table and mapped each question with each answer.

4. The important keywords for each answer were highlighted.

5. The keywords were compared in order to identify the similarities.

6. From the similarities, the codes were identified.

7. The codes were analyzed for similarities in order to discover themes.

8. The themes and their codes were compared with the cloud adoption drivers and barriers from the financial institution perspective identified in section 4.3 and section 4.4 to improve the naming of the themes and their coders.

8. The themes and their codes were categorized under either a challenge or a solution.

Appendix D presents the most important citations from the interviews.

8.2.1 Organizational Challenges & Solutions from Interviews

Organizational Challenge 1: Shortage of Cloud Skills

All the interviewees agreed that their financial institutions clients lacked the required skills for adopting the cloud. Starting from the top management, who did not know well the benefits and the challenges of cloud computing. This is why they requested Accenture support. At first, Accenture conducted a maturity assessment for the organizational readiness in order to identify the required skills, and then they conducted a maturity assessment for the IT infrastructure in order to identify how they will integrate their current IT infrastructure from mainframes, private cloud, or public cloud with the new public cloud(s). The following paragraphs present the most important citations from the interviews so that the readers can read the answers of the interviewees and notice the similarities. The similar keywords were bolded in order to identify the similarities because from the similarities, the codes and the themes are created.

The interviewee Int-02 (Technical Architecture) said:

*"The bank has gone through **full transformation**. So the bank was not ready for cloud. They set it up per department. The main **challenge** is **security**. Everyone in the bank **was not familiar with the cloud** or the **real benefits**. For the **shortage** of **skills**, the bank use third party vendors like Accenture. So they were short on skills and over time they have grown mature."*

The interviewee Int-01 (Enterprise Architecture - Multi-cloud Integration) said:

*"They have gone through **re-organization** last year. What they have done it that, there are two divisions. **CIO division** and **CTO division**. The CIO covers all the products of the bank. And the CTO covers the technology part. The CTO is kind of enabler. Whatever the business needs from technologies, all the technologies are implemented by enablers teams. There are different enablers team such as the integration teams which I work with now. Some of their members are member of **CCOEs**."*

The interview Int-04 (Strategy for Banking) said:

*"I mean we find that making an effort to **train your workforce** for cloud is really **effective**. One of my banks trained over **1,700 technologists for public cloud in less than a year**. That is a pretty good number."*

Organizational Challenge 2: Security Concerns from Public Cloud due to Shortage of Skills

The next challenges were security and governance concerns. Many financial institutions established CCOC or CCOE in order to govern and manage their multi-cloud environment. The members of CCOC or CCOE are usually Enterprise Architects, Security Architects, and Cloud Architects.

The interviewee Int-01 (Enterprise Architecture - Multi-cloud Integration) said:

*"So, for how it works, for **each cloud environment**, there is a **Cloud Competence Center (CCOC) or Cloud Center of Excellence (CCOE)**. So, there are **owners of the muti-cloud environment**. And what they do firstly, they look into the services and **conduct risk assessments** because in financial industry **risk assessment is a crucial part** of onboarding any new service or any new vendor. So, what these CCOE do is that **they look into services** that are offered by these **cloud environments**. And they **do risk assessment** and then once the services are risk assessed,*

*they approved them. Only then, I can use it. So what these **CCOE** do it that, they **keep an eye on the available cloud services**, and then they **do risk assessment**. Once, it passed, they make it **available**. And they are also responsible for onboarding DevOps teams to different cloud environments."*

The interviewee Int-02 (Technical Architecture) said:

*"There is a **Cloud Center of Authority**. When I need a cloud service that is not available in the landing zones. Then I need to ask the Cloud Center of Authority who **are group of Enterprise Architects, Security Architects, and Cloud Architects** who review the requested cloud service. After their approval, the **CCOE** will set up the controls and allow it in the landing zones. After that, I will be able to use it."*

Organizational Challenge 3: Complexity of defining Cloud Adoption and Migration Strategy

The last challenge was the lack of cloud migration strategy and cloud exit strategy. One of the financial institutions migrated to the cloud without any strategy. Their business users were buying resources using credit cards. This behavior was also found by another research that was mentioned in chapter 1 table (1) (How banks approach the clouds) Hon & Millard (2018a).

The interview Int-11 (Cloud Consultancy) said:

*"They were already engaged with Azure. They had some deployment done. There was no structure, no landing zones actually. First of all **the strategy was important**. They had several departments that use a credit card type of work to deploy cloud resources**. It was not a strategy**. So, we obviously, we need to help the client **to build up the strategy**, and the cloud reference architecture."*

8.2.1.1 Summary of the organizational challenges and their solutions:

1. Shortage of Skills:

a. Shortage of Cloud Engineering Skills.

b. Shortage of Mainframe engineering skills.

c. Shortage of DevOps skills.

d. Shortage of Multi-Cloud Management Skills.

Since each public cloud provider has its own cloud management portal. The organizations usually use multi-cloud management solutions that can monitor and manage different cloud environments from a centralized portal.

2. Security Concerns from Public Cloud due to Shortage of Skills.

3. Complexity of defining Cloud Adoption and Migration Strategy.

The solutions that were adopted to solve the organizational challenges were:

1. Conduct organizational readiness assessment:

a. To identify the re-organization requirement.

b. To identify the required skills and knowledge in order to identify the trainings and the recruitment requirements.

2. Establish CCOC or CCOE:

a. To define with the stakeholders the cloud migration strategy.

b. To define Security Architecture of the cloud.

c. To conduct risk assessment for cloud providers and their cloud services.

d. To create a catalog of approved cloud services.

3. Define the cloud migration strategy and the cloud exist strategy at the same time:

a. To avoid vendor-lock in.

b. To improve portability between cloud providers.

c. Decrease the effort and the cost of cloud exit strategy.

8.2.2 Technological Challenges from Interviews

Technological Challenge 1: Vendor-lock in due to the usage of Cloud Native Tools

Some of the financial institutions that adopted cloud computing a few years ago, developed their infrastructure and workloads on the cloud using cloud native tools. Then, when they decided to adopt a second public cloud provider, they found that they were vendor-lock-in because they would have to re-develop their infrastructure and workloads again for the second public cloud provider. In order to avoid this challenge, it would be better to develop infrastructure and workloads using cloud agnostic tools.

The interview Int-02 (Technical Architecture) said:

*"At the moment they are **vendor-lock in**. At first the **strategy** in the bank was **not multi-cloud**, it was leverage a single cloud. Unfortunately, in AWS, they developed everything using AWS **native tools**. So, AWS CloudFormation to **build infrastructure**. However, later on Azure, they started to use Terraform. It was the maturity of the bank was better.*

*So, the bank is looking now to export the code that was written in AWS CloudFormation to Terraform. There is a **dedicated project** that will brings the code to Terraform. The goal is to rebuild the AWS infrastructure using Terraform. So, until now there is **no portability**, if **something breaks** in AWS, it can be rebuild in AWS, but not in Azure."*

The interview Int-03 (Technology Delivery) said:

*"So, we did a lot of work to **use** whatever possible to **use cloud agnostic tools**. We **avoided** using the **cloud native tools**."*

The interview Int-10 (Cloud Consultancy) said:

*"They migrated to **one public cloud**. Then they realized later on that they are **vendor-lock in**. **After 2 years**, they decided to **re-consider the cloud migration strategy** and consider other public cloud. It is a good practice to develop your infrastructure using **cloud agnostic**."*

Technological Challenge 2: Complexity of Applications Dependency

Analyzing the cloud applications dependencies is a complex challenge especially if the employees of the financial institution do not understand the difference between their cloud environment and the new cloud environments.

The interview Int-11 (Cloud Consultancy) said:

*"Setting up a landing zone is not a big challenge. I call it it is more in the recent years a commodity. Any organization can set a landing zone. The **challenge** is **understanding** the **application landscape** and their **dependencies**."*

Technological Challenge 3: Limitation of Mainframe Applications

The next challenge was the mainframe applications limitations because they usually did not support standard API. As a result, the financial institution sometimes had to consult the mainframe vendors to implement interfaces that would allow the mainframe to be integrated with public cloud providers.

The interviewee Int-01 (Enterprise Architecture - Multi-cloud Integration) said:

*"IBM allowed the **mainframe** to **expose** its services via **http endpoints**. Then the cloud applications can call the http endpoints and **consume** services from mainframe. Similar, the mainframe can **consume** from cloud applications."*

The interviewee Int-04 (Strategy for Banking) said:

*"They are software engineers that are specialized in **multi-cloud integration**. What we find is that you can **modernize a mainframe** and make things **available** for **digital consumptions**. What we see is some of our clients is essentially **creating an API layer** that serves up the data that is in the mainframe for **consumption** by cloud products."*

The interviewee Int-06 (Cloud Consultancy) said:

*"We had to move part of the **mainframe hardware** to private cloud because it was **impossible** to **re-platform** some of the applications."*

Technological Challenge 4: Complexity of Applying Security Controls across different clouds.

The last challenge is applying security controls across the different cloud providers. One of the possible solutions is standardize and automate as much as possible security controls across the different cloud providers.

The interviewee Int-06 (Cloud Consultancy) said:

*"The challenges as I said was around **security**…. The security was managed by **security principles**. There is **security architects** who **manage all security solutions**. They define **consistency** in **security controls** across the **cloud providers**. The goal is to apply to the cloud providers **similar controls** based on security policies defined in the bank across the vendors. The cloud vendors AWS and Azure both have to follow the same security policies of the bank. So, the bank get the same security assurance and risk across both cloud providers."*

8.2.1.2 Summary of the technological challenges and their solutions

The Technical Challenges:

1. Vendor-lock in due to the usage of Cloud Native Tools:

Re-migrating the workloads to another public cloud providers was impossible or expensive because the landing zones were developed using cloud native tools. The financial institutions have to re-develop the landing zones on the new public cloud.

2. Complexity of Applications Dependency:

In order to migrate an application to another cloud. The financial institution must analyze the applications dependency in order to understand which components

must be migrated first and how they will integrate with the other components on the other clouds.

3. Limitation of Mainframe Applications:

a. Migration Limitation:

Sometimes the applications are tightly coupled with the hardware that it is impossible to migrate them to the cloud.

b. Integration Limitation:

Sometimes the applications do not support standard APIs that can integrate the mainframe with clouds.

4. Complexity of Applying Security Controls across different clouds.

The solutions that were adopted to solve the technical challenges were:

1. Use Cloud Agnostic Tools:

a. To avoid vendor-lock in.

b. To improve cloud portability between different clouds.

2. Make sure the current IT employees fully understand the applications dependencies.

3. Modernize Mainframe Applications:

a. Re-architect the monolithic applications into micro-service architecture.

b. Re-place mainframe applications with cloud native applications.

4. Standardize and Automate Security Controls.

8.2.3 Environmental Challenges from Interviews

All the interviewees agreed that the top priorities of financial institutions are security, stability, and cost reduction more than sustainability when they migrated to cloud a few years ago. However, some of them mentioned that in Europe, sustainability is becoming more important due to the Environmental, Social, and Governance (ESG). On the other hand, the interviewees found that some of their clients are considering building platforms with their suppliers and partners in order to create ecosystems. **Therefore, there were not any environmental challenges or solutions that could be identified.**

The interviewee Int-02 (Technical Architecture) said:

*"The **sustainability** is not a goal at the moment for a bank. For example if a service on a cloud is more green IT compared to on-premises, it does not matter for a bank. Their **top priority** is the **security**. The two main concerns for a bank when they want to migrate to cloud are **security** and **cost**. The goal is not to get greener, the goal is **reduce the cost and improve security**."*

The interviewee Int-04 (Strategy for Banking) said:

*In the US, I did not see much about **sustainability**. There are some legislation in the US and Canada that we might see the **influence of sustainability** on **cloud decisions**. I am hearing from my colleagues in **Europe** that this is a **big topic in Europe** because of the **regulatory environment** around **ESG**. It is regulatory requirement that the bank has to demonstrate that they met the resilience and availability requirements. Sometime, we see the banks use the public cloud as a backup solution. You must make sure of the cost of moving the data between the public cloud providers. You must factor that in as a part of your strategy."*

The interviewee Int-01 (Enterprise Architecture - Multi-cloud Integration) said:

*"There is something that I see with banks. That the **OpenBanking Concept** is coming. So, they are more open **to open up their own services to their partners**. These banks manage a lot of data. They are slowly opening up and a chance to **monetize** it. It is like **Banking-as-a-Service** that allow other organizations to use it. Personally, I did not experience it yet."*

8.2.3 Multi-Cloud Benefits for Financial Institutions

At the end of each interview, each interview was asked about the benefits their clients got from their multi-cloud environment. The benefits of multi-cloud for financial institutions that were identified in the interviews were very similar to the benefits that were identified from the literature at section 5.3. All the interviewees agreed on: choosing the best-of-breed of cloud services, agility, shorter time-to-market, and cost reduction.

The interviewee Int-02 (Technical Architecture) said:

*"Mainly the **agility** and **cost reduction**. Most of enterprises struggle with hardware. Traditionally, banks provisions servers on-premises takes weeks. On cloud, the provisioning is done within hours. There is a big improvement in **Time-to-Market**. And the **cost** is **reduced**. Also, the enablement of **OpenBanking** for **exchange of data**."*

The interview Int-03 (Technology Delivery) said:

*"They want to **reduce cost**, improve provisioning and **flexibility** to allow them to get **products quicker** to the **market**."*

The interview Int-12 (Technology Consulting for Banking) said:

*"The bank migrated to multi-cloud to get **cost savings**, **resilience**, operational improvement, and also **reduce time to market**."*

Conclusion of Chapter 8

This chapter analyzed the interviews with the experts. From the interviews the research identified the organizational challenges and the technical challenges that the financial institutions encounter before, during, and after migration to multi-cloud. The solutions for these challenges were identified. Regarding the environmental challenges, the interviewees agreed that in the past sustainability and ESG was not much important as of now. On the other hand, the interviewees found that the financial institutions are considering building ecosystems with their partners and suppliers in order to reach more customers and improve their services.

Chapter 9 First Version of Governance Framework

Introduction of Chapter 9

This chapter explains the process of building the first version of the multi-cloud governance framework for the financial institutions. The framework was built based on:

- Digital Transformation Framework - Section 4.3 (Warner and Wäger, 2019)
- Cloud Governance Structure - Section 6.3 (Prasad et al., 2014)
- Cloud Governance Lifecycle Model - Section 6.2 (Karkošková and Feuerlicht, 2017)
- Cloud Governance Model - Section 6.1.1 (Karkošková, 2018)
- The results of the expert interviews - Chapter 8

The Digital Transformation Framework (Warner and Wäger, 2019) was chosen, because:

- Cloud transformation is an example of digital transformation.
- The framework considers the digital transformation cycle from analyzing the adoption triggers to the digital sensing to the renewal of culture.
- Reference to chapter 4, most of the financial institutions are pre-digital organizations that had to become digital organizations due the disruptive digital technologies, the emergence of new competitors such as the FinTech, and the changing consumer behavior.

The Cloud Governance Structure (Prasad et al., 2014) was chosen, because:

- It investigated the cloud governance entities that organizations established in order to govern and manage the cloud, such as Chief Cloud Officer, Cloud Center of Competency.

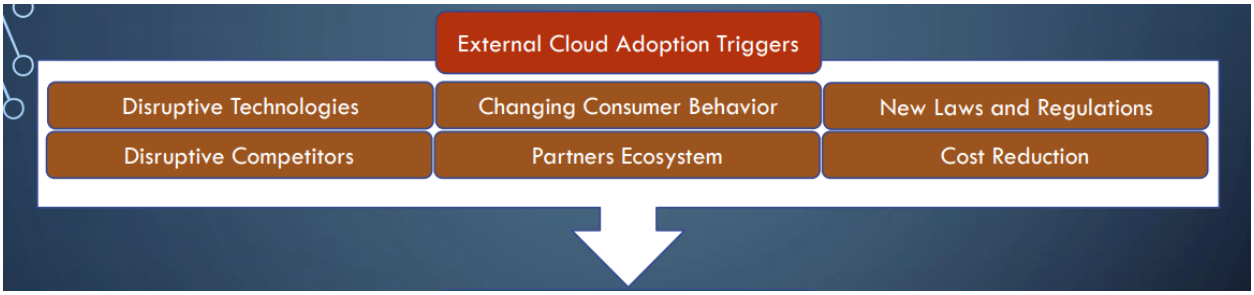
The Cloud Governance Lifecycle Model (Karkošková and Feuerlicht, 2017) was chosen, because:

- Their cloud governance lifecycle model provides guidance on the implementation and the continuous improvement of cloud governance activities.

The Cloud Governance Model (Karkošková, 2018) was chosen, because:

- It is based on the ITIL Framework.
- It considered the cloud governance and management activities starting from designing cloud adoption strategy to cloud transition tasks to cloud continuous improvement.

9.1 Starting Point Cloud Adoption External Trigger



Since cloud transformation is an example of digital transformation, the Warner and Wäger Digital Transformation Framework (section 4.3) was analyzed. The starting point of their digital transformation framework was considering the external triggers such as Disruptive Digital Technologies, Disruptive Digital Competitors, and Changing Consumer Behavior. Therefore, the researcher decided to start the framework by considering the cloud adoption external triggers because the triggers are the reasons that may force the financial institution to adopt multi-cloud. The cloud adoption triggers were identified in chapter 4.

9.2 Stage 1 Discover New Cloud Technologies

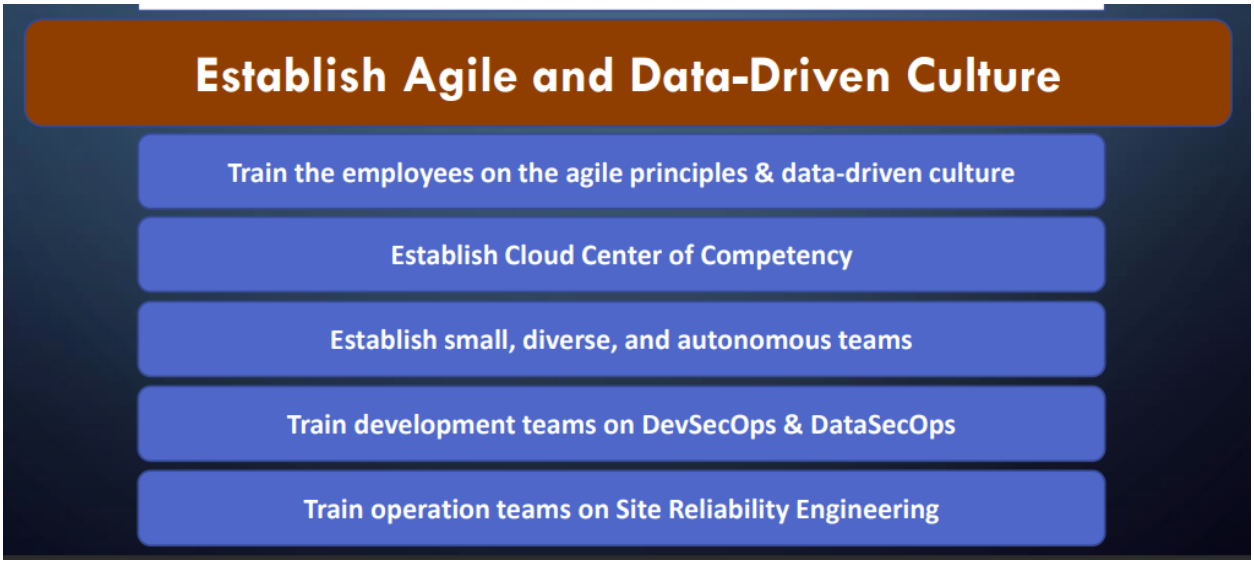
Reference to Warner and Wäger Digital Transformation Framework (section 4.3) and Karkošková Cloud Governance Framework (section 6.1.1), the first stage was to discover the cloud market and evaluate the cloud providers and their cloud services.

After evaluating the cloud providers and their cloud services and identifying the industry trends in the cloud market. The financial institution can create new use cases, new services, and then new business models.

9.3 Stage 2 Conduct Organizational & IT Maturity Assessment

Reference to the interviews analysis for the organization challenges (section 8.2) and the Digital Transformation within Financial Industry Model (section 4.2), it was concluded that the financial institutions were not originally structured as digital organizations. As a result, they usually need to re-organize in order to improve their hierarchical and conservative culture and their skill set. Therefore, they usually need to conduct organizational readiness assessment for their organizational structure and their skill set. And they need to conduct an IT maturity assessment for their current IT infrastructure. The purpose of these assessments is that they will be able to understand the as-is state, define the to-be state, and then build the strategy and plans that will take them to the to-be state.

