Cloud Migration & Security

Case study of Rabobank

Cloud Migration & Security

Case study of Rabobank

by

Anshita Purwar

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Wednesday August 25, 2021 at 11:30 AM.

Student number:	5132371	
Project duration:	March 1, 2021 – August 31, 2021	
Thesis committee:	Dr R.M. (Robert) Verburg,	Values, Technology and Innovation
	Dr F.S. (Seda) Gurses,	Multi-actor Systems
	Oka Arntzen,	Rabobank

This thesis is confidential and cannot be made public until August 25, 2022.

TU Delft

Rabobank

Acknowledgements

This thesis report is the pinnacle of my time at the Delft University of Technology. My journey at Delft started two years ago to pursue an MSc degree in Management of Technology. As a result, I had the opportunity to learn about different aspects of looking at technological advancements. During this time, my passion for cyber-security never ceased to exist, which led me to pursue an internship as a security innovation intern at Rabobank. Rabobank provided me with an open opportunity to choose an advanced technology and analyze associated security challenges and risks. I wanted to blend my experience in cyber-security and cloud computing in this thesis project; hence, I chose the topic, ”Cloud Migration & Security - A case study of Rabobank”.

I would like to dedicate this thesis to my father, Akhilesh Kumar Purwar, who has motivated and pushed me at every step of my life. He is my constant source of inspiration and strength, and my two years journey wouldn’t have been possible without him.

Further, this project wouldn’t have been a success without the constant support of my supervisor Dr Seda. Her guidance and understanding inspired me to carry out this work during the global pandemic. I want to thank my mentor at Rabobank, Oka Arntzen. He has provided support and advice at every phase of my internship and thesis. Furthermore, I am genuinely thankful to my family and friends, who were there to make the work from home time enjoyable and stress-free. Finally, I would like to express my gratitude towards the assessment committee for their time and effort.

Executive Summary

Innovation can be defined as creating a better product or making a process more efficient. Organizations have been talking about innovation concerning process and product for a long time. The industrial revolutions in the history are a perfect example of innovation in action. Starting from the steam engine in the first industrial revolution to Industry 4.0 in the fourth industrial revolution, numerous advanced technologies have been developed. These technologies have led to huge changes in an organization, like technological development along with organizational transformation. This transition in organizations drive customer satisfaction but also anticipate challenges and risks. Out of these challenges and risks, security is one of the major concern for both customer and the organization.

Numerous organizations have been running their IT infrastructure on legacy systems, which pose multiple risks to the organizations like expensive and challenging maintenance, system patches from scratch, more vulnerability to malware attacks etc. These risks, along with technological advancements, push organizations to move to a more scalable, secure, productive infrastructure called cloud computing. This technology enables organizations to deploy different computing resources (networks, servers, storage, applications etc.) with minimal effort. In addition, the cloud comes with numerous benefits like reduced cost, speed, global-scale, productivity, better performance, reliability with data backup and security. All these benefits are the driving factors for organizations to adopt the cloud.

Adopting the cloud is not easy, as it is a massive technological shift for an organization. However, it enables changes in other aspects like organizational, economic, security, and ethical aspects. The process of shifting the legacy infrastructure to the cloud is called cloud migration. This process involves migrating the systems, processes and data to the cloud and could lead to services and business discontinuity. Therefore, organizations need to plan the migration process and strategies considering their current infrastructure.

Rabobank is a Dutch banking and financial services, with a primary focus on food and agriculture financing and sustainability-oriented banking. With its vast national and international customer base, Rabobank understands its impact on the economy. The advanced digitization has also touched Rabobank, and they are also planning to move most of their services to the cloud. Being a financial institution, the organization stores and processes sensitive and confidential customer data. However, migrating to the cloud would lead to specific challenges, operational difficulties like an incompatibility between the legacy and cloud system, difficulties in data migration and integration, and change in the process. These would impact the organisation's security by causing data loss, data theft and authentication and authorization issues.

Various researchers and organizations have done research to improve and advance the migration process, but they focus on the above-mentioned technical challenges. However, there could be non-technical challenges like lack of resources, knowledge and skills, and stakeholder conflict. These difficulties could lead to security risks but have not been considered by many.