9.4 Stage 3 Establish Agile and Data-Driven Culture



Reference to the benefits that the financial institutions want to get from cloud adoption (section 4.3), establishing an agile culture can allow the financial institution to reduce time-to-market and the data-driven culture can allow the financial institution to create more value from their data.

Reference to the interviews analysis (section 8.2) and the Prasad Cloud Governance Structure (section 6.3), establishing CCOC or CCOE is a strategic decision that will allow the financial institution to govern their cloud transformation and cloud management.

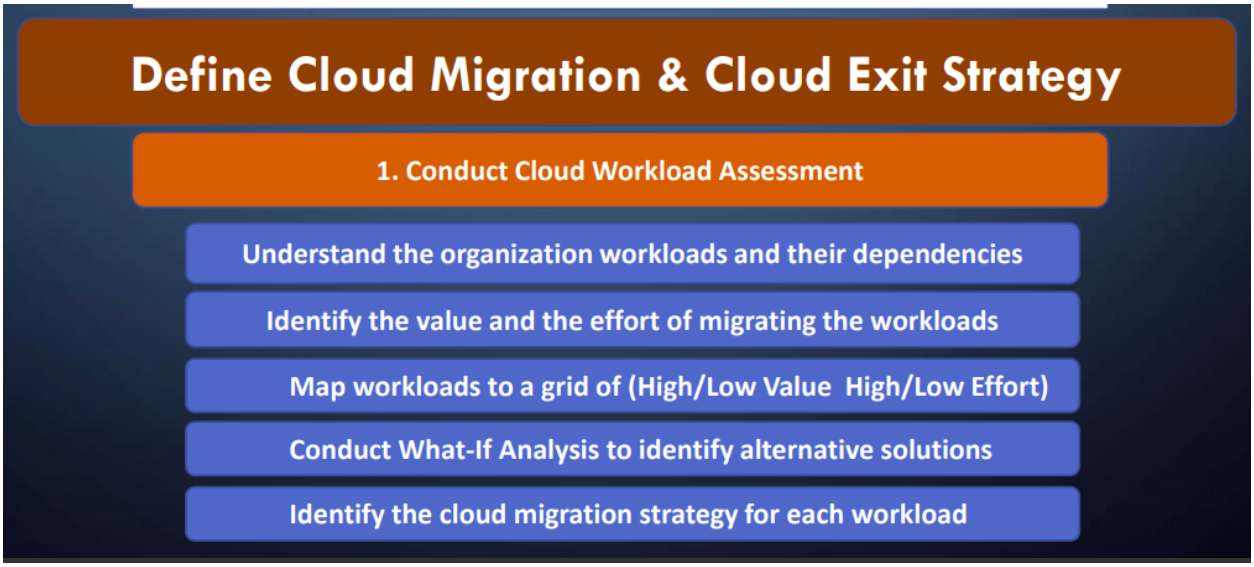
Reference to the interviews analysis, creating a production environment and non-production environment on the cloud is a great decision. Therefore, creating small diverse autonomous teams that can test different cloud solutions across the multi-cloud can maximize the potential benefits of their multi-cloud environment.

Since the financial institutions are security-driven organizations, the DevSecOps will allow them to build security-by-design applications, while the DataSecOps will allow them to build and automate security-by-design data governance systems. Finally, the site reliability engineering will allow them to automate as much as possible the cloud management operations across their multi-cloud environment.

9.5 Stage 4 Define Cloud Migration Strategy & Cloud Exit Strategy

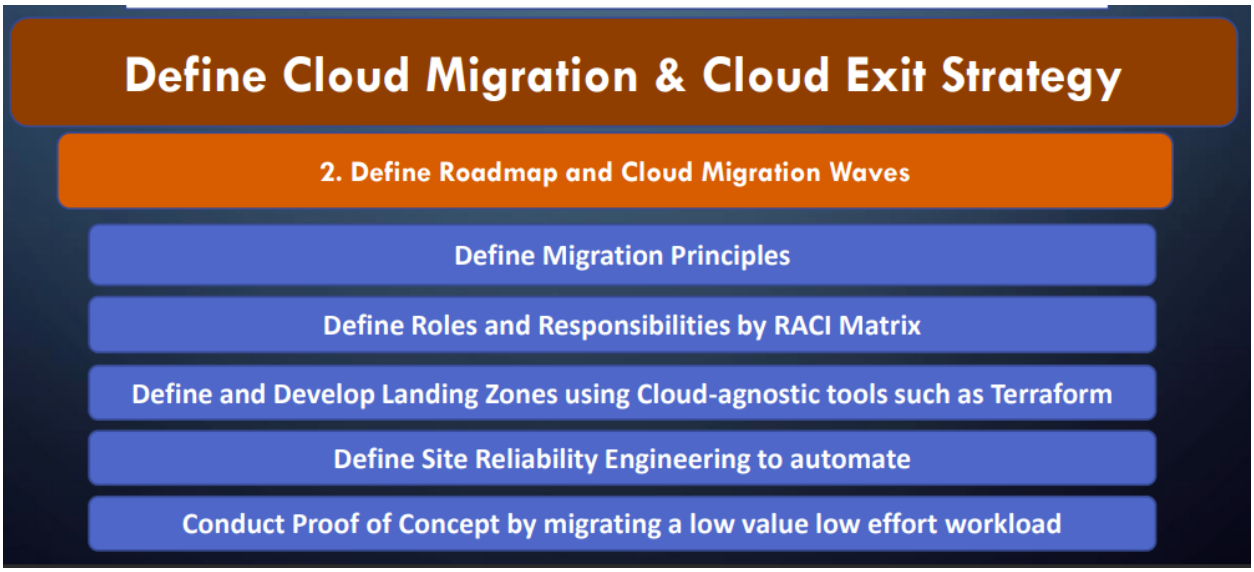
Reference to the interview analysis (chapter 8) and Karkošková Cloud Governance Model (section 6.1.1), defining the cloud migration strategy and the cloud exit strategy at the same time is very important in order to avoid vendor-lock in, improve cloud portability, and minimize the cost and the effort of cloud exit plans as much as possible. This stage has 7 sub-stages.

9.5.1 Sub-stage 1 Conduct Cloud Workload Assessment



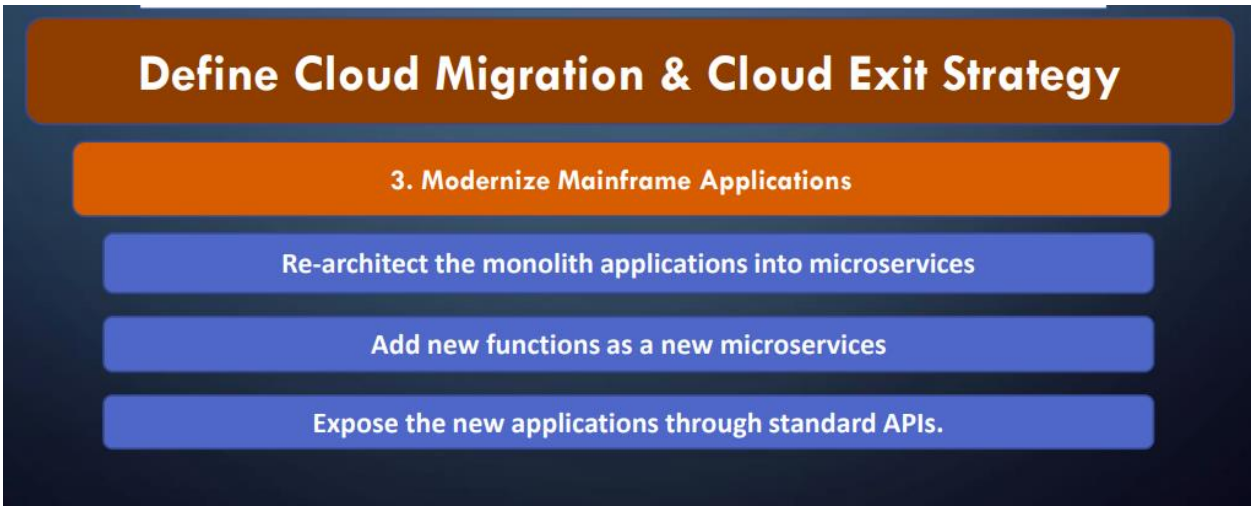
Reference to the interview analysis and the cloud migration strategies, it is recommended to conduct workload assessment in order to understand the workloads dependencies and the value and the effort of migrating each one. Then, conduct What-If analysis to identify all the possible migration strategies for each workload in order to evaluate the value and the cost of each migration strategy and then identify the optimal or the sustainable strategy.

9.5.2 Sub-stage 2 Define Cloud Migration Roadmap and Wave



Reference to Karkošková and Feuerlicht Cloud Governance Lifecycle model (section 6.2), during the Definition Phase, the organization should define the organization structure and assign roles and responsibilities and then develop cloud migration roadmap. Therefore, the researcher decided to include the task that may be needed to prepare for the migration and test it. Firstly, the financial institution should define the migration principles such as the type of encryption of data before the transfer. Then, assign the roles and responsibilities of the migration team. Then, develop the landing zones using cloud-agnostic tools in order to avoid vendor-lock in and improve the cloud portability. After that, develop the software codes of site reliability engineering in order to automate as much as possible of cloud operations. Finally, conduct proof of concept of low value low effort workloads to test the migration plan.

9.5.3 Sub-stage 3 Modernize Mainframe Applications



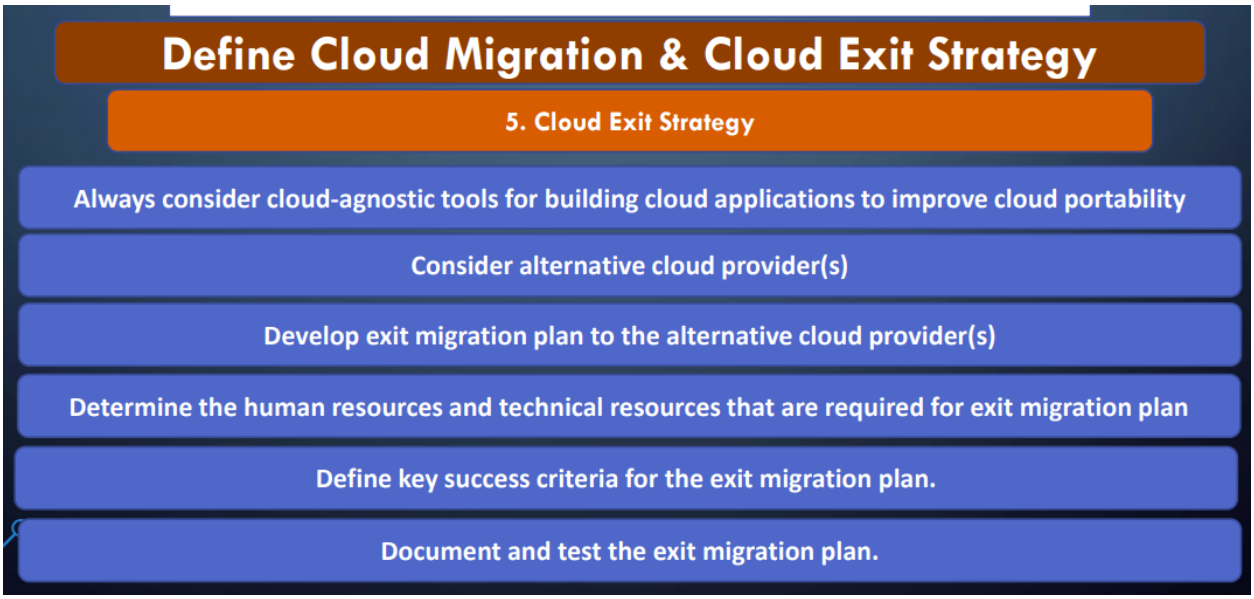
Reference to the technical challenges that were identified in the interviews (chapter 8), the mainframe limitations are sometimes a huge challenge for financial institutions because they are usually developed using very old programming languages that it is very expensive to migrate them to cloud. This step is a recommendation. It would be better to re-architect the mainframe application into microservices instead of a lift and shift approach. Then, add new functions as microservices. Finally, expose the applications through standard APIs so that they and the cloud applications from different cloud providers can integrate.

9.5.4 Sub-stage 4 Risk & Audit Management

Since the financial institutions are security-driven organizations and they are always under the audit from external auditors. They must be able to monitor and audit any risk in order to stay in compliance and prevent the occurrence of any incident. AWS Cloud Reference Architecture recommends the 3 Lines of Defense for Risk and Audit Management as the following:

1. The First Line of Defense: Operations Team
    a. Establish risk controls for each cloud provider.
    b. Monitor the day-to-day risk of each cloud provider.
2. The Second Line of Defense: Risk Management Team
    a. Monitor all the operations teams of the first line of defense.
    b. Anticipate the occurrence of any risk at a cloud provider that may cause an incident at another cloud provider. For example: When the components of an applications are segmented across different cloud providers.
3. The Third Line of Defense: Audit Teams
    a. Monitor the first line and the second line.
    b. Conduct audit for risk controls.
    c. Provider assurance to the board members, regulators, and external auditors about the effectiveness of risk management across multi-cloud environment.

9.5.5 Sub-stage 5 Cloud Exit Strategy



Reference to Karkošková Cloud Governance Framework (section 6.1.1), the organization needs to:

Cloud Provider Portfolio Management:

This process evaluates the cloud service providers available on the market.

Cloud Exit Strategy Management:

This process involves preparing plans for ending the contract with the cloud provider and migrate to on-premises datacenter, private cloud, or another public cloud.

Therefore, it is recommended to design the cloud exit strategy:

a. Consider at least one alternative cloud provider.

b. Prepare cloud exit plan for the alternative cloud provider.

c. Determine the required resources because it might be very expensive and time consuming. This point was mentioned clearly in an interview.

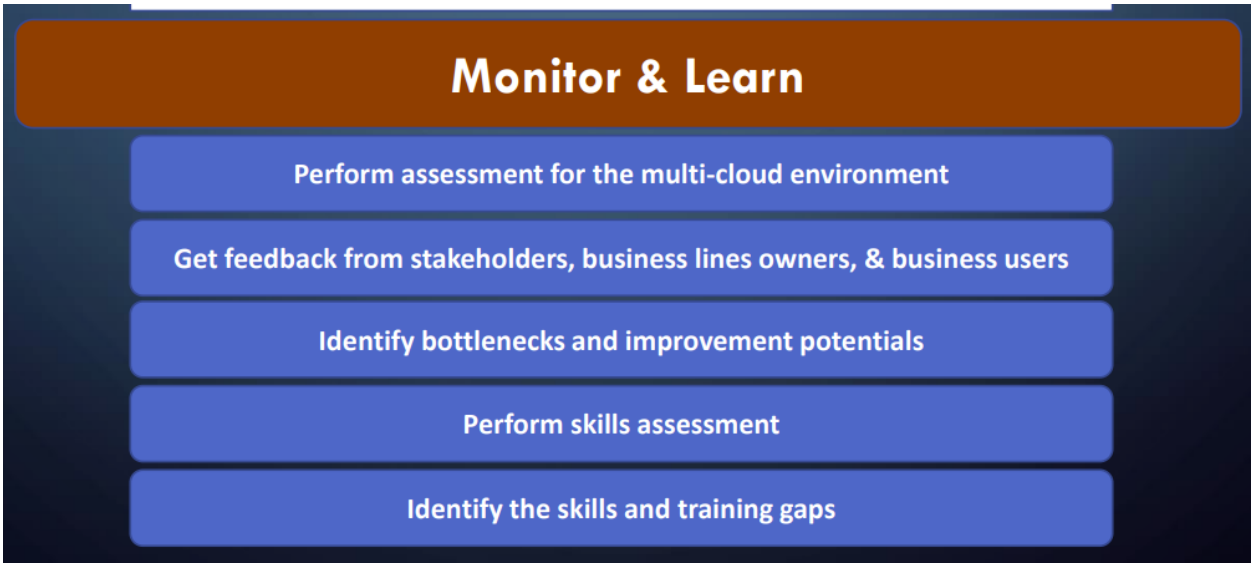
The interview Int-04 (Strategy for Banking) said:

"You must make sure of the cost of moving the data between the public cloud providers. You must factor that in as a part of your strategy."

d. Define key success criteria for the exit plan.

e. Document and test the exit plan.

9.6 Stage 5 Monitor & Learn



Reference to Karkošková Cloud Governance Framework (section 6.1.1), the organizations need to Cloud Continual Service Improvement:

> This phase ensures the continuous improvement of cloud services in terms of effectiveness, efficiency, acceptable level of risks, and cost-reduction. If the cloud consumer is not satisfied with cloud services, they can request change to cloud service or to SLAs.

Adding to his phase, from the interview analysis, the organizations also need to get feedback from the stakeholders and the business users and perform assessment for their skills in order to identify the bottlenecks and improvement potentials.

Chapter 10 Validation Interviews & Final Framework

Introduction of Chapter 10

This chapter presents the results of the validation interviews for the first version of the multi-cloud governance framework that was mentioned in Chapter 9, and it presents the final version of the framework based on their feedback.

10.1 Interview Overview

In order to validate the correctness of the first version of multi-cloud governance framework, 17 interviews were conducted. Firstly, 8 interviewees from the expert interviews phase were interviewed because they are already familiar with thesis research, and they will be able to identify whether the researcher managed to gather the right answers and build the correct framework or not. Then, 5 new interviewees from cloud consultancy were interviewed in order to get new answers and feedback. Finally, 4 new interviewees from cybersecurity from different cybersecurity domains were interviewed because from the analysis of the expert interviews, it was concluded that the security is the top challenge for financial institutions. Therefore, they were interviewed in order to get their feedback from a cybersecurity perspective. After each interview, the suggestions of the interviewee were implemented immediately before the next interview. After a few interviews, the correctness of the framework was improved to the point that the latter interviewees did not give more suggestions. The details of the interviewees are summarized in the following table.

ID	Region	Level	Title	Interviewed Before	Domain
Int-01	Netherlands	Manager	Technical Architect	Yes	Enterprise Architecture Technical Architecture Multi-cloud Integration
Int-02	Ireland	Senior Manager	Technical Architect	Yes	Technical Architecture Cloud Infrastructure
Int-03	UK & Ireland	Associate Director	Technology Delivery Lead	Yes	Technology Delivery
Int-04	USA & Canada	Managing Director	Technology Strategy	Yes	Strategy for Banking
Int-05	Netherlands	Senior Manager	Cloud Migration & Implementation	Yes	Cloud Consultancy
Int-06	Netherlands	Manager	Cloud Migration & Implementation	Yes	Cloud Consultancy
Int-07	UK	Senior Manager	Technology Consulting	Yes	Technology Consulting for Banking
Int-08	USA & Canada	Managing Director	Data & AI Value Strategy	Yes	Data and AI
Int-09	Netherlands	Leadership	Tech Consulting Executive Principal	**No**	Cloud Consultancy
Int-10	Netherlands	Senior Manager	Cloud Migration & Implementation	**No**	Cloud Consultancy
Int-11	Netherlands	Manager	Cloud Migration & Implementation	**No**	Cloud Consultancy

Int-12	Netherlands	Leadership	Senior Security Executive	**No**	Cybersecurity
Int-13	Netherlands	Senior Manager	Cybersecurity Senior Manager	**No**	Cybersecurity
Int-14	Netherlands	Manager	Security Delivery Manager	**No**	Identity and Access Management
Int-15	Netherlands	Specialist	Security Delivery Specialist	**No**	Cloud Security
Int-16	Netherlands	Senior Analyst	Cloud Migration & Implementation	**No**	Cloud Consultancy
Int-17	Netherlands	Analyst	Cloud Migration & Implementation	**No**	Cloud Consultancy

Table (14): Details of Validation Expert Interviewees

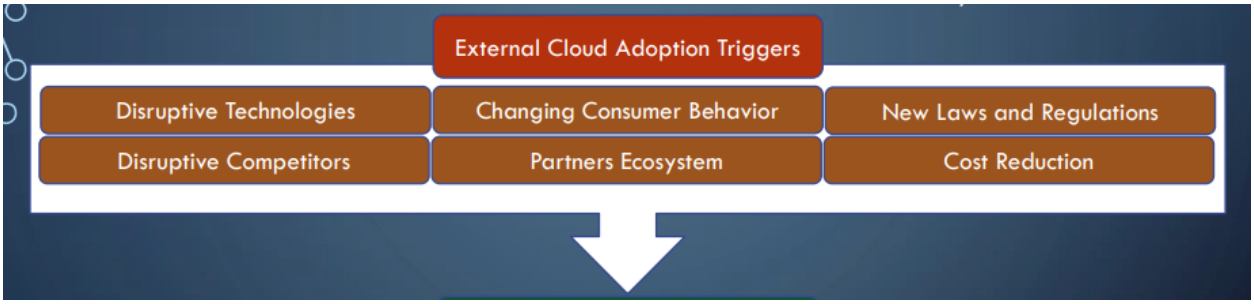
10.2 Validation Interviews Results & Final Framework

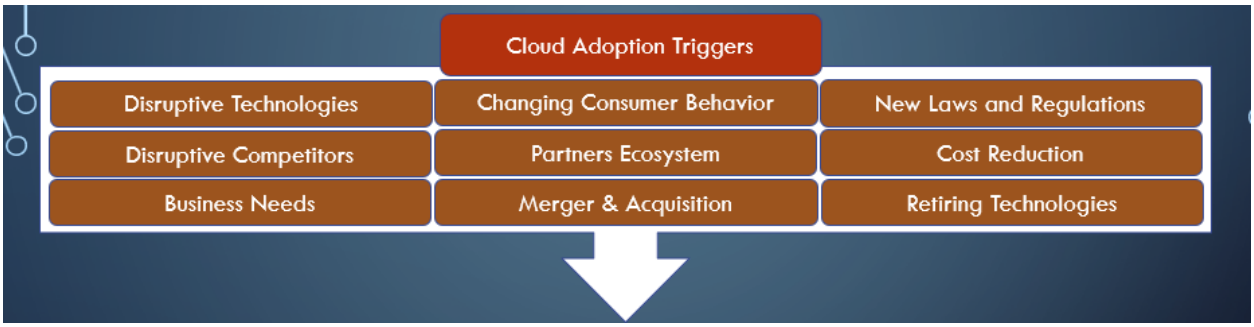
All the interviewees gave positive feedback for the framework. However, many of them said that the framework did not differentiate between single cloud and multi-cloud. In addition, the cybersecurity interviewees suggested security and risk suggestions. Their suggestions are summarized as the following.