This thesis addresses that research gap and presents a case study of challenges faced by an organization in migration, with Rabobank as the use case. In this study, both technical and non-technical challenges have been considered and the security risks impacted by them, leading to a solution to those challenges.

The problems statement is tapped by answering the following research question and sub-questions:

How can an organization mitigate diverse challenges and security-related risks triggered in the process of cloud migration?

There is more information needed to answer the central question. For this following, research questions have been defined:

RQ1: What are the various factors an organization considers for the selection of a cloud service provider?

RQ2: Who are the various stakeholders involved in the process of cloud migration?

RQ3: What are the different phases in the process of cloud migration?

RQ4: What are the security-related risks and challenges faced by stakeholders in the various stages of cloud migration?

RQ5: How can an organization develop a tool to mitigate those challenges and security risks?

RQ6: To what extent would this tool be feasible to handle the security-related risks?

The research methodology starts with a systematic literature review to understand cloud computing, its benefits, and different cloud deployment models. The literature on cloud migration processes, strategies, and risks and challenges provided an overview of ways to migrate to the cloud. A study was done on the technology adoption model, and as per the research objectives, people, process & technology framework was considered for further analysis. The literature study suggested that researchers focus mainly on technical challenges and security risks impacted by them.

This was followed by case analysis of Rabobank, their cloud journey, innovation model, and cloud migration processes and strategies. It is essential to understand the different stakeholders involved in migration to analyze the process in a better way.

To answer the fourth research question, a multi-method approach was used to study the problems and dangers an organization faces. First, group interviews and individual interviews were conducted with the primary stakeholders. The output of these interviews resulted in three aspects: challenges faced, security and other risks and requirements of the users. First, the difficulties identified highlighted the importance of non-technical factors and the security risks triggered by them in the migration process. Second, the requirements gathered were categorized and prioritized using the Shared Requirements model and the MoSCoW method. The shared requirements model has been derived from the shared responsibility model that CSPs use to divide the responsibilities of the systems between the customers and themselves. Finally, the identified challenges and risks were compared and validated with the literature review and experts. The three outputs have been summarized in the table below:

The requirements after categorization were translated into a prototype called Cloud Catalyst. The prototype had four main features, knowledge base, information centre, planning & stakeholder management and learning. These features have been mapped out from the gathered user requirements. A concept was ideated to enable a proper knowledge management system, open communication channels between the stakeholders, continuous feedback, adequate planning and resource allocation in the migration process.

Finally, Cloud Catalyst as a concept, was evaluated by conducting individual interviews with the key stakeholders to understand its usability and feasibility. The results revealed that teams are looking forward to such a prototype to assist them in every migration process. Furthermore, the teams agreed and validated the outputs of data analysis and agreed to the design of such a platform. Along with this, the study reflected upon the challenges faced by teams at a micro-level and made other stakeholders aware of these concealed challenges and needs.

Because of the small and similar sample size, the current COVID-19 situation, and the flaws in the prototype design, this study has some limitations. However, the research provided some useful insights and findings for Rabobank, as an organization, to look into.

List of Tables

List of Figures

Contents

1 Introduction

1.1. Background

The word *Innovation* is the most acclaimed word in the last decade. It can be defined as creating better or efficient processes or generating the ideas or culture that will lead to such changes [21]. Thus, innovation can be categorized as process and product innovation. In addition, numerous factors drive innovation within organizations like customer satisfaction, leadership and supportive culture, cultivating an organization's strategic fit with its environment and enhancing the various economic, relationship, and product performance outcomes [17].

The industrial revolutions in history is a clear example of innovation in action. The invention of the steam engine in the first industrial revolution to the creation of the Internet in the third industrial revolution is all examples of product innovations that triggered process innovations in organizations. Internet, along with the Internet of Things (IoT), has led to the rise of numerous advanced technologies like artificial intelligence (AI), machine learning (ML), and cloud computing, and smart technology, accelerating to the fourth industrial revolution or Industry 4.0. These technologies have led to considerable transformations in all aspects of an organization. The rate of technological development is exponential; therefore, the rate of challenges and risks are also anticipated with these developments [52]. These challenges and risks pose various concerns to the organizations, like security issues, privacy issues, data storage challenges. Out of these, security is one of the primary concerns for everyone.