The conclusion from the validation interviews:

1. Cloud Adoption Triggers

They found that the cloud adoption triggers focus on the external triggers only. They suggested the following internal triggers.



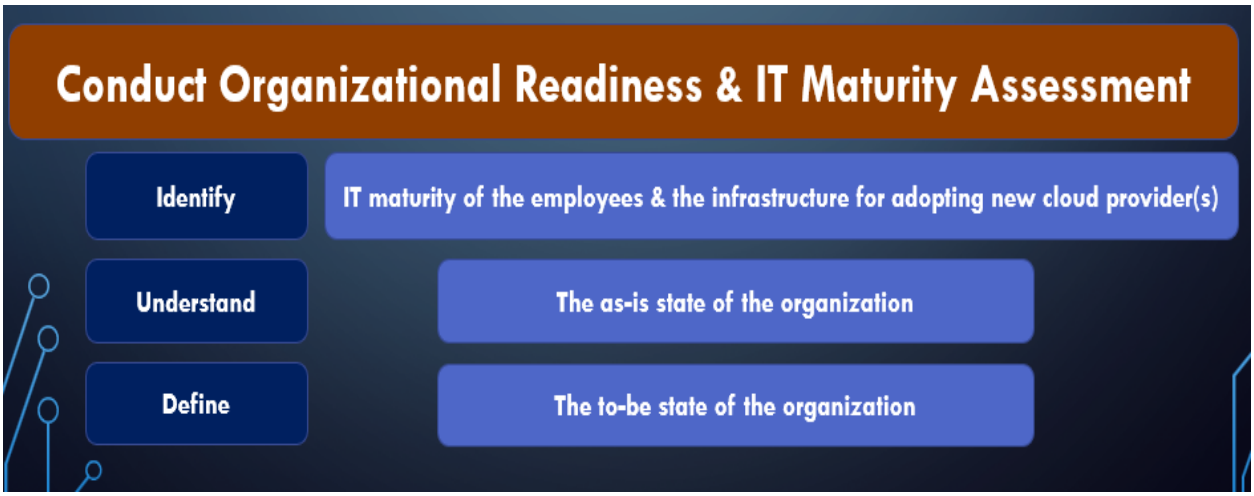


2. Discover New Cloud Capabilities:

They suggested identifying the business needs and the IT needs in addition to discovering new cloud capabilities.

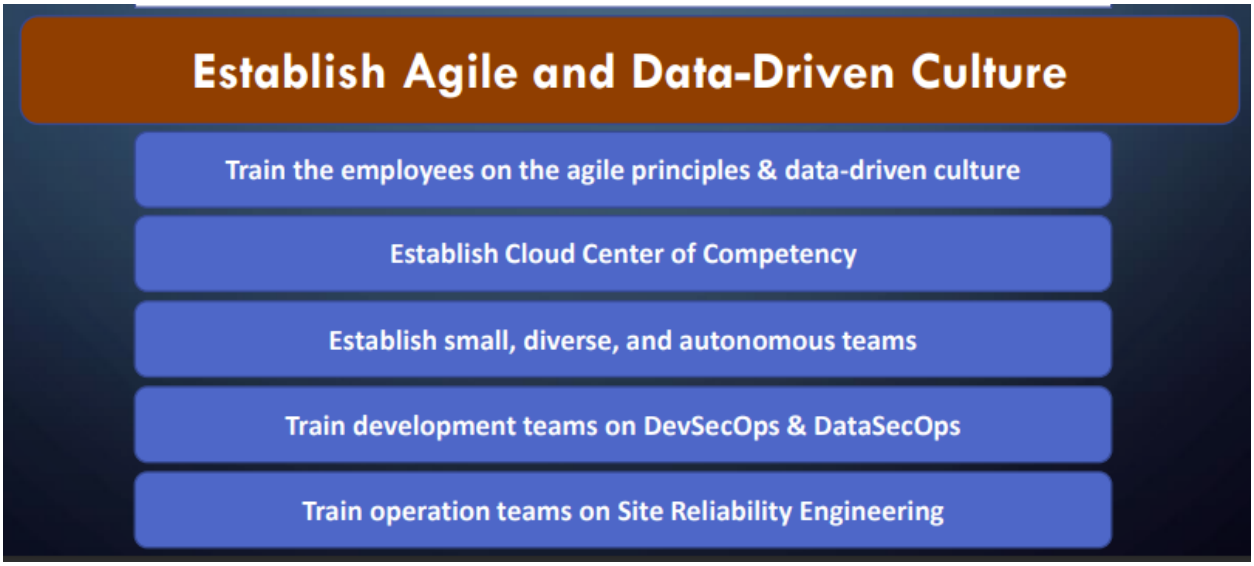
3. Conduct Organizational & IT Maturity Assessment

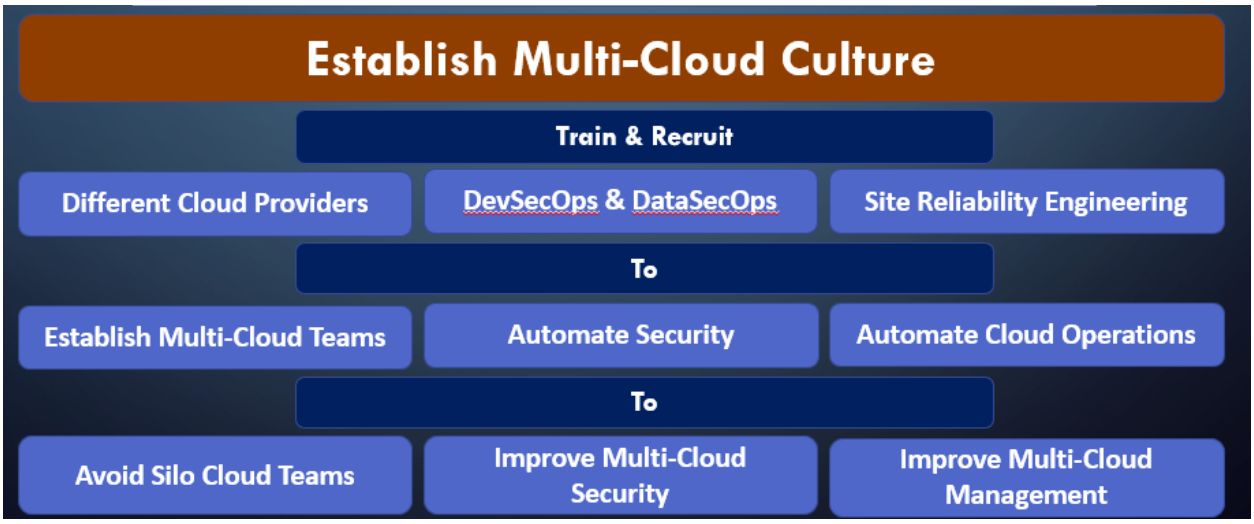
They agreed on this stage.



4. Establish Multi-Cloud Culture

Most of them found that establishing an agile and data-driven culture is not an accurate step because they believe that not all the financial institutions are agile and data-driven organizations. In addition, most of the financial institutions already have cloud culture. Therefore, they suggested Establishing Multi-Cloud Culture.





They defined the shortage of skills as the following:

a. Shortage of Multi-Cloud Skills instead of Cloud Skills

The financial institution needs people who are skilled in different cloud providers, so that they can identity the best-of-breed of cloud services at each cloud provider and avoid the vendor-lock in and avoid silo Cloud Teams.

b. Shortage of Multi-Cloud Security Skills.

The financial institution needs people who are skilled in developing cloud security controls that can standardize and automate security across their multi-cloud environment.

c. Shortage of Multi-Cloud Management Skills.

Since each public cloud provider has its own cloud management portal. The organizations usually use multi-cloud management solutions that can monitor and manage different cloud environments from a centralized portal. For example, each public cloud provider has its own Identity and Access management system. Therefore, maintaining consistency for each provider is a very complex task. As a result, organizations use a third-party cloud agnostic solution that can allow them to standardize and manage all the Identity and Access management systems from one portal.

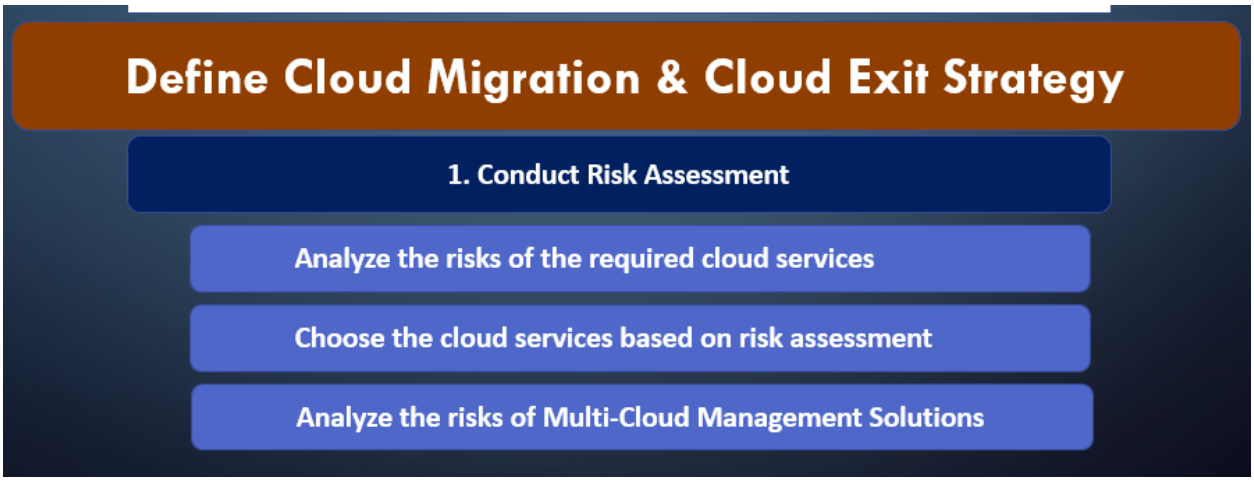
5. Conduct Risk Assessment

The cybersecurity interviewees said that the first step in defining cloud migration strategy and cloud exit strategy is to conduct risk assessment for cloud providers and the cloud services in order to identify the cloud services that can be used by the financial institution. Then, the financial institution should try to negotiate SLAs that can be aligned between cloud providers in order to avoid incidents. Finally, the financial institution conducts risk assessment for multi-cloud management solutions before adopting any of them. From this step, the financial institution can define their multi-cloud security strategy.

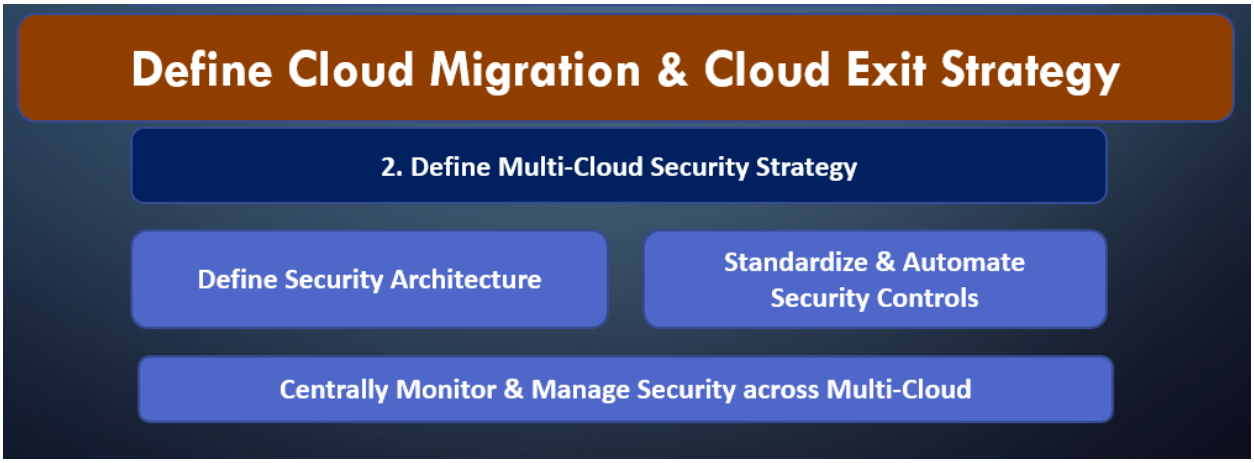
Their suggestions are also supported by Karkošková Cloud Governance Framework (section 6.1.1) at step:

Cloud Service Risk Management:

This process performs analysis of the potential risks of migrating to cloud.



6. Define Multi-Cloud Security Strategy



Reference to the interviewee Int-02 (Technical Architecture) from expert interview stage and validation interview stage, he said that after the financial institution had conducted the risk assessment, it must define their multi-cloud strategy in order to:

a. Define Security Architecture and its principles.

b. Standardize and Automate Security Controls across the multi-cloud environment.

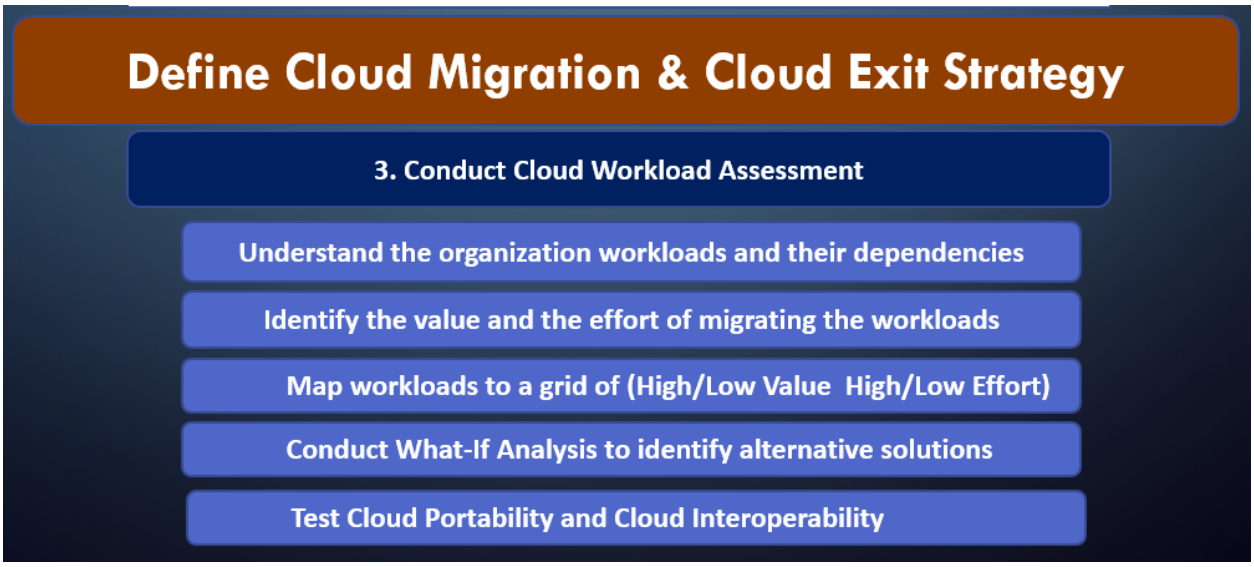
c. Centrally monitor & Manage Security across the multi-cloud environment.

The interviewee Int-02 from expert interview stage

*"The **security** was managed by **security principles**. There is **security architects** who **manage all security solutions**. They define **consistency** in se**curity controls across the cloud providers**. The goal is to apply to the cloud providers **similar controls** based on **security policies** defined in the bank across the vendors. The cloud vendors AWS and Azure both have to follow the **same security policies** of the bank. So, the bank get the **same security assurance and risk** across both cloud providers."*

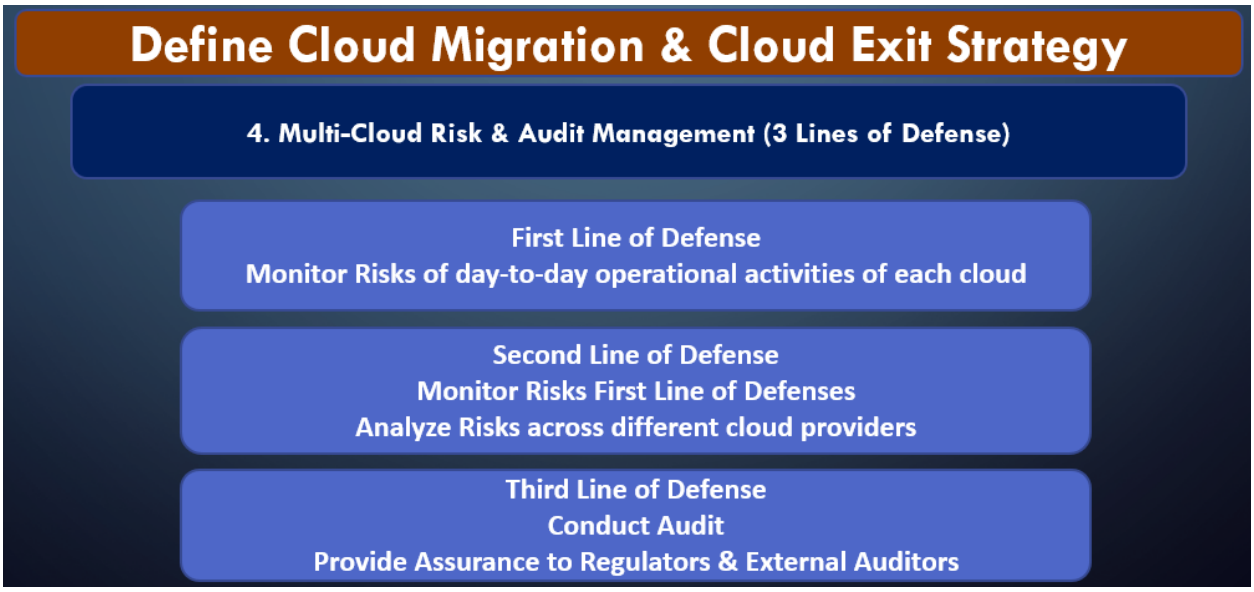
7. Conduct Cloud Workload Assessment

All the interviewees agreed on this step.



8. Multi-Cloud Risk & Audit Management (3 Lines of Defense)

The interviewees agreed on this step, and they suggested changing the title of the step from Risk & Audit management to Multi-Cloud Risk & Audit Management.