Consider the example of the banking sector, the Internet and digital transformation has changed how traditional banks work and reinvent how these banks engage with the customers [69]. Banking organizations use advanced technologies like APIs, artificial intelligence, machine learning, etc., to develop this new banking system and provide engaging and personalized solutions to their customers. Banks have developed attributes like support multiple sales channels, open platform for bank partners, self-learning and continuous improvement, mobility on the go, enable new integrations with other digital platforms and next-generation communication [69]. But with these features, risks like system and data security also increase.

The most significant transformation comes from how the organizations design and develop their information technology (IT) systems. Numerous organizations have been running their IT services on legacy systems for a long time now. Legacy systems can be defined as "mission-critical systems with monolithic code architecture having restrictions to archaic hardware, software and are short of resources in terms of skill sets, documentation" [28]. These systems are complex and the process to change them is risky and costly. With the new definition of technological attributes, legacy systems will create problems for the organizations and the customers. These systems were developed using no longer-used technologies; hence, maintenance is difficult and expensive. Legacy systems are highly complex, making it difficult for them to be flexible with technological advancements [61]. Hence, organizations consider migration of legacy systems to the cloud as a way of modernization [28].

Organizations vision cloud computing as a critical business strategy to mature their legacy systems to cloud-enabled infrastructure [5]. Cloud computing has many benefits from a technical perspective (increased scalability, interoperability, efficient resource management) and financial perspective (pay-per-use model and reduced service maintenance cost) [5]. In addition, it increases the productivity of the organization [5].

Cloud computing can be defined as 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” [26]. The term ”cloud computing” was first introduced in 1996 about the distributed computing [74]. In the mid-1990s, the concept started turning into services with Google and Microsoft investing in the design and development of cloud environments [74]. This initiative led to the cultural shift in various industrial sectors. In 2006, Amazon joined the market and launched Elastic Compute Cloud (EC2), combining virtualization and computing, bringing a revolution in the domain of Information Technology (IT) [74]. There are different types of service models, and deployment models within the cloud explored further.

Numerous organizations migrate to the cloud and choose the service and deployment model according to their existing infrastructure and requirements. Cloud migration can be defined as ”the process of moving data, applications, other business elements from an organization’s computer to the cloud” [34]. Different processes perform the migration based on the requirements, and various stakeholders are involved based on their expertise. As a result, multiple researchers and organizations have come up with different methods like Gartner’s 5Rs (Rehost, replatform, refactor, retire and retain), Amazon Web Services (AWS) 6Rs (Rehost, replatform, refactor, retire, retain and repurchase) ([9], [56]), and different frameworks as mentioned by [5], and [28].

When planning for migration, there are various factors that organizations need to consider, and these can be divided into two categories: technical and non-technical. For example, organizations focusing on customer-centric solutions must focus on data migration and look after data integrity and security. This is because they store customer data and sensitive customer information that need to be kept safe and secure. On the other hand, the non-technical challenges could be the unavailability of a cloud migration strategy, less prior expertise in the cloud environment, and organizational preparedness for new technology [70]. Various researchers have also explored these challenges and found out that issues like choosing the right vendor, process change, lack of knowledge, regulatory problems, data breaches, malware attacks and many more are there ([53], [37]). Out of these data security, attacks on infrastructure, malware attacks are the major concerns for the organizations. Hence, security is the biggest concern for any organization in the process of cloud migration.

1.2. Problem Statement

There are various ways to tackle security-related challenges in the migration process. Researchers have explored the risks and ways to reduce security risks, such as a risk assessment framework that assesses the factors concerning cloud and facilitates them to lower the effect of risk [31]. In addition, a phased plan to migrate the services and data can be implemented, like cloud requirements, cloud preparation, and cloud migration [43]. These methods are effective, but most researchers overlook organizational factors like business model, governance model, and organizational change that lead to the disorganized cloud migration process implementation. The process and the planning needs to be done as per the dynamic needs and requirements of the organization migrating to the cloud.

To understand the needs and requirements from an organizational perspective in cloud migration, the research will be conducted with Rabobank. Rabobank is a Dutch banking and financial services company located in Utrecht, Netherlands. Rabobank is also planning to move most of its services online and invest more and more in innovation [42]. Among the numerous technologies, they focus more on moving their infrastructure to the cloud for its many benefits like easy accessibility, scalability, and efficient collaboration. Thus, they are in the transition phase, or as they call it, ”old to cloud”, initiated with Office 365 in the cloud [40].