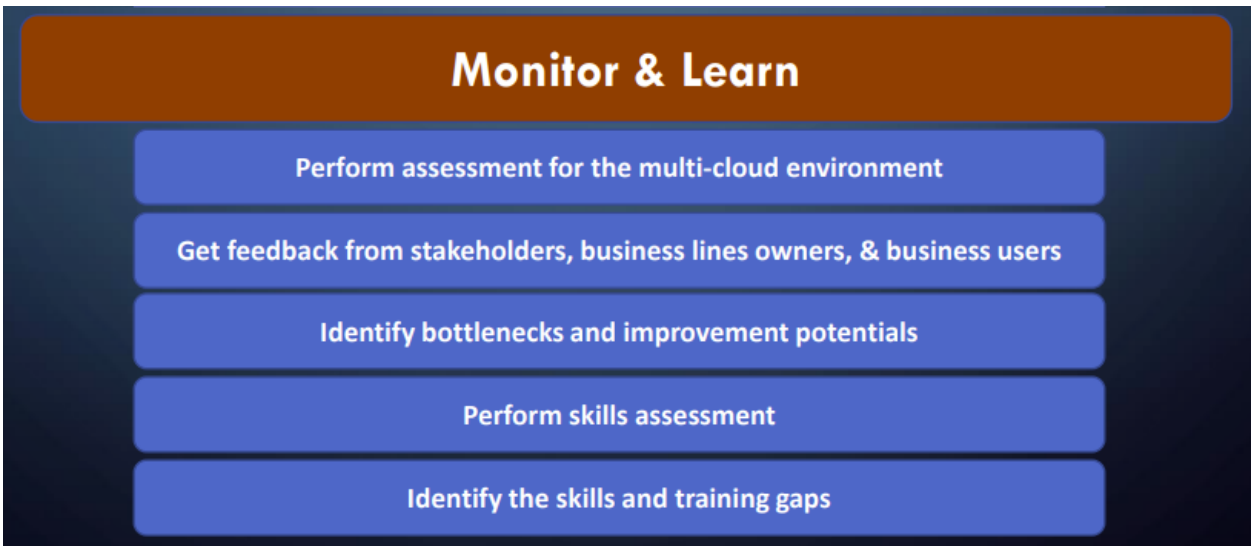


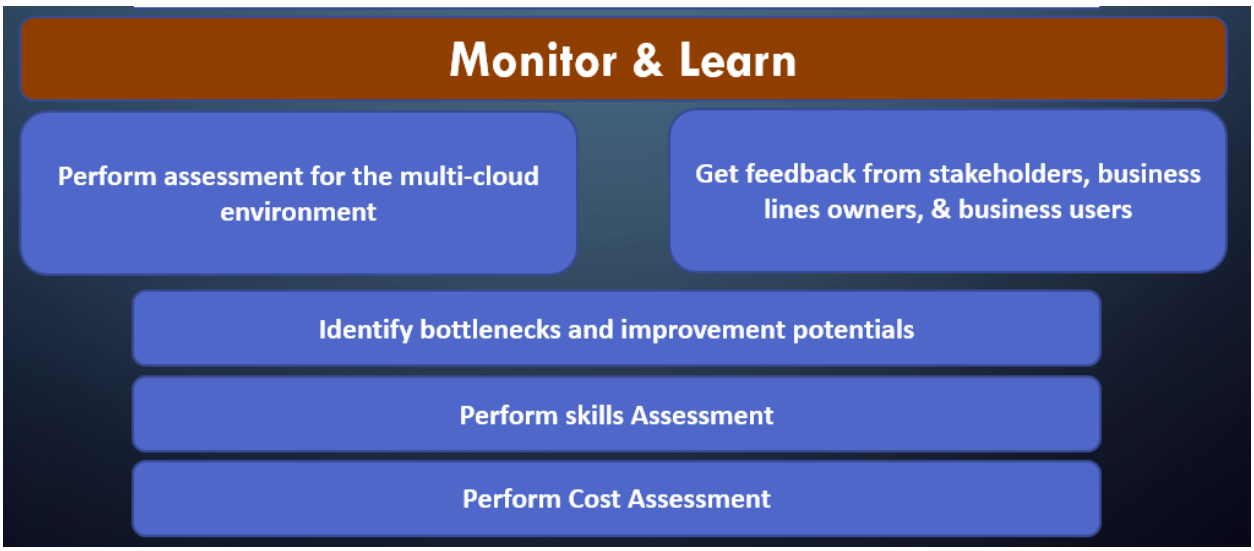
9. Monitor & Learn

All the cloud consultants said that adding Perform Cost Assessment is a very necessary step at this stage before repeating the cycle. There suggestion is also supported by Karkošková and Feuerlicht Cloud Governance Lifecycle (section 6.2) as the following:

Monitoring phase:

The activity of this phase involves collection data on cloud governance processes. Then, evaluating the cloud governance process in order to improve cloud governance in the next cycle.





Conclusion of Chapter 10

Seventeen validation interviews were conducted in order to validate the correctness of the first version of multi-cloud governance framework. The initial feedback of all the interviewees was positive. However, they noticed that the framework did not differentiate well between single and multi-cloud. Then, they provided their suggestions based on their area of expertise. The final version of the framework can be found in Appendix C.

11 Discussion

Introduction of Chapter 11

This chapter presents the discussion of this thesis research results. This chapter is structured by categorizing the results into four sections: Literature Review Results, Expert Interviews Results, Validation Interviews Results and Research Recommendations. Section 11.1 presents the results of the literature review. Sections 11.2 presents the results of experts interviews. Section 11.3 presents the results of validation interviews. Section 11.4 presents a list of recommendations that are concluded from the results of this research. Section 11.5 presents the research relevance. Section 11.6 presents the limitations of the research and suggestions for future research.

11.1 Literature Review Results

From the literature review, it was concluded that most of the financial institutions were originally paper-based organizations. Therefore, they were organized as pre-digital organizations. However, with the emergence of disruptive technologies such as cloud technologies, new disruptive competitors emerged such as FinTech organizations that were organized as digital organizations in order to offer digital financial services. On the other hand, the continuous increasing dependency on digital technology by the people, leads to changing consumer behavior. As a result, most pre-digital financial organizations had to adopt the digital transformation in order to cope with the digital economy. One of the most important digital innovations in the 21 century is cloud computing.

Since the 2000s, organizations across different industries started to adopt cloud computing due to its benefits such as auto-scale of resources and pay-per-usage model. However, many financial

institutions were late in adopting cloud computing due to many reasons such as security concerns from losing control on applications and data, and the complexity of migrating their mainframe core applications to cloud. Therefore, many financial institutions start to adopt a multi-cloud deployment that consists of their on-premises mainframe or their own private cloud with one or more public cloud providers. Unfortunately, some financial institutions encounter challenges such as the complexity of managing their multi-cloud environment and the shortage of cloud skills.

Finally, a literature review was conducted in order to identify and analyze the available cloud governance frameworks. It was found that the many researchers found that the commonly used IT governance frameworks such COBIT and ITIL are not well suited for cloud governance. Therefore, they worked on adapting it to cloud computing.

Therefore, from this point, it was important to conduct research in order to identify clearly the challenges that financial institutions encounter when they adopt and migrate to multi-cloud and the solutions that they took to solve those challenges in order to build a multi-cloud governance framework that can support the financial institutions in adopting and governing the migration to multi-cloud.

11.2 Expert Interviews Results

From the interviews with Accenture experts, it was concluded that many financial institutions are struggling in their journey to adopting multi-cloud. First, they had a lack of knowledge of cloud computing because they were pre-digital organizations. They struggled with changing their organizational culture due to shortage of cloud skills. Therefore, they had to consult cloud consultancy organizations in order to support them. They started by conducting organizational readiness and IT maturity assessment in order to identify their current as-state and define the to-be state, so that they understand and define how they will adopt more cloud

providers. It was found that some of them were in a vendor-lock in to their current cloud provider due to the usage of cloud-native tools for implementing their cloud infrastructure and applications. The reason for that was the lack of defining cloud exit strategy before migrating to a cloud provider. As a result, the cloud consultants recommend defining the cloud migration strategy and the cloud exit strategy at the same time in order to improve the portability of cloud applications between different cloud providers and avoid potential problems such as vendor-lock in and minizine the costs of the exit strategy as much as possible.

During defining the cloud migration strategy, some financial institutions struggled in analyzing their mainframe core applications and their dependencies, due to the shortage of employees who understand mainframe applications and cloud computing. As a result, many financial institutions are training their employees on mainframe skills and cloud skills. Most of the financial institutions established cloud governance entities such as CCOC. The CCOC defines with the stakeholders the cloud migration strategy and cloud exit strategy. The CCOC maintains communication with different cloud providers. The CCOC conducts risk assessment for different cloud providers and their cloud services in order to build a catalog of potential cloud providers and their cloud services that their business users can use. Finally, they define the security architecture of their multi-cloud environment.

After migrating to multi-cloud, it was found that some organizations struggled in managing their multi-cloud environment due to the complexity of managing multi-cloud computing such as the complexity of standardizing and automating security controls across different cloud providers.

From the results of the literature review and the results of the expert interviews, it was obvious that there is a clear need for building a multi-cloud governance framework that can support the financial institutions in adopting and governing the migration to multi-cloud.

11.3 Validation Interviews Results

From the results of literature review and the results of the expert interviews, the first version of the multi-cloud governance framework was built. The framework was validated by interviewing 17 cloud experts from different domains. At first, all the interviews gave positive feedback for the framework. However, most of them noticed that the framework did not differentiate well between single cloud computing and multi-cloud computing. After a few interviews, the correctness of the framework was improved to the point that the latter interviewees did not need to give more suggestions.

The final framework starts by considering the external and internal cloud adopting triggers. Then, the next stage is analyzing the triggers, discovering the current cloud capabilities and industry trends. Then, identifying the possible new use cases in order to build new services. The next stage starts by conducting organizational readiness and IT maturity assessment in order to understand the as-is state and define the to-be state. The next stage is establishing multi-cloud culture by training and recruiting employees for different cloud providers and establishing diverse multi-cloud teams in order to avoid silo cloud teams. Then, train them on DevSecOps and DataSecOps culture in order to establish the security-by-design culture. Finally, train them on site reliability engineering in order to automate the cloud operations and decrease the manual work and improve the multi-cloud management.

The next stage is the CCOC should conduct a risk assessment for the cloud providers and their services in order to identify the cloud providers and their cloud services that satisfy the required risk levels and can be integrated with their current cloud environment. Then, the CCOC should define the multi-cloud security strategy by defining the security architecture and standardizing and automating security controls in order centrally monitor and manage security across multi-cloud.

The next stage is conducting workload assessment in order to understand the workloads and their dependencies in order to define cloud migration waves and roadmap. The financial institutions need to take in consideration the portability and interoperability of cloud applications in order to avoid vendor-lock in and minimize the cost of cloud exit strategy.

The next stage is defining multi-cloud risk and audit management strategy using the 3 Lines of Defense. First, first lines of defenses must be established for each cloud provider to monitor the risks of that provider. Then, a second line of defense must be established for monitoring all the first lines and analyzing all the risks across their multi-cloud environment in order to avoid any incident. Finally, a third line of defense must be established to conduct an audit in order to provide assurance for the board members, the regulators and the external auditors about the effectiveness of their multi-cloud risk and audit management strategy.

Finally, the final stage is to monitor and learn by performing assessment for a multi-cloud environment in order to identify bottlenecks and improvement potentials. Then, getting feedback from stakeholders and business users. Finally, perform skills assessment and cost assessment in order to improve their next cloud training especially regarding the cloud cost awareness.

11.4 Research Recommendations

This section presents a list of recommendations that was concluded from the results of this research. These recommendations should be considered by the financial institutions in order to improve their adoption of multi-cloud:

- Analyzing the cloud market for new cloud technologies and industry trends.
- Conducting cloud skill assessment for the current employees.
    - Cloud cost awareness
    - Multi-cloud engineering skills.
    - Multi-cloud management skills.
    - Mainframe skills.
- Define the cloud migration Strategy and cloud exit strategy at the same time.
- Standardize and automate cloud controls across the multi-cloud environment.
- Avoid using cloud-native tools and use cloud-agnostic tools in order to avoid being in vendor-lock state and improve the portability and interoperability of cloud applications across the different cloud providers.

11.5 Research Relevance

This section presents the relevance of this research for academia and industry.

11.5.1 Academic Relevance

In chapter 1, it was identified that the financial institutions still struggle with adopting multi-cloud. And in chapter 6, it was identified that the current available IT governance frameworks do not suit cloud governance. Therefore, this research filled this gap in knowledge by building a multi-cloud governance that will support the financial institutions in adopting and governing the migration to multi-cloud.

11.5.2 Industry Relevance

This research is useful for financial institutions and cloud consultancy organizations because it will allow them to consider a list of possible challenges that the financial institutions usually encounter when they migrate to multi-cloud, and the solutions that they took to solve these challenges. It also provides them with a framework with clear stages and steps that can support them in adopting and governing the migration to multi-cloud. Finally, it provides them with a list of recommendations that will allow them to improve their cloud migration strategy and cloud exit strategy.

11.6 Research Limitation and Future Research

First of all, due to the internship contract limitation, it was not allowed to interview any clients. Therefore, the experts from the hosting company were interviewed. All the interviewees spoke from their positions as cloud consultants. Second, the multi-cloud governance framework is evaluated from experts from the same company based on their area of expertise. Third, all the interviewees work in Europe Union and America, so the results are specific for these two regions. It cannot be generalized to the rest of the world because each country or a region has different laws, regulations, and culture that may lead to different cloud adoption drivers and challenges.

Reference to these limitations, the researcher suggests for future research that the same research should be conducted again by interviewing the financial institutions directly. The new researchers should interview employees from CCOC or CCOE, cloud architects, security architects, business owners, and business users from the financial institutions in order to get a different perspective. Then, the results of the new research should be compared with this research in order to identify the differences between the perspective of the financial institutions as cloud consumers and the perspective of the cloud consulting organizations as cloud consultants. After that, improving the framework of this research by adding the findings of the financial institutions. Finally, test the framework with the financial institutions and the cloud consultants in order to test its correctness, usability, and usefulness. The last suggestion is to conduct the research for other countries or regions such as Asia, Africa, and South America in order to compare the results and identify their cloud adoption drivers and challenges and how they solved their challenges.

Chapter 12 Conclusion

Introduction of Chapter 12

This chapter presents the research conclusion and my personal reflections of the research. Section 12.1 presents the conclusion of the research by answering the research questions. Section 12.2 presents my personal reflections regarding the research.

12.1 Research Conclusion

This thesis research investigated the challenges that the financial institutions encounter before, during, and after migration to multi-cloud in order to develop a holistic governance framework that will support them in adopting and governing the migration to multi-cloud. Therefore, the main research question was defined as the following:

The Main Research Question

How can a financial institution govern the challenges of migrating to a multi-cloud environment?

In order to answer the main research question, the following sub-research questions were defined.

Sub-Research Question 1 (SRQ1)

What is cloud computing?

The literature review for cloud computing was conducted in order to build the base foundation of the research. This sub-research question was answered by conducting literature

review for academic papers and industry papers. It was concluded that cloud computing is not a standalone computing technology, but it was the result of integrating and leveraging other technologies such virtualization, cluster computing, and grid computing. In addition, IT outsourcing is also part of cloud computing because the cloud consumer outsources IT infrastructure to cloud providers. There are many strategies to migrate applications to cloud such as rehost, replatform, and rearchitect. Each migration strategy has its own value and effort. Adding to that, not all the strategies are applicable to all applications because sometimes there are applications that are tightly coupled to the hardware, so it is impossible or extremely expensive to rehost or replatform it to a cloud environment. This question was answered in chapter 3.

Sub-Research Question 2 (SRQ2)

What are the cloud adoption divers and cloud adoption barriers of financial institutions?

This question was answered by conducting literature review. Firstly, the history of the financial institutions with the usage of technology was investigated. It was obvious that most of the financial institutions used to be paper-based working organizations. Therefore, their organizational structures, cultures and business processes were originally defined for the paper-based work. This means they were pre-digital organizations. However, the continuous evolution of IT created new disruptive technologies that allowed for the emergence of new disruptive competitors such as the FinTech that are digital organizations that offer digital services to their customers. On the other hand, as the people and organizations are becoming more dependent on IT from their daily lives and daily businesses, this dependency on IT is changing their behavior toward using online services and mobile services. As a result, the financial institutions are in continuous competition for creating new digital services. Therefore, digital transformation has become a critical key concern for pre-digital organizations because the digital transformation impacts the inner aspects of an organization such as the products, services, processes, and organizational structure and the outer aspects of the organization such as their customer behavior, partners, and suppliers. The digital transformation within the financial industry was

investigated because cloud transformation is also an example of digital transformation, so that an abroad view of digital transformation was obtained before diving into cloud transformation. It was found that the financial institutions always need to identify and analyze all the factors that influence their digital transformation in order to improve their digital transformation strategy and hence their cloud transformation by considering the following factors: Political or Regulation Factors, Economical Factors, Technological Factors, Changing Behavior of Consumers, Suppliers, and Partners, and the emergence of competitors and substitutes. Historically, the financial institutions used to build and manage their own mainframes in order to have full control over the applications and data. Since the early 2000s, cloud computing allowed new players such as neo-banks and fintech institutions to compete with the traditional financial institutions and gain market share by developing new innovative solutions. As a result, this led to changing the behavior of the consumers which is one of the factors of digital transformation. Consequently, the traditional financial institutions decided to adopt cloud computing. The most important cloud adoption drivers are agility, shorter time to market and strengthening business continuity and disaster recovery. On the other hand, the cloud adoption barriers are security, compliance, privacy risks, and shortage of cloud and mainframe skills, and the limitation of their mainframes and their core application. This question was answered in detail in chapter 5.

Sub-Research Question 3 (SRQ3)

What are the available cloud governance and management frameworks?

The literature review was conducted in order to find and analyze the commonly used cloud governance and management framework in order to identify the requirements of the multi-cloud governance framework. The research investigated two of the most common IT governance frameworks ITIL framework and COBIT framework, and the lifecycle of cloud governance and the organizational structures within cloud governance. It was concluded that in order to govern the cloud environment. The financial institutions need to establish an entity that is usually called Cloud Center of Competency (CCOC) or Excellence (CCOE). The CCOC or CCOE is a cloud governance entity that is responsible for analyze any cloud adoption triggers within the organization or outside the organization, analyze any business needs, analyze the cloud market

for the available cloud capabilities and industry trends, identify the best of breed cloud services at different cloud providers and provide cloud guidance for the organization. The financial institution also needs to establish a cloud migration team that will be responsible for any cloud migration by evaluating the workloads and their dependencies, identify the best possible migration strategies for each workload and execute the migration. Then, the financial institutions should define cloud adoption and migration strategy. Firstly, they need to evaluate the cloud providers and their cloud services. Secondly, they need to perform risk analysis for their cloud services. Thirdly, they need to evaluate the regulatory requirements of cloud services. Fourthly, they need to define a cloud exit strategy before migrating to the selected cloud provider in order to minimize the cost and the effort of the cloud exit plan.

Sub-Research Question 4 (SRQ4)

What are the challenges that a financial institution encounters before, during, and after the migration to a multi-cloud environment?

Some of the challenges were identified from the literature review. Then, the interviews with the experts were conducted. The challenges were categorized under two categories: Organizational Challenges, and Technical Challenges. The organizational challenges are Shortage of Cloud Engineering Skills, Shortage of Mainframe engineering skills, Shortage of DevOps skills, and Shortage of Multi-Cloud Skills. The rest of the organizational challenges are Security Concerns from Public Cloud, Complexity of the re-organization and Complexity of defining Cloud Adoption and Migration Strategy. The technical challenges are Vendor-lock in due to the usage of Cloud Native Tools, Complexity of Applications Dependency, and Limitation of Mainframe Applications.

Sub-Research Question 5 (SRQ5)

What are the governance strategies that a financial institution can use for governing the challenges of migrating to a multi-cloud environment?

The governance strategies were identified from the same interviews with the experts. The solutions for the organizational challenges that were identified in the previous question are Conducting organizational readiness assessment, Establishing CCOC or CCOE, and Defining the cloud migration strategy and the cloud exit strategy at the same time. The solutions for the technical challenges are using Cloud Agnostic Tools, training the IT employees to fully understand the application dependencies, Modernizing Mainframe Applications, and Standardizing and Automating Security Controls.

Sub-Research Question 6 (SRQ6)

What are the requirements of a holistic strategic framework for governing the challenges of migrating to a multi-cloud environment for financial institutions?

The framework starts with analyzing any external and internal cloud adopting triggers. Then, the next stage is discovering the new cloud technologies, identifying the business needs and the IT needs in order to create new use cases and business models. Then, the next stage is conducting organizational and IT maturity assessment in order to identify the as-is state and define the to-be state. Then, the next stage is establishing a multi-cloud culture by training and recruiting employees for multi-cloud skills. Then, defining the cloud migration strategy and the cloud exit strategy by firstly conducting risk assessment for the cloud providers and the cloud services in order to identify the cloud services that can be used. Then, define multi-cloud security strategy in order to standardize and automate security controls across multi-cloud and centrally monitor and manage security across multi-cloud. Then, conducting cloud workload assessment in order to analyze the workloads and their dependencies, identify the cloud migration strategies for each workload, and test the chosen cloud migration strategies for portability and interoperability in order to avoid vendor-lock in. After that, define multi-cloud risk and audit

management using 3 lines of defense strategy. Finally, get feedback from the stakeholders, perform assessment for multi-cloud and costs and identify bottlenecks and improvement potentials.

12.2 Personal Reflection

This thesis research allowed me to achieve my goal which is improving my knowledge in cloud consultancy as the following. It allowed me to understand in-depth cloud computing and cloud migration strategies. It allowed me to understand cloud computing challenges and solutions within one of the heaviest regulated industries which is financial institutions. It allowed me to understand and analyze IT governance frameworks such as COBIT and ITIL framework and how to build new frameworks from other frameworks. The internship improved my professional network by allowing me to get to know cloud experts from different domains from different countries.

Looking back at the thesis as a whole. I am proud of this thesis because it allowed me to use all the knowledge and skills that I have learnt from my bachelor study, my master study, and my career experience. I believe it is the best way to finish my master study.

References

Abbott, M. (2021). *Challenges and opportunities in banks' cloud migration*. Accenture. https://bankingblog.accenture.com/challenges-opportunities-banks-cloud-migration

Abbott, M. (2022). *Banking Cloud Altimeter Volume 4 | Mainframe Migration | Accenture*. Accenture. https://bankingblog.accenture.com/banking-cloud-altimeter-magazine/volume-4-bank-cloud-mainframe-migration

Abubakar, A. A., & Tasmin, R. (2012). The Impact of Information and Communication Technology on Banks' Performance and Customer Service Delivery in the Banking Industry. *The International Journal of Latest Trends in Finance and Economic Sciences*, *2*(1). https://doi.org/10.2047/ijltfesvol2iss1

Accenture. (2021). *Cloud imperative for banking*. https://www.accenture.com/_acnmedia/PDF-144/Accenture-Cloud-Imperative-for-Banking-Growth-Markets.pdf

Accenture. (2022). *Have some banks taken off into the cloud without a flight plan?* Accenture Banking in Cloud. https://www.accenture.com/content/dam/accenture/final/industry/banking/document/Accenture-Banking-Cloud-Altimeter-Volume-6.pdf

Accenture Cloud Migration Strategies. (2021). Accenture. https://www.accenture.com/_acnmedia/PDF-145/Accenture-Maximizing-Value-from-Migrating-your-Enterprise-to-Cloud.pdf

Adamuthe, A. C., & Thampi, G. T. (2019). Technology forecasting: A case study of computational technologies. *Technological Forecasting and Social Change*, *143*, 181–189. https://doi.org/10.1016/j.techfore.2019.03.002

Ahn, B., & Ahn, H. (2020). Factors Affecting Intention to Adopt Cloud-Based ERP from a Comprehensive Approach. *Sustainability*, *12*(16), 6426. https://doi.org/10.3390/su12166426

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting Information Security and IT Governance Under COBIT 5 Framework: A Case Study. *Webology*, *18*(Special Issue 02), 294–310. https://doi.org/10.14704/web/v18si02/web18073

Alhomdy, S., Thabit, F., Abdulrazzak, F. H., Haldorai, A., & Jagtap, S. (2021). The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications. *International Journal of Intelligent Networks*, *2*, 166–174. https://doi.org/10.1016/j.ijin.2021.08.001

Ali, O., Shrestha, A., Osmanaj, V., & Muhammed, S. (2020). Cloud computing technology adoption: an evaluation of key factors in local governments. *Information Technology &Amp; People*, *34*(2), 666–703. https://doi.org/10.1108/itp-03-2019-0119

Alkhalil, A., Sahandi, R., & John, D. (2017). An exploration of the determinants for decision to migrate existing resources to cloud computing using an integrated TOE-DOI model. *Journal of Cloud Computing*, *6*(1). https://doi.org/10.1186/s13677-016-0072-x

Al-Mamary, Y. H. S., Abdulrab, M., Alwaheeb, M. A., Shamsuddin, A., & Jazim, F. (2020). The impact of technological capability on manufacturing companies: A review. *Journal of Public Affairs*, *22*(1). https://doi.org/10.1002/pa.2310

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England. *Journal of Enterprise Information Management*, *26*(3), 250–275. https://doi.org/10.1108/17410391311325225

Alt, R., Beck, R., & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electronic Markets*, *28*(3), 235–243. https://doi.org/10.1007/s12525-018-0310-9

Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of Business Research*, *136*, 602–611. https://doi.org/10.1016/j.jbusres.2021.08.011

Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2012). How to adapt applications for the Cloud environment. *Computing*, *95*(6), 493–535. https://doi.org/10.1007/s00607-012-0248-2

Avram, M. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. https://doi.org/10.1016/j.protcy.2013.12.525

Bharadwaj, A., Sawy, O. a. E., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *Management Information Systems Quarterly*, *37*(2), 471–482. https://doi.org/10.25300/misq/2013/37:2.3

Böhm, M., Leimeister, S., Riedl, C., & Krcmar, H. (2011). Cloud Computing – Outsourcing 2.0 or a new Business Model for IT Provisioning? *Application Management*, 31–56. https://doi.org/10.1007/978-3-8349-6492-2_2

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bughin, J., Catlin, T., Hirt, M., & Willmott, P. (2018). Why digital strategies fail. *McKinsey Quarterly*.

Byrd, T. A., & Turner, D. E. (2000). Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct. *Journal of Management Information Systems*, *17*(1), 167–208. https://doi.org/10.1080/07421222.2000.11045632

Chang, B. Y., Hai, P. H., Seo, D. W., Lee, J. H., & Yoon, S. H. (2013). The determinant of adoption in cloud computing in Vietnam. *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*. https://doi.org/10.1109/commantel.2013.6482429

Chatterjee, S., Rana, N. P., Dwivedi, Y. K., & Baabdullah, A. M. (2021). Understanding AI adoption in manufacturing and production firms using an integrated TAM-TOE model. *Technological Forecasting and Social Change*, *170*, 120880. https://doi.org/10.1016/j.techfore.2021.120880

Chauhan, M. A., & Babar, M. A. (2012). Towards Process Support for Migrating Applications to Cloud Computing. *2012 International Conference on Cloud and Service Computing*. https://doi.org/10.1109/csc.2012.20

Cheng, M., Qu, Y., Jiang, C., & Zhao, C. (2022). Is cloud computing the digital solution to the future of banking? *Journal of Financial Stability*, *63*, 101073. https://doi.org/10.1016/j.jfs.2022.101073

Christiansen, V., Haddara, M., & Langseth, M. (2022). Factors Affecting Cloud ERP Adoption Decisions in Organizations. *Procedia Computer Science*, *196*, 255–262. https://doi.org/10.1016/j.procs.2021.12.012

Dash, S., & Pani, S. K. (2016). E-Governance Paradigm Using Cloud Infrastructure: Benefits and Challenges. *Procedia Computer Science*, *85*, 843–855. https://doi.org/10.1016/j.procs.2016.05.274

De Haes, S., Huygh, T., Joshi, A., & Van Grembergen, W. (2016). Adoption and Impact of IT Governance and Management Practices. *International Journal of IT/Business Alignment and Governance*, *7*(1), 50–72. https://doi.org/10.4018/ijitbag.2016010104

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, *27*(1), 307–324. https://doi.org/10.2308/isys-50422

Dhar, S., & Balakrishnan, B. (2006). Risks, Benefits, and Challenges in Global IT Outsourcing. *Journal of Global Information Management*, *14*(3), 59–89. https://doi.org/10.4018/jgim.2006070104

Diener, F., & Špaček, M. (2021). Digital Transformation in Banking: A Managerial Perspective on Barriers to Change. *Sustainability*, *13*(4), 2032. https://doi.org/10.3390/su13042032

Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: Yesterday, Today, and Tomorrow. *Present and Ulterior Software Engineering*, 195–216. https://doi.org/10.1007/978-3-319-67425-4_12

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84. https://doi.org/10.1016/j.jss.2016.04.061

ENISA. (2014). *Secure Use of Cloud Computing in the Finance Sector*. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/cloud-in-finance

Fachrunnisa, O., Adhiatma, A., Lukman, N., & Ab Majid, M. N. (2020). Towards SMEs' digital transformation: The role of agile leadership and strategic flexibility. *Journal of Small Business Strategy*.

Fain, J. (2022). *Reading, Understanding, and Applying Nursing Research (Fain, Reading, Understanding and Applying Nursing Research) 3th (third) edition*.

Feuerlicht, G. (2010). Next Generation SOA: Can SOA Survive Cloud Computing? *Advances in Soft Computing*, 19–29. https://doi.org/10.1007/978-3-642-10687-3_2

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*.

Furht, B. (2010). Cloud computing fundamentals. *In Handbook of Cloud Computing*.

Fuzes, P. (2018). How Does Cloud Computing Change the Strategic Alignment Between Business and IT. *In Conference on Digital Information Processing*.

Gale, N., Heath, G., Cameron, E., Rashid, S. F., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, *13*(1). https://doi.org/10.1186/1471-2288-13-117

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, *28*(1), 107–130. https://doi.org/10.1108/jeim-08-2013-0065

Gartner. (2020, November 19). *Gartner Says Audit Chiefs Identify IT Governance as Top Risk for 2021*. https://www.gartner.com/en/newsroom/press-releases/2020-11-19-gartner-says-audit-chiefs-identify-it-governance-as-top-risk-for-2021

Gartner. (2021). *Core Banking Hot Spot: Use Cases for Moving to the Cloud*. https://www.gartner.com/en/documents/4008180

Gholami, M. F., Daneshgar, F., Low, G., & Beydoun, G. (2016). Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software*, *120*, 31–69. https://doi.org/10.1016/j.jss.2016.06.068

Ghule, S., Chikhale, R., & Parmar, K. (2018). Cloud Computing In Banking Services. *Journal of Emerging Technologies and Innovative Research*, *5*(11), 139–141.

Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher*, *21*(6), 34–38. https://doi.org/10.7748/nr.21.6.34.e1252

Grozev, N., & Buyya, R. (2014). Multi-Cloud Provisioning and Load Distribution for Three-Tier Applications. *ACM Transactions on Autonomous and Adaptive Systems*, *9*(3), 1–21. https://doi.org/10.1145/2662112

Hiran, K. K., & Henten, A. (2019). An integrated TOE–DoI framework for cloud computing adoption in the higher education sector: case study of Sub-Saharan Africa, Ethiopia. *International Journal of System Assurance Engineering and Management*, *11*(2), 441–449. https://doi.org/10.1007/s13198-019-00872-z

Hogan, M. D., Liu, F., Sokol, A. W., & Jin, T. (2011). NIST-SP 500-291, NIST Cloud Computing Standards Roadmap | NIST. *Special Publication (NIST SP) - 500-291*.

Holland, C., & Light, B. (1999). A critical success factors model for ERP implementation. *IEEE Software*, *16*(3), 30–36. https://doi.org/10.1109/52.765784

Hon, W. K., & Millard, C. (2016). Use by Banks of Cloud Computing: An Empirical Study. *Social Science Research Network*.

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2862715_code1577160.pdf?abstractid=2856431&mirid=1&type=2

Hon, W. K., & Millard, C. (2018a). Banking in the cloud: Part 1 – banks' use of cloud services. *Computer Law &Amp; Security Review*, *34*(1), 4–24. https://doi.org/10.1016/j.clsr.2017.11.005

Hon, W. K., & Millard, C. (2018b). Banking in the cloud: Part 2 – regulation of cloud as 'outsourcing.' *Computer Law &Amp; Security Review*, *34*(2), 337–357. https://doi.org/10.1016/j.clsr.2017.11.006

IDC. (2022). *Banks and Their Multicloud Strategies*. https://www.idc.com/getdoc.jsp?containerId=EUR148659522

ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*.

Ivanov, I. I. (2008). Utility Computing: Reality and Beyond. *E-Business and Telecommunications*, 16–29. https://doi.org/10.1007/978-3-540-88653-2_2

Joshi, K. P., Yesha, Y., & Finin, T. (2014). Automating Cloud Services Life Cycle through Semantic Technologies. *IEEE Transactions on Services Computing*, *7*(1), 109–122. https://doi.org/10.1109/tsc.2012.41

Karkošková, S. (2018). Towards Cloud Computing Management Model Based on ITIL Processes. *Proceedings of the 2nd International Conference on Business and Information Management*. https://doi.org/10.1145/3278252.3278265

Karkošková, S., & Feuerlicht, G. (2017). Cloud computing governance reference model for cloud service consumers. *Springer*.

Kaya, F., Van Den Berg, M., Wieringa, R., & Makkes, M. X. (2020). The Banking Industry Underestimates Costs of Cloud Migrations. *IEEE Conference on Business Informatics*. https://doi.org/10.1109/cbi49978.2020.00039

Kothari, S. R. (2004). *Research Methodology: Methods and Techniques*.

Kratzke, N. (2018). A Brief History of Cloud Application Architectures. *Applied Sciences*, *8*(8), 1368. https://doi.org/10.3390/app8081368

Kumar, R., & Charu, S. (2015). Comparison between cloud computing, grid computing, cluster computing and virtualization. *International Journal of Modern Computer Science and Applications*.

Lanza, N. (2022). *The ultimate guide to banking in the cloud*. Accenture. https://bankingblog.accenture.com/the-ultimate-guide-to-banking-in-the-cloud

Lian, J. W., Yen, D. C., & Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), 28–36. https://doi.org/10.1016/j.ijinfomgt.2013.09.004

Lin, H. J., Wen, M. M., & Lin, W. T. (2012). The Relationships between Information Technology, E-Commerce, and E-Finance in the Financial Institutions: Evidence from the Insurance Industry. *Intelligent Information and Database Systems*, 194–206. https://doi.org/10.1007/978-3-642-28490-8_21

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management &Amp; Data Systems*, *111*(7), 1006–1023. https://doi.org/10.1108/02635571111161262

Lynn, T., Liang, X., Gourinovitch, A., Morrison, J., Fox, G., & Rosati, P. (2018). Understanding the Determinants of Cloud Computing Adoption for High Performance Computing. *Proceedings of the 51st Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2018.489

MacKinnon, W., Grant, G., & Cray, D. (2008a). Enterprise Information Systems and Strategic Flexibility. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. https://doi.org/10.1109/hicss.2008.149

MacKinnon, W., Grant, G., & Cray, D. (2008b). Enterprise Information Systems and Strategic Flexibility. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. https://doi.org/10.1109/hicss.2008.149

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems*, *51*(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

Megargel, A., Shankararaman, V., & Walker, D. K. (2020). Migrating from Monoliths to Cloud-Based Microservices: A Banking Industry Example. *Springer International Publishing EBooks*, 85–108. https://doi.org/10.1007/978-3-030-33624-0_4

Mell, P., & Grance, T. (2011). SP 800-145. The NIST Definition of Cloud Computing. *NIST*.

Mocetti, S., Pagnini, M., & Sette, E. (2016). Information Technology and Banking Organization. *Journal of Financial Services Research*, *51*(3), 313–338. https://doi.org/10.1007/s10693-016-0244-3

Modisane, P., & Jokonya, O. (2021). Evaluating the benefits of Cloud Computing in Small, Medium and Micro-sized Enterprises (SMMEs). *Procedia Computer Science*, *181*, 784–792. https://doi.org/10.1016/j.procs.2021.01.231

Mourad, M. B. A., & Hussain, M. (2014). The Impact of Cloud Computing on ITIL Service Strategy Processes. *International Journal of Computer and Communication Engineering*, *3*(5), 367–371. https://doi.org/10.7763/ijcce.2014.v3.351

Nedelcu, B., Stefanet, M., Tamasescu, I., Tintoiu, S., & Vezeanu, A. (2015). Cloud Computing and its Challenges and Benefits in the Bank System. *Database Systems Journal*, *6*(1), 44–58.

Okumus, F. (2003). A framework to implement strategies in organizations. *Management Decision*, *41*(9), 871–882. https://doi.org/10.1108/00251740310499555

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information &Amp; Management*, *51*(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006

Omarini, A. E. (2017). The Digital Transformation in Banking and The Role of FinTechs in the New Financial Intermediation Scenario. *International Journal of Finance, Economics and Trade*, 1–6. https://doi.org/10.19070/2643-038x-170001

Pahl, C., Xiong, H., & Walshe, R. (2013). A Comparison of On-Premise to Cloud Migration Approaches. *Service-Oriented and Cloud Computing*, 212–226. https://doi.org/10.1007/978-3-642-40651-5_18

Parahoo, K. (2007). *Nursing Research: Principles, Process And Issues*. Palgrave MacMillan.

Paraiso, F., Merle, P., & Seinturier, L. (2014). soCloud: a service-oriented component-based PaaS for managing portability, provisioning, elasticity, and high availability across multiple clouds. *Computing*, *98*(5), 539–565. https://doi.org/10.1007/s00607-014-0421-x

Parne, P. (2021). Cloud Computing Strategy and Impact in Banking/Financial Services. *Computer Science and Information Technology Trends*. https://doi.org/10.5121/csit.2021.111704

Pauwels, L. (2011). *The Sage Handbook of Visual Research Methods*. Sage Publications Ltd.

Petcu, D. (2011). Portability and Interoperability between Clouds: Challenges and Case Study. *Towards a Service-Based Internet*, 62–74. https://doi.org/10.1007/978-3-642-24755-2_6

Petcu, D. (2013). Multi-Cloud. *Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds - MultiCloud '13*. https://doi.org/10.1145/2462326.2462328

Petcu, D., Macariu, G., Panica, S., & Crăciun, C. (2013). Portable Cloud applications—From theory to practice. *Future Generation Computer Systems*, *29*(6), 1417–1430. https://doi.org/10.1016/j.future.2012.01.009

Peterson, R. (2004). Crafting Information Technology Governance. *Information Systems Management*, *21*(4), 7–22. https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2

Peterson, R., O'Callaghan, R., & Ribbers, P. M. (2000). Information technology governance by design: investigating hybrid configurations and integration mechanisms. *International Conference on Information Systems*, 435–452. https://doi.org/10.5555/359640.359775

Pohl, M., Babel, A., Staegemann, D., Haertel, C., Kharitonov, A., Nahhas, A., & Turowski, K. (2022). Migration Patterns for Applications in Cloud Computing Environments. *Proceedings of Seventh International Congress on Information and Communication Technology*, 621–630. https://doi.org/10.1007/978-981-19-2394-4_57

Prasad, A., Green, P., & Heales, J. (2014). On governance structures for the cloud computing services and assessing their effectiveness. *International Journal of Accounting Information Systems*, *15*(4), 335–356. https://doi.org/10.1016/j.accinf.2014.05.005

Qasem, Y. a. M., Asadi, S., Abdullah, R., Yah, Y., Atan, R., Al-Sharafi, M. A., & Yassin, A. A. (2020). A Multi-Analytical Approach to Predict the Determinants of Cloud Computing Adoption in Higher Education Institutions. *Applied Sciences*, *10*(14), 4905. https://doi.org/10.3390/app10144905

Rahimah, K., & Aziati, N. (2017). The Integrated Framework of Cloud Computing Implementation in Higher Education Institution: A Review of Literature. *Advanced Science Letters*, *23*(2), 1475–1479. https://doi.org/10.1166/asl.2017.8370

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. *Journal of Enterprise Information Management*, *22*(1/2), 10–24. https://doi.org/10.1108/17410390910922796

Ritchie, J., Lewis, J., Nicholls, C. M. N., & Ormston, R. (2013). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. SAGE Publications.

Rogers, D. L. (2016). *The Digital Transformation Playbook: Rethink Your Business for the Digital Age (Columbia Business School Publishing)* (Illustrated). Columbia Business School Publishing.

Rosian, M., Altendeitering, M., & Otto, B. (2021). A Socio-Technical Analysis of Challenges in Managing Multi-Clouds. *Wirtschaftsinformatik 2022 Proceedings 3*.

Sadashiv, N., & Kumar, S. M. D. (2011). Cluster, grid and cloud computing: A detailed comparison. *2011 6th International Conference on Computer Science &Amp; Education (ICCSE)*. https://doi.org/10.1109/iccse.2011.6028683

Safari, F., Safari, N., Hasanzadeh, A., & Ghatari, A. R. (2015). Factors affecting the adoption of cloud computing in small and medium enterprises. *International Journal of Business Information Systems*, *20*(1), 116. https://doi.org/10.1504/ijbis.2015.070894

Samreen, F., Blair, G. S., & Rowe, M. (2014). Adaptive decision making in multi-cloud management. *Proceedings of the 2nd International Workshop on CrossCloud Systems - CCB '14*. https://doi.org/10.1145/2676662.2676676

Scarfone, K. A., Souppaya, M. P., & Hoffman, P. (2011). Guide to security for full virtualization technologies. *NIST*. https://doi.org/10.6028/nist.sp.800-125

Schneider, S., & Sunyaev, A. (2016). Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. *Journal of Information Technology*, *31*(1), 1–31. https://doi.org/10.1057/jit.2014.25

Sfondrini, N., Motta, G., & Longo, A. (2018). Public Cloud Adoption in Multinational Companies: A Survey. *2018 IEEE International Conference on Services Computing (SCC)*. https://doi.org/10.1109/scc.2018.00030

Shimizu, K., & Hitt, M. A. (2004). Strategic flexibility:Organizational preparedness to reverse ineffective strategic decisions. *Academy of Management Perspectives*, *18*(4), 44–59. https://doi.org/10.5465/ame.2004.15268683

Shu, W., & Strassmann, P. A. (2005). Does information technology provide banks with profit? *Information &Amp; Management*, *42*(5), 781–787. https://doi.org/10.1016/j.im.2003.06.007

Sneader, K., & Sternfels, R. A. (2020). From surviving to thriving: Reimagining the post-COVID-19 return. *McKinsey & Company*.

Sohal, A. S., & Fitzpatrick, P. (2002). IT governance and management in large Australian organisations. *International Journal of Production Economics*, *75*(1–2), 97–112. https://doi.org/10.1016/s0925-5273(01)00184-0

Sony, M., Antony, J., & Mc Dermott, O. (2022). How do the technological capability and strategic flexibility of an organization impact its successful implementation of Industry 4.0? A qualitative viewpoint. *Benchmarking: An International Journal*. https://doi.org/10.1108/bij-09-2021-0541

Spillner, J., Bogado, Y., Benítez, W., & López-Pires, F. (2018). Co-Transformation to Cloud-Native Applications - Development Experiences and Experimental Evaluation. *Proceedings of the 8th International Conference on Cloud Computing and Services Science*. https://doi.org/10.5220/0006790305960607

The Economist. (2021a). *Branching out: can banks move from city centres to digital ecosystems?* https://www.temenos.com/wp-content/uploads/2021/06/eiu-global-banking-report-2021.pdf

The Economist. (2021b). *Capturing value in the cloud*. https://www.temenos.com/wp-content/uploads/2021/11/Cloud-report-V1.pdf

Thorne, S. (2000). Data analysis in qualitative research. *Evidence-Based Nursing*, *3*(3), 68–70. https://doi.org/10.1136/ebn.3.3.68

Tornatzky, L. G., Fleischer, M., & Chakrabarti. (1990). *Processes of technological innovation.*

Trovato, F., Sharp, A., & Siman, T. (2019). Cloud, co-location, on-premises and hybrid disaster recovery solutions: Pros, cons, and a cost comparison. *Journal of Business Continuity and Emergency Planning*, *13*(2), 120–135.

Truyen, E., Kratzke, N., Van Landuyt, D., Lagaisse, B., & Joosen, W. (2020). Managing Feature Compatibility in Kubernetes: Vendor Comparison and Analysis. *IEEE Access*, *8*, 228420–228439. https://doi.org/10.1109/access.2020.3045768

Van Grembergen, W. (2004). IT Governance and Its Mechanisms. *Information Systems Control Journal*.

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172–2175. https://doi.org/10.1016/j.matpr.2021.11.121

Voas, J., & Zhang, J. (2009). Cloud Computing: New Wine or Just a New Bottle? *IT Professional*, *11*(2), 15–17. https://doi.org/10.1109/mitp.2009.23

Vugec, D. S., Spremić, M., & Bach, M. P. (2017). IT Governance Adoption in Banking and Insurance Sector: Longitudinal Case Study of COBIT Use. *International Journal for Quality Research*, 691–716. https://doi.org/10.18421/ijqr11.03-13

Wahsh, M. A., & Dhillon, J. S. (2015). An investigation of factors affecting the adoption of cloud computing for E-government implementation. *2015 IEEE Student Conference on Research and Development (SCOReD)*. https://doi.org/10.1109/scored.2015.7449349

Warner, K. S., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Werth, O., Schwarzbach, C., Rodríguez Cardona, D., Breitner, M. H., & Graf Von Der Schulenburg, J. M. (2020). Influencing factors for the digital transformation in the financial

services sector. *Zeitschrift Für Die Gesamte Versicherungswissenschaft*, *109*(2–4), 155–179. https://doi.org/10.1007/s12297-020-00486-6

Westerlund, M., & Kratzke, N. (2018). Towards Distributed Clouds: A Review About the Evolution of Centralized Cloud Computing, Distributed Ledger Technologies, and A Foresight on Unifying Opportunities and Security Implications. *2018 International Conference on High Performance Computing &Amp; Simulation (HPCS)*. https://doi.org/10.1109/hpcs.2018.00108

Yan, G. (2017). Application of Cloud Computing in Banking: Advantages and Challenges. *Proceedings of the 2017 2nd International Conference on Politics, Economics and Law (ICPEL 2017)*. https://doi.org/10.2991/icpel-17.2017.8

Zhu, K., Dong, S., Xu, S. X., & Kraemer, K. L. (2006). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. *European Journal of Information Systems*, *15*(6), 601–616. https://doi.org/10.1057/palgrave.ejis.3000650

Appendix A : Experts Interviews Questions

Interviewer Introduction

The researcher introduces himself.

The researcher explains the purpose of the research and the interview.

Interviewee Introduction

Q1: What is your current role within Accenture?

Q2: Could you briefly describe your experience with multi-cloud projects within the financial sector?

Q3: Which project do you think is the most interesting to focus on for the rest of the interview?

Project Context

Q4: What are the characteristics of the multi-cloud project?

Example: number of clouds, deployment model and service model.

Q5: What are the characteristics of the organization?

Example: type, size, country

Q6: How experienced was the organization with multi-cloud before the project started?

Q7: What are the reasons for adopting this multi-cloud project?(ex: Laws & Regulation, Cost Reduction, Legacy IT systems,,, etc.)?

Q8: How did the organization evaluate the technological benefits (Relative Advantage) of the project?

Organizational Dimension

Q9: What are the organizational challenges that the organization encountered before and during implementing the multi-cloud project?

Example: Security Concerns, Organizational Culture or Readiness, Shortage of Skills

Q10: How did the organization solve each organizational challenge?

Technological Dimension

Q11: What are the technological challenges that the organization encountered before and during implementing the multi-cloud project?

Example:

Integration between the different cloud providers (Interoperability)

Managing the security across the different cloud providers

SLA between the different cloud providers (Support and Maintenance)

Q12: How did the organization solve each technological challenge?

Environmental Dimension

Q13: What are the environmental challenges that the organization encountered before and during implementing the multi-cloud project?

Example:

Laws & Regulations

Sustainability & Green IT

The role of customers, suppliers, and partners of the organization

Q14: How did the organization solve each environmental challenge?

Project Outcome

Q15: What are the benefits of the project?

Extra Questions

Q16: Is there anything else that you would like to mention about this project?

Q17: Do you have any recommendations for any other Accenture contact persons?

Q18: Do you want to ask me any questions?

Appendix B : Validation Interviews Questions

Interviewer Introduction

The researcher explains the purpose of the interview.

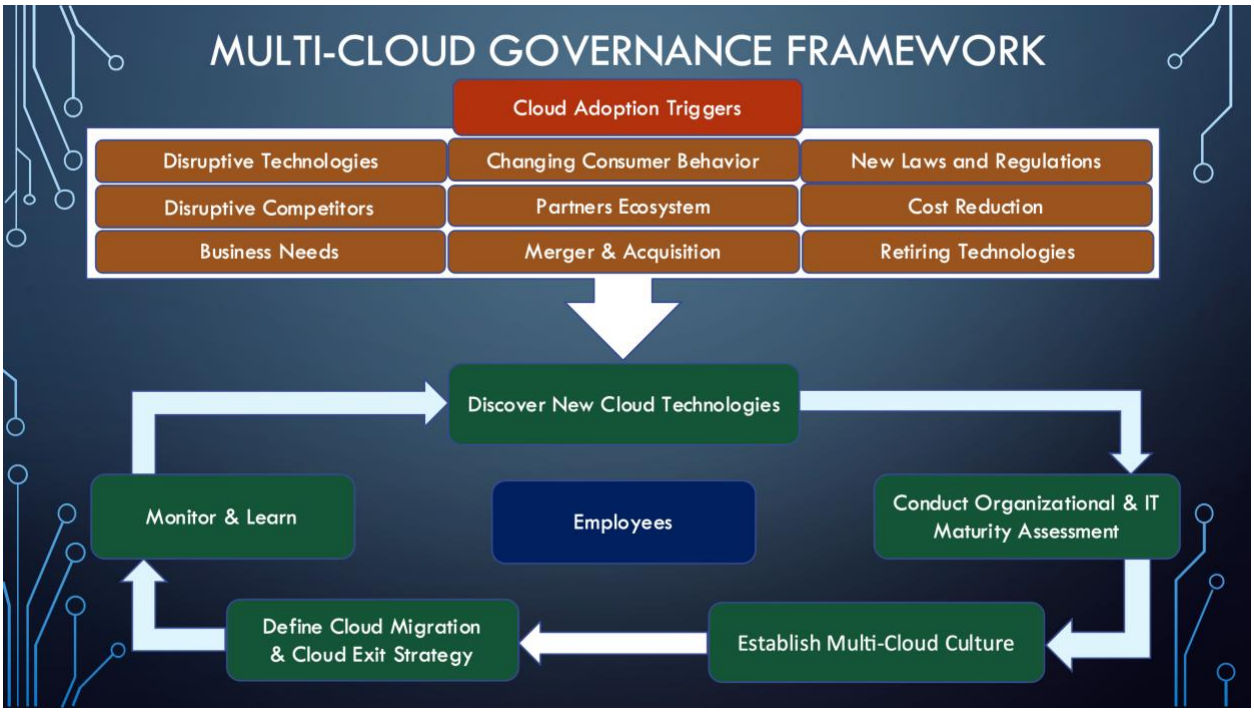
The researcher explains the first version of Multi-Cloud Governance Framework.

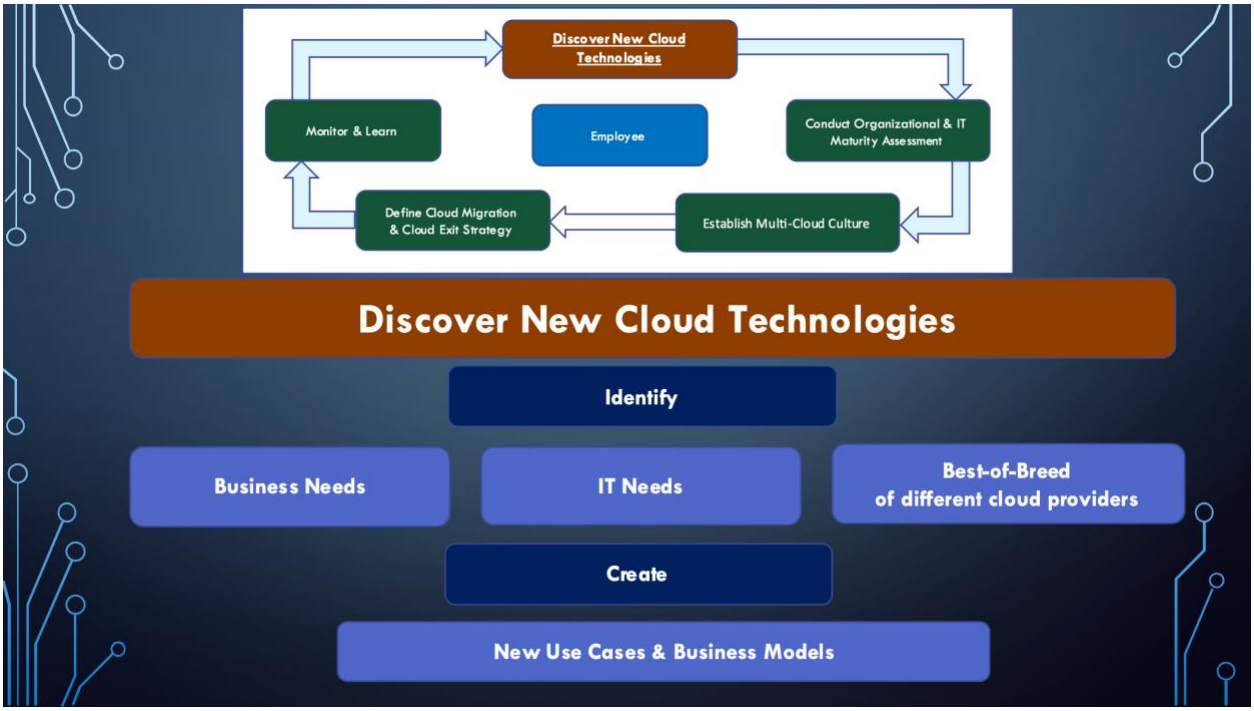
Q1: What are the elements that you think are missing from the framework?

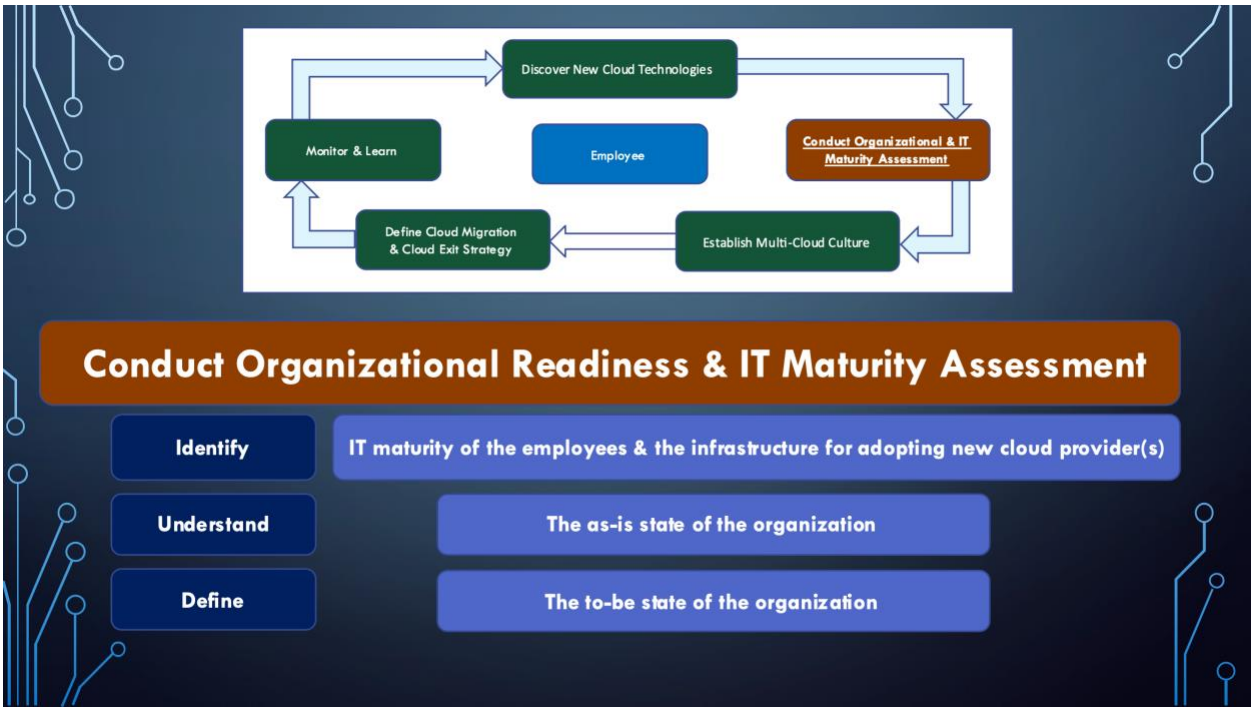
Q2: Do you agree with the steps in the framework?

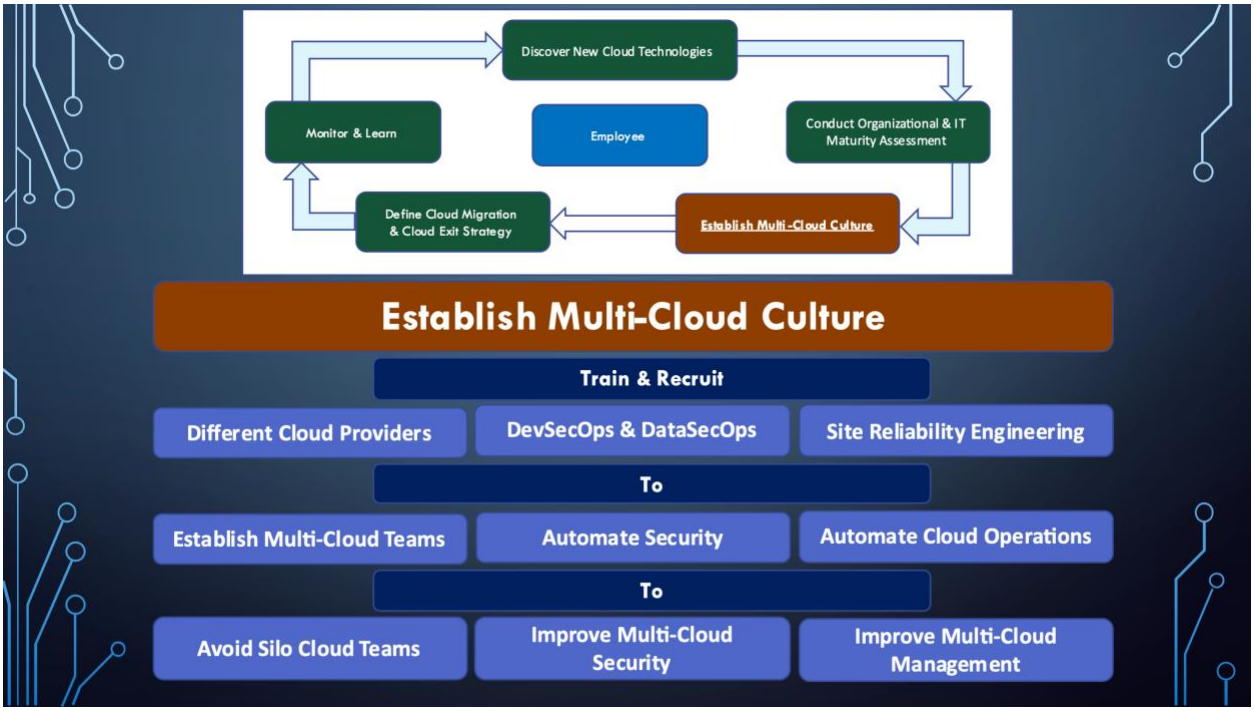
Q3: Do you agree with the order of the steps in the framework?

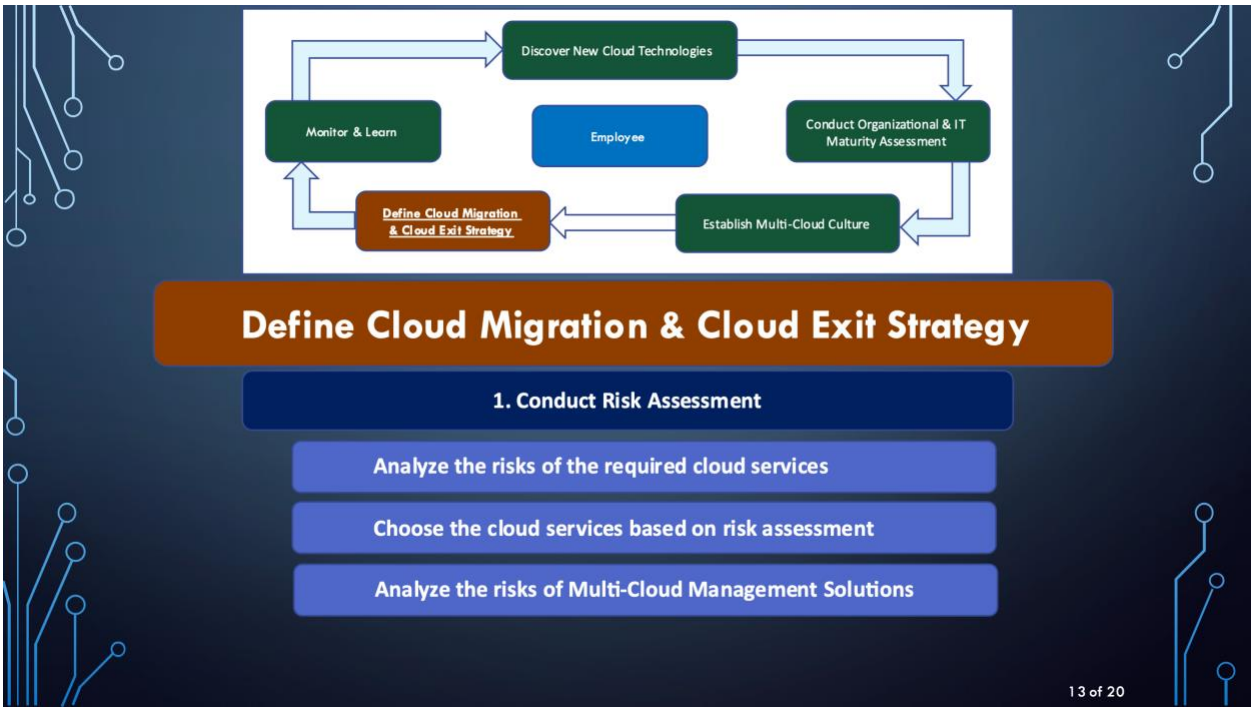
Appendix C : Final Version of Multi-Cloud Governance Framework

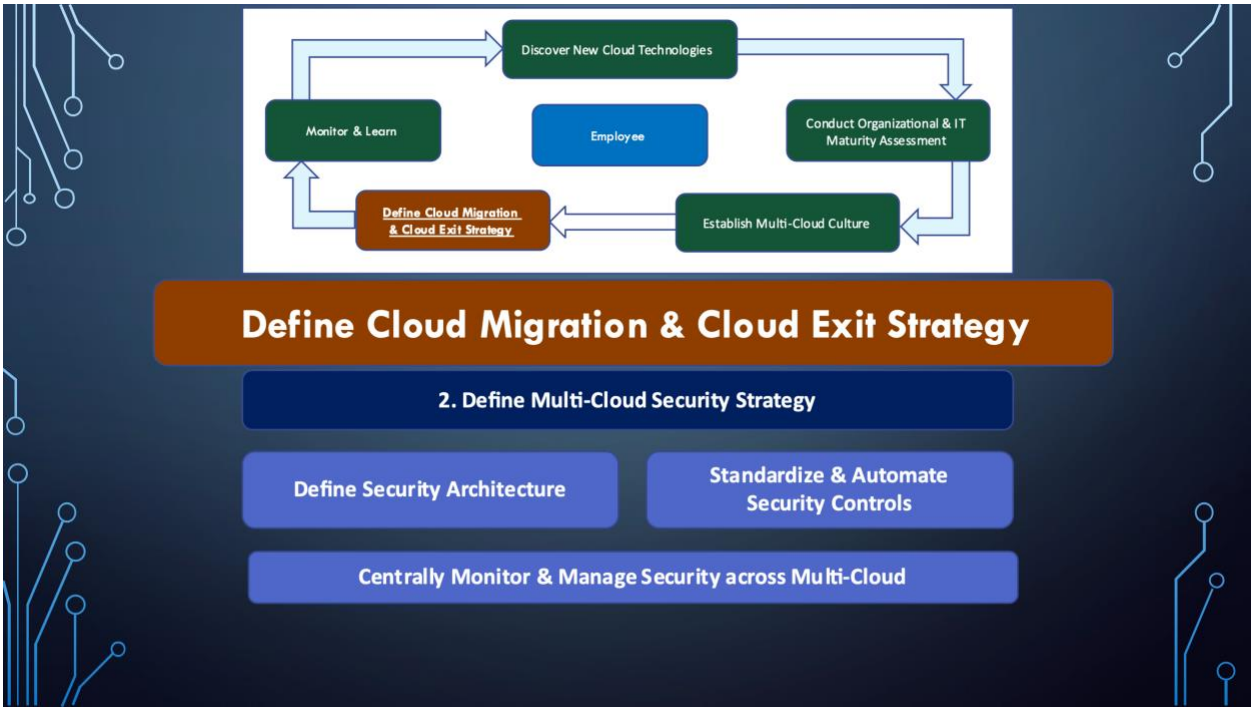


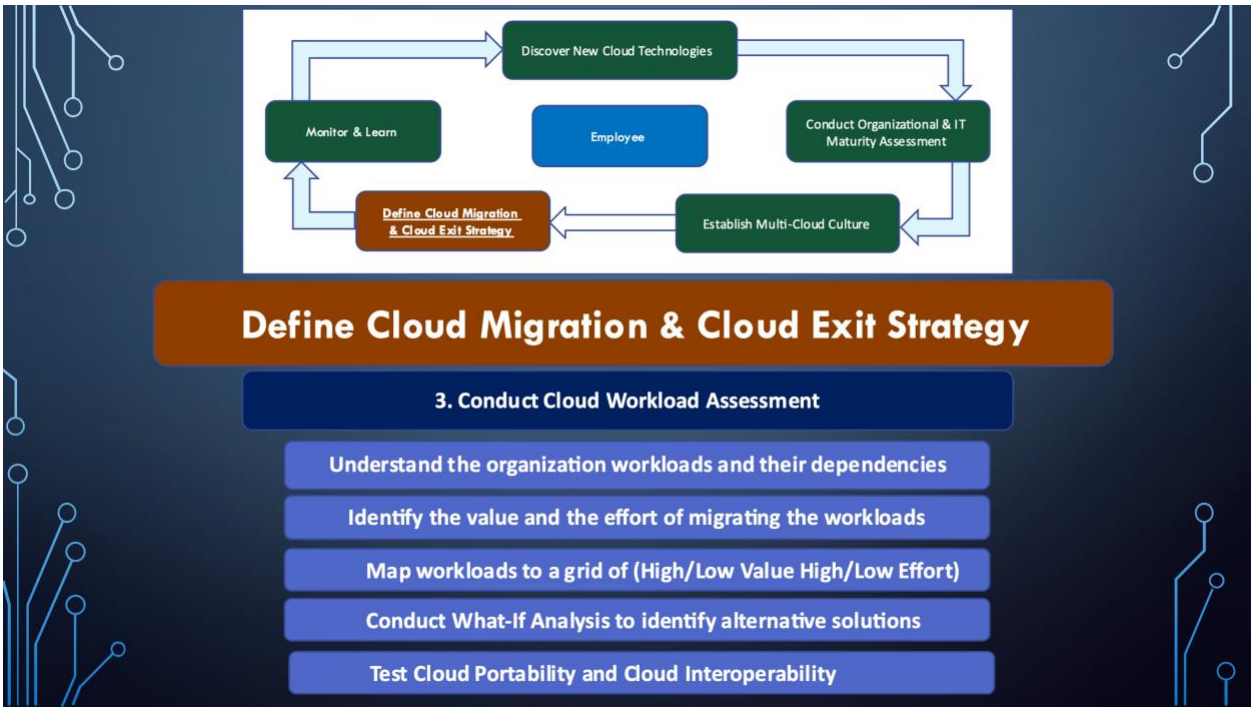


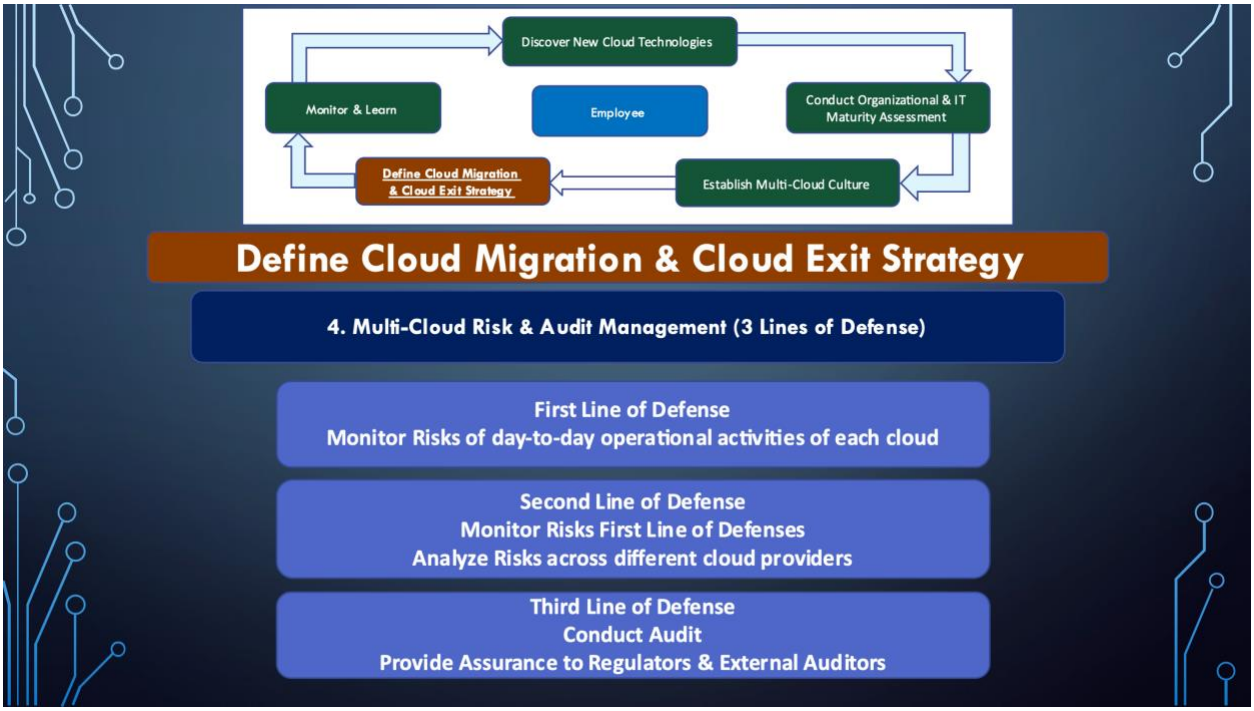

Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Conduct Organizational Readiness & IT Maturity Assessment
Identify
IT maturity of the employees & the infrastructure for adopting new cloud provider(s)
Understand
The as-is state of the organization
Define
The to-be state of the organization

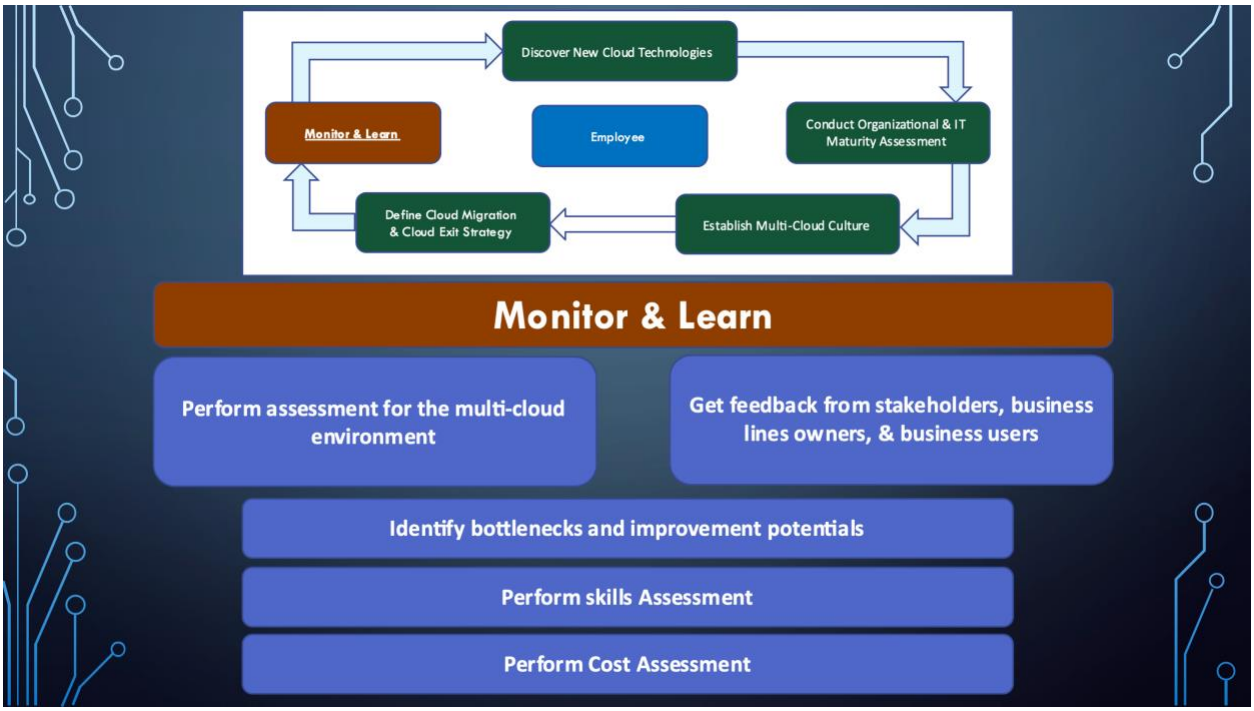

Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Establish Multi-Cloud Culture
Train & Recruit
Different Cloud Providers
DevSecOps & DataSecOps
Site Reliability Engineering
To
Establish Multi-Cloud Teams
Automate Security
Automate Cloud Operations
To
Avoid Silo Cloud Teams
Improve Multi-Cloud Security
Improve Multi-Cloud Management


Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Define Cloud Migration & Cloud Exit Strategy
1. Conduct Risk Assessment
Analyze the risks of the required cloud services
Choose the cloud services based on risk assessment
Analyze the risks of Multi-Cloud Management Solutions
13 of 20


Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Define Cloud Migration & Cloud Exit Strategy
2. Define Multi-Cloud Security Strategy
Define Security Architecture
Standardize & Automate Security Controls
Centrally Monitor & Manage Security across Multi-Cloud


Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Define Cloud Migration & Cloud Exit Strategy
3. Conduct Cloud Workload Assessment
Understand the organization workloads and their dependencies
Identify the value and the effort of migrating the workloads
Map workloads to a grid of (High/Low Value High/Low Effort)
Conduct What-If Analysis to identify alternative solutions
Test Cloud Portability and Cloud Interoperability


Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Define Cloud Migration & Cloud Exit Strategy
4. Multi-Cloud Risk & Audit Management (3 Lines of Defense)
First Line of Defense
Monitor Risks of day-to-day operational activities of each cloud
Second Line of Defense
Monitor Risks First Line of Defenses
Analyze Risks across different cloud providers
Third Line of Defense
Conduct Audit
Provide Assurance to Regulators & External Auditors


Discover New Cloud Technologies
Monitor & Learn
Employee
Conduct Organizational & IT Maturity Assessment
Define Cloud Migration & Cloud Exit Strategy
Establish Multi-Cloud Culture
Monitor & Learn
Perform assessment for the multi-cloud environment
Get feedback from stakeholders, business lines owners, & business users
Identify bottlenecks and improvement potentials
Perform skills Assessment
Perform Cost Assessment

Appendix D : Most Important Citations from Expert Interviews

This appendix presents the most important citations from the Expert Interview.

Q4: What are the characteristics of the multi-cloud project?

Interviewee	Answer	Keywords
Int-01	They have **private cloud on premise**. The users can **provision virtual resources**, so it behaves like a public cloud. And other multi-cloud. The big vendors there like Azure and AWS. There are multiple legacy systems mainframe IBM that run core baking applications. So, for how it works, for each cloud environment, there is a **Cloud Competence Center (CCOC) or Cloud Center of Excellence (CCOE)**. So, there are owners of the muti-cloud environment. And what they do firstly, they **look into the services** and **conduct risk assessments** because in financial industry **risk assessment** is a crucial part of **onboarding any new service** or any **new vendor**. So, what these **CCOE** do is that they look into services that are offered by these cloud environments. And they do risk assessment and then once the services are risk assessed, they approved them. Only then, I can use it. So what these CCOE do it that, they **keep an eye on the available cloud services**, and then they **do risk assessment**. Once, it **passed**, they make it **available**. And they are also responsible for **onboarding DevOps teams** to different cloud environments. They also create **framework** to ensure that a **proper governance** is done even if a cloud team uses a certain service, they need to do it in a certain manner. These CCOE ensure that all the checks are done, and they have all the **governance roles** are set. Every team get two subscription **production subscription and non-**	**CCOE** **Cloud Technologies Discovery** **Risk Assessment to Cloud Services** **DevOps** **Production Cloud Environment** **Non-Production Cloud Environment** **Governance Frameworks** **Processes scan deployed cloud resources.**

	production subscription. CCOE have processes that scan the resources that the teams have created to check if the resources follow the **security principles** or not. They create reports that send it out if someone violate it. There is also **Cyber Defense Central Team** which has different kind of scanners. They **install agents in all the deployed cloud services**. The agents **scan for vulnerabilities** and report them. For how they choose which approved cloud service to deploy. For each area, there is a solution architect who look into the approved cloud services and then they decide.	**Auto reporting violations** **Cyber Defense Central Team**
Int-02	In this client what they currently have is **on-premise datacenter, AWS, Azure cloud** and they use a little bit of **Google cloud**. The main goal of the bank is to **deliver landing zones**. Basically **moving workloads** from on-premise to cloud. The way to facilitate that is the enablement of landing zones. In both cloud providers, Azure and Amazon. The reason for that is that the **landing zones** is **a standardized way** to provider **a secure and a better accounts** in Amazon and **subscriptions** in Azure in an **automatic way** and is accustomed to the bank in a short time with a **pre-set of capabilities and controls** that already agree with **security**. Ensure that everyone consume cloud in a standard secure way because the most important thing in a bank is security. The approach is to have **two different environments**. So we have **non-production environment** which is a replica of the **production environment** that it is maintained by **Cloud Center of Excellence (CCOE)**. They **develop a mature landing zones**. The CCOE do two things. One they offer products. In this case the landing zones. And they operate products within these products. Let's say there are ten projects in Amazon. Some of those are **self-managed by different departments** in the bank, but in other cases some departments do not have the expertise to manage their cloud	**Develop Landing Zones** **Production Cloud Environment** **Non-Production Cloud Environment** **CCOE** **Cloud Center of Authority** **Risk Assessment to Cloud Services**

	infrastructure. So the **CCOE is the one that operate their infrastructure**. They have three cloud accounts. One from **sandbox**. The second from **less critical** like pre-production. And the last one the **production accounts**. Each of those have **different security profiles** and **different security risk assessments**. There is a **Cloud Center of Authority**. When I need a cloud service that is not available in the landing zones. Then I need to ask the Cloud Center of Authority who are group of **Enterprise Architects, Security Architects, and Cloud Architects** who review the requested cloud service. After their approval, the CCOE will set up the controls and allow it in the landing zones. After that, I will be able to use it. In the past, they thought about the private cloud, but they decided to go to public cloud. The current approach, if something new then if it is better sit on cloud than on-premises datacenter, then it will go to cloud. They stopped any new build on on-premises datacenter unless it is critically required. **The on-premises datacenter will remain, but it usage will reduce by the time.**	
Int-05	The project was a **merger** and **acquisition** between two insurance companies. The daughter company had an old on-premises datacenter and the mother company had another private cloud and SaaS solutions. All the data and applications on the on-premises datacenter must be migrated to the private cloud. Most of the applications are **re-platformed** on private cloud for **faster migration velocity**.	**Migration Velocity**
Int-11	They were already engaged with Azure. They had some deployment done. There was **no structure**, **no**	**No Strategy**

	landing zones actually. First of all the **strategy** was **important**. They had several departments that use a **credit card type** of work to **deploy cloud resources**. It was **not a strategy**. So, we obviously, we need to help the client to **build** up the **strategy**, and the **cloud reference architecture**. We helped the client to develop the **cloud reference architecture**. And we built the **landing zones** based on **reference architecture** and **creating** a **detailed designs** for specific cloud components, think about **backup**, key vaults and identity and access management. So, these detailed designs were created at the beginning. We then deployed the landing zones for both Azure and AWS. After my departure, I heard that they are also considering Google cloud.	**Cloud Reference Architecture** **Landing Zones**

Q9:

What are the organizational challenges that the organization encountered before and during implementing the multi-cloud

project?

Q10:

How did the organization solve the organizational challenges?

Interviewee	**Answer**	**Keywords**
Int-01	They have gone through **re-organization** last year. What they have done it that, there are two divisions. **CIO division and CTO division**. The CIO covers all the products of the bank. And the **CTO** covers the **technology part**. The **CTO** is kind of **enabler**. Whatever the **business needs** from **technologies**, all the technologies are implemented by enablers teams. There are different **enablers** team such as the **integration teams** which I work with now. Some of their members are **member of CCOEs.** There are	Re-**organization** **DevOps** **Agile Methodology**

	also infrastructure teams, file transfer teams, and network teams. There are tooling teams that make sure all the required tools that are needed by the business areas are available. So that how the teams are divided. All of them are working in a **DevOps** manner and **agile methodology** and **scrums**. Whatever service you build on the business side or technology side, you build it and maintain it. They follow a triangle area. For each area, there is an IT Lead responsible for IT resources. There is an Area Lead responsible for products. And then there is an **Area Architect** that is a representative in **Architects Board**. This is how they **align between the business and IT.** For how they choose which cloud vendor, it depends on the **skills of team** and the **learning curve**. They check the **approved cloud services**, then they choose the one that fulfil the business requirements. For the **Enterprise Architecture**, there are **layers** of **Architects**. There are **Enterprise Architects who are with the board members**. They define overall **Enterprise Architecture Principles** for the entire organization. And there are **Architects** within each **Business Area**. And the principles govern the Business Areas. There are **Solution Architects** within each area who implement **Architecture Principle** and also have their own Architecture Principles for their own applications within the Business Area. They **outsource** IT services to companies like Accenture and IT enabler services. It different from area to area. **Core banking** is very **hard** to **migrate** to **cloud**. Especially the big bank. Sometimes **technical limitation**, sometimes **lack** of **trust** of public cloud	**Current Cloud Skills of each team** **Enterprise Architecture Principles** **Outsource** **Mainframe limitation**

	because it is a **sensitive data** that they want to **keep close**. Generally, sometimes I see that the **technical limitations** are the **main challenge** that prevent them from **migrating the legacy applications to the cloud.**	
Int-02	The bank has gone through **full transformation**. So the bank was **not ready for cloud**. They set it up per department. The main challenge is **security**. Everyone in the bank was **not familiar with the cloud** or the **real benefits**. For the **shortage of skills**, the bank use **third party vendors** like Accenture. So they were short on skills and over time they have grown mature. **Everything that you listed in the interview questions was a challenge**. Some is not a challenge. **Security** is still a challenge, but **not a concern anymore**, because there is **Security Architects in the CCOE**. So, **every cloud solution** has a **point of view of security**. The **stakeholders communications** are **improved**. The people in the bank now knows what is the cloud and how to use and consume it and how it the lead and the bank has defined policies. Each department has **Account Management Officer (AMO)**. All the **CCOE** and **AMOs** know the **MAGs (Microsoft, AWS and Google)**. The bank has **FinOps**. However, they still need Amazon, Microsoft, Avanade and Accenture to provide the services that they need. The members of their **CCOE** are **leadership**, **architects**, the delivery people how deliver the work like the software developers are **third party**. They have people how **oversight** what the third party are doing to ensure that they **maintain** the **knowledge** in the **bank** and do not get lock in IT outsource vendor. First, they conduct **maturity assessment**. They hired **a third party consultancy company to do maturity**	Re-**organization** **Security Concerns** **Skill Shortage** **Security Architects** **Account Management Officer** **FinOps** **Maturity Assessment** **Roadmap**

	assessment and **define** actions and **roadmap**. Based on the maturity assessment, they **defined their weaknesses** and then they **developed road map** and **address them one by one** from **organizational culture, to organizational readiness, to skills sets, to how to manage the cloud.**	
Int-03	The key challenge is **building skills** because it is an organization that was implementing cloud for the first time. They do not have the **necessary cloud skills**. A lot of the work that we do is to effectively **establish capabilities** within the organization to be able to build the cloud platform and also be to run it and manage it. So, a lot of the new skills are cloud engineering, infrastructure,,, etc. The other challenge is taking the set of applications that they had and then **migrating** them to cloud particularly the ones that are not cloud native. We had to **decide whether rehost or re-engineer them**. **Security** is a **big** one**. Awareness** of **security** is very **important**. We had to make sure that they got the right **security controls** and in place **early before** building anything on the cloud. The security teams are part of the **agile teams**. They adopted **DevSecOps** approach to make sure that **security** is at the **heart** of **everything** on the cloud**.** **Regulatory challenges** is also a big **challenge**. We did a lot of work to make sure that we put the **regulators** are on the line with us and **demonstrate** the **roadmap** and how to **mitigate** the **risks** and **demonstrate** how to **migrate** to **another cloud provider** when the chosen one is unavailable. I think the final think is **cost management**. This means they will need a lot of **proof of concepts** as	**Building Skills** **Migration Strategy** **Security** **Security Awareness** **DevSecOps** **Regulators** **Cloud Portability** **Cost Management** **Cloud Cost Awareness** **Enterprise Architecture** **Guardrails**

	early as possible. They need to monitor cloud to **monitor** the **costs** and inform the developers to shut down the unneeded resources. Again get **cost monitoring** from the start and make sure that there is a **cost awareness** about cloud resources. Obviously, they need to give the engineers teams enough trainings to become fully aware with cloud costs. From **enterprise architecture perspective**, they run **agile team** and they want to make sure that the work is aligned with the **principles**, **frameworks**, and **guardrails**.	
Int-04	I mean we find that **making** an **effort** to **train** your workforce for cloud is **really effective**. One of my banks trained over **1,700 technologist** for public cloud in less than a year. That is a pretty **good number**. And the other thing we also found that you can **train folks** for **mainframes**. So, one of my clients had a big investment in training their **workforce** for **mainframe** because they want to keep the **mainframes** running for a while. So, bunch of their software developers are learning **COBOL**.	**Building Skills** **Mainframe Skills**
Int-09	We started with them to how to become **data-driven organization** of the future. And what do we need in term of underlying **capabilities** and **operating models**. How can we think about **data governance** and **security**. We started with **strategy** by putting together insights about what the others are doing in the market. What are the **benefits** that we see about moving to the cloud. And what are the **target state**, what do it look like as well as what it is going to take in terms of investment. It is a **collaborative journey** we had to **bring different people from line of business, data groups, and technology groups**. By the end of the **meetings**, everyone had a chance to	**Data-driven** **Data Governance** **Target State** **Feedback**

	put their **inputs**. After that we decided to what we will do for each migration wave. The other thing that we do is that we had to look at the **organizational maturity**. We spoke about **roles** and **responsibilities**, we did a lot of detailed work regarding, first of all, what are the outcomes that are we going toward, how are the involved players, and we used the **RACI framework** as well. What are the **roles** and **responsibility**, who is gonna be **accountable** and informed. They practice **continuously improvements**. They had a **quarterly meetings** to **check** what **progress** that they had made, how they improve things over time.	**Organization Maturity** **RACI framework** **Role & Responsibilities**
Int-10	**Shortage** of **skills** for the new cloud technologies. The **enablement** of **CI/CD**. These always a **problem** for **all banks**. The challenges were solved by **outsourcing 60% of workforce**. When you outsource, you outsource the hands and limbs.	**Skills Shortage** **CI/CD**
Int-11	The most **important challenge** was **security**. Of course, the other thing is about the **operations**. Most of the **organizations** do not completely understand the magnitude of the operations that the cloud brings with it self, right. So, have a **skilled people** that will **operate** and **maintain** the **environments**. And also running those **environments** from **organizational perspective** like **DevOps** and how they will work together and such. And most of the time they **depend** on **organizations** such as Accenture to help them out. You need to **skill** the **people** and you need to set up people to **maintain** these **environments** in a **secure** manner. And obviously, the hyperscale have a very big say in this. There are constant involvement from AWS and Microsoft experts with them and us to support them in operating and maintain the environment.	**Security** **DevOps** **Skills Shortage** **CCOE** **Feedback**

	As I said in the beginning we supported the customer in the **cloud journey** about how they are **skilled** now. So, we **did** a lot of **assessment** for that. And what are the **skills** that they will **need**. And the **gap** was presented to the **organization** to start the **trainings**. Cloud **migration** is a vehicle of change because you change the **way** of **working** and **roles** that exist before will be no longer there. As a part of the **transformation** at that time, we spoke about **CCOE** and **Cloud Management Organization** as we call it at that time. What we propose is actually there are 2 units. One is the **Cloud Management Office** of people are mainly **architects**, **business**, and **security** where ideas about the cloud are developed. The **second one** is the **CCOE** that **execute** those ideas into platforms and make them available for the organization to use it. There are **meeting** every **weeks** that discuss the **new challenges**, or **existing projects** or **new projects** or new **development** with the hyperscalers. So that it can be implemented in the landing zones. We usually call the cloud providers the hyperscalers.	
Int-15	They are **struggling** with the **skills shortage**. They are **putting** a lot of effort to **train** their **employees**. They are asking cloud **vendors** to come and give them **trainings**.	**Skills Shortage**

Q11:

What are the technological challenges that the organization encountered before and during implementing the multi-cloud project?

Q12:

How did the organization solve technological challenges?

Interviewee	Answer	Keywords
Int-01	If they want to **integrate** a **public cloud resource** with **on-premises**, then they will have to check the **Architecture Principles** on how the **integration** must be **implemented**. For example, if there an application on Azure and application on AWS and they need to have a file transfer, how will that happen. For example, Azure exposes its services via **http endpoints**, so then what we do, we set **enterprise gateways** on Azure, AWS, and on-premises. And then always proxy their services via enterprise gateways. Even the IBM **mainframe** is **modernized** a bit, a IBM allowed the **mainframe** to expose its services via **http endpoints**. Then the **cloud applications** can call the **http endpoints** and **consume services** from **mainframe**. Similar, the **mainframe** can **consume** from **cloud** applications.	**Architecture Principles** **Enterprise Gateways** **Modernize mainframe** **Http endpoints**
Int-02	The challenges as I said was around **security**. The bank has a B2B interface when they encounter third party. What they have is that they integrate with AWS and Azure as **normal business vendor**. They dedicate **infrastructure** on the **on-premises datacenter** that **connects directly with cloud providers**. The **security** was managed by **security principles**. There is **security architects** who manage all security solutions. They define **consistency in security controls across the cloud providers**. The goal is to apply to the cloud providers similar	**Security** **Security Principles** **Security Architects** **SLAs Categorization**

	controls based on security policies defined in the bank across the vendors. The cloud vendors **AWS** and **Azure** both have to **follow the same security policies** of the **bank**. So, the bank get the same security assurance and risk across both cloud providers. The integration is done based on **patterns**. On AWS **landing zones**, if you want to integrate SaaS, there is a **pattern**. There is a **way that is documented and assessed by security architects**. SLAs. When the bank introduce any vendor. They agree with the vendor on SLAs. **The bank categories the services and then define SLAs**. Category one services that affect the bank customers. Category 2 and 3 do not affect the customers. The services that are deployed on Azure are category 3. They are internal services. So, they do not need expensive SLAs for them. On AWS, there are category one. So they are 24/7 running in the production environment. The bank pays for premium SLAs for AWS. The SLAs depend on use cases. **At the moment they are vendor-lock in.** At first the **strategy** in the bank **was not multi-cloud**, it was leverage a single cloud. **Unfortunately**, in AWS, they developed everything using **AWS native tools**. So, AWS CloudFormation to build infrastructure. However, later on Azure, they started to use **Terraform**. It was the **maturity of the bank was better**. At the same time the bank created the **CCOE**, they created **DevOps CCOE**. The goal of **DevOps CCOE** is to define the **standards** in the **DevOps** and **automation**. So the **DevOps CCOE** are pushing for **Terraform** for **cloud agnostic** Infrastructure-as-Code (IoC) technology. In this way, anything that is	**Landing Zones** **Vendor-lock in** **Cloud Native Tools** **Terraform** **CCOE** **DevOps CCOE** **Cloud Agnostic**

	deployed using Terraform can deployed on any cloud provider more or less. We that the interoperability between cloud providers are not 100%, but it is **far more better than using cloud native tools**. So, the bank is looking **now** to **export the code that was written in AWS CloudFormation to Terraform**. There is a **dedicated project** that will brings the **code to Terraform**. The goal is to **rebuild** the AWS infrastructure using **Terraform**. So, until now there is no portability, if something breaks in AWS, it can be rebuild in AWS, but not in Azure. Terraform is the language for IoC. So, everything in cloud is built using **automation**. So we use **DevOps**. So we have **pipelines**. We have **sequence** of steps to automate the **creation of infrastructure**. Terraform is a generic that can be used in any cloud provider.	
Int-03	So, we did a lot of work to use whatever possible to use **cloud agnostic tools**. We **avoided** using the **cloud native tools**.	**Cloud agnostic tools**
Int-04	They are **software engineers** that are specialized in **multi-cloud integration**. What we find is that you can modernize a **mainframe** and make things **available** for **digital consumptions**. What we see is some of our clients is essentially creating an **API layer** that serves up the data that is in the **mainframe** for **consumption** by cloud products.	**Mainframe API Layer**
Int-05		**Integration Level**

	The **integration** was on **various levels**. On the **functional level**, if the **applications** want to talk to each other, think about the **interface** by **matching** the **data**. On the **technical level**, maybe **certain protocols** or **integration components**, this means on **technical** level, you need to ensure that the applications can talk over new protocols. And finally on the network level.	
Int-06	I think the first one is that they are moving to a **new environment**. So, a lot of the **application** are running on specific **hardware** and this **hardware does** not **exist** in the new **environment**. So, the **applications** had to be **re-platformed** to land on the new infrastructure. They **did not modernize** their **applications** to **cloud native application** because of the **time constraints**. And also because they are **moving** to **private** cloud**.** They want to do it as fast and easy as possible which is lift and shift. We **analyzed** the **applications** of the daughter company and we met with solutions architects of the mother company about how can we **map them** to the **private cloud**. So what components need re-platform and what components need changing. For **migration** strategy**,** we had to decide the **migration waves** and **analyze** the **dependencies** between the **applications**. We had to move part of the **mainframe hardware** to private cloud because it was impossible to re-platform some of the applications.	**Re-platform** **Migration Waves** **Dependency Analysis**

Int-10	They migrated to one public cloud. Then they realized later on that they are **vendor-lock** in. After 2 years, they decided to **re-consider** the **cloud migration strategy** and consider other public cloud. It is a good practice to develop your infrastructure using **cloud agnostic**.	**Vendor-lock in**
Int-11	**Setting** up a **landing zone** is not a big challenge. I call it it is more in the recent years a commodity. Any organization can set a landing zone. The challenge is understanding the application landscape and their dependencies.	**Landing Zones**

Q11:

What are the environmental challenges that the organization encountered before and during implementing the multi-cloud project?

Q12:

How did the organization solve environmental challenges?

Interviewee	Answer	Keywords
Int-01	There is something that I see with banks. That the **OpenBanking Concept** is **coming**. So, they are more open to **open up their own services to their partners**. These banks manage a lot of data. They are slowly opening up and a chance to monetize it. It is like **Banking-as-a-Service** that allow other organizations to use it. Personally, I did not experience it yet. I agree that the o**n-premises datacenter is unsustainable**.	**OpenBanking** **Ecosystem** **Banking-as-a-Service**

Int-02	The **sustainability** is **not** a **goal** at the **moment** for a **bank**. For example if a service on a cloud is more green IT compared to on-premises, i**t does not matter for a bank**. Their **top priority** is the **security**. The two main concerns for a bank when they want to **migrate** to cloud are **security** and **cost**. The goal is not to get greener, the goal is **reduce** the **cost** and **improve security**.	**Cost Reduction**
Int-03	I think all their **decisions** are based on **financial decisions instead** of any **sustainability** decisions. If we got back 4 or 5 years. I think **ESG** had not reach this **level** of **importance**.	**ESG**
Int-04	In the US, I did not see much about **sustainability**. There are some legislation in the US and Canada that we might see the influence of sustainability on cloud decisions. I am hearing from my colleagues in **Europe** that this is a **big topic** in **Europe** because of the **regulatory environment** around **ESG**. It is **regulatory requirement** that the bank has to demonstrate that they met the resilience and availability requirements. Sometime, we see the banks use the public cloud as a backup solution. You must make sure of the **cost** of **moving** the **data between** the **public cloud** providers. You must factor that in as a **part** of **your strategy**.	**Europe** **ESG**
Int-11		**Flexibility**

	Customers are **expecting** more **flexibility** from **banks**. And also the **suppliers** of **applications** to the **bank**. We **did** assessment for the bank application to **understand** if this **applications** could be **supported** on cloud by **third party**. Well to be honest, I was not there when the benefits analysis was done. I guess their development teams become more flexible to develop new applications and features without thinking about the backend. In the past they had to go the IT department and request servers. With the cloud, they request VMs and within 20 minutes or hour, they can have the requested environment to start working. This also lead to cost reduction. However, you still need to ask them after 4 or 5 years.	**Suppliers**

Q7:

What are the reasons for adopting multi-cloud project?

Q15:

What are the benefits of the project?

Interviewee	**Answer**	**Keywords**
Int-01	I think the **Time-to-market** and in general the adherence to **DevOps** principles have been more faster and easier with cloud adoption. The cost is also come down because they can **auto scale up and down based on usage**. I think these are the two big benefits. I think more governance are needed to make sure the right services are used in the right manner because within the cloud there are different tiers of services. You can use the premium tier or the stand tier. I think **cost optimization** is an	**Time to Market** **DevOps** **Cost Reduction** **More Governance**

	exercise that they need to focus on. Sometime people deploy premium tier for a service that is available in the standard tier. And also **automate process** to optimize the deployment. The **CCOE do trainings** all over the year. They need to look into **how to train and re-skill people**. For **each vendo**r they go to, they always **have an alternative for it**. For AWS, Azure is the **cloud exit strategy**. And the opposite. So, whenever a vendor is onboarded, an alternative is also chosen that will be the choice of cloud exit strategy. We developed all the infrastructure using **Terraform**. Terraform works for Azure, AWS, Google Cloud, and Alibaba. It is like **one syntax for all of them**. It is easier than using the **cloud native tools** that can lead to **vendor-lock in**. Generally, it is a good idea to **avoid cloud native tools**, then the **cloud exit strategy is easier**.	**Cost Optimization** **Cloud Cost Education** **Process Automation** **Re-consider Cloud trainings** **Cloud Exit Strategy** **Consider Alternative Cloud Providers** **Terraform** **Cloud-agnostic tool** **Cloud native tool** **Vendor-lock in**
Int-02	Mainly the **agility** and **cost reduction**. Most of enterprises struggle with hardware. Traditionally, banks provisions servers on-premises takes weeks. On cloud, the provisioning is done within hours. There is a big improvement in **Time-to-Market**. And the cost is reduced. Also the enablement of **OpenBanking** for **exchange of data**.	**Agility** **Cost Reduction** **Time-to-Market**

	They want to use all the latest technologies to provide services better and faster to the customers.	**OpenBanking**
Int-03	They want to **reduce cost**, **improve provisioning** and **flexibility** to allow them to get **products quicker** to the market.	**Cost Reduction** **Flexibility** **Time-to-Market**
Int-05	The acquired company need to migrate to the private cloud of mother company and shut down their mainframe. **Mainframes** are **stable**, but **supportability** is a **limited**.	**Mainframe Supportability is Limited**
Int-11	That is the movement in the market and **reducing cost** and being more **flexible** are mean reasons for moving to the cloud. That was in the past. Now some organizations are moving away from public cloud to private cloud. But this movement that you can see in the recent years or 2. There several reasons for that. It more because many years ago that cloud is still a hype and less costly. In some cases, it is visible any more or providing the flexibility or control on the environment. Some of them are moving to private cloud where they can have more control.	**Cost Reduction** **Flexibility**

Int-12	The bank migrated to multi-cloud to get **cost savings**, **resilience**, **operational improvement**, and also **reduce time** to **market**.	**Cost Reduction** **Resilience** **Operational Improvement** **Time-to-Market**