Rabobank faces numerous risks and challenges going from ”old to cloud” as an organization in the transition phase. These challenges could be operational, such as incompatibility between the existing legacy system and new cloud environment, change in the process, difficulties in data integration, or organizational like lack of resources with the proper skill set, people not prepared for migration, change in governance model etc. In addition, they can affect the organization's security like data loss, data theft, authorization and authentication issues.

Researchers have provided solutions to the operational problems faced by an organization, but the security risks still exist and lead to monetary troubles. It also points to the research gap that researchers and organizations focus mainly on technical challenges, but non-technical challenges also cause security risks. Therefore, an organization must analyze the operational(technical) and organizational (non-technical) challenges in an innovative way to keep them secure.

The problem statement can thus be summarized as follows: The process of cloud migration is not secure. Numerous technical and non-technical challenges affect the security of an organization and its customer base. Therefore, the security risks posed by these challenges need to be analyzed and mitigated using innovative tools or measures.

1.3. Research Objective

As mentioned earlier, advanced transitions in technology play an essential role in the smooth running of any organization. The radical growth in information and communications technology (ICT) has led to changes in everyone's lifestyle, so organizations need to develop advanced services to accommodate such changes. For example, the introduction of the Internet and browser led to e-banking, and the extensive use of mobile phones daily led to mobile banking. As a result, account owners can handle all aspects of their accounts over the Internet rather than visit the bank (Innovations in the Banking Sector 2021, 2020). Along with this, the banks are more focused on providing customer-oriented solutions, with different themes like financially healthier living, starting a business, baby on the way, live together, etc. [62].

With such crucial technology shifts and changes in the technology landscape, organizations face numerous risks. Advanced systems consist of layered infrastructure compromising computers, networks, databases, servers, business and customers' information that needs to be protected from cyber-attacks [2]. These developments have been happening over the years, and organizations rely on legacy infrastructure. There are many risks of the legacy infrastructures, like hindering innovation and being more vulnerable to malware attacks [32]. These attacks happen in various forms like identity theft, supply chain attacks, ransomware, ATM malware and jackpotting, and synthetic fraud [54]. Moreover, some parts of the legacy infrastructure have no patches, or the upgrading must be done from scratch [32]. Hence, the legacy infrastructure creates an insecure system and blocks a company's growth in the emerging market.

With the increasing technological advancement, organizations need high computing capability, scalability and more secure systems [29]. Cloud computing provides such benefits along with being cost-efficient, more productive and reliable. These advantages are convincing many organizations to move their legacy infrastructure to a cloud environment. But the migration to cloud services is not easy. There are numerous challenges that an organization faces in the migration process. The unique requirements of cloud, elasticity, multi-tenancy that are not attributed to the legacy systems raise challenges for organizations to adopt the cloud system [29]. Most researchers have focused on the technical difficulties. Still, an organization needs to alleviate non-technical challenges like organizational changes, operational barriers, process and skills advancement, and the above-mentioned technical challenges. Additionally, the researchers also fail to analyze the security risks triggered by these non-technical challenges.

As a result, this master's thesis aims to investigate and analyze both technical and non-technical concerns about cloud migration and the security threats posed by these concerns. Further analysis of the

severity of the risks, multiple stakeholders involved, and design an innovative and strategically relevant tool and practices to mitigate those risks.

1.4. Research Questions

To achieve the research objectives, research questions should be defined. The central question for this problem is:

How can an organization mitigate diverse challenges and security-related risks triggered in the process of cloud migration?

There is more information needed to answer the central question. For this following, research questions have been defined:

RQ1: What are the various factors an organization considers for the selection of a cloud service provider?

RQ2: Who are the various stakeholders involved in the process of cloud migration?

RQ3: What are the different phases in the process of cloud migration?

RQ4: What are the security-related risks and challenges faced by stakeholders in the various stages of cloud migration?

RQ5: How can an organization develop a tool to mitigate those challenges and security risks?

RQ6: To what extent this tool would be feasible to handle the security-related risks?

1.5. Thesis Outline

The thesis is organized in the following way: Chapter 2 discusses the research methodology that will be used to conduct this research study. Next, Chapter 3 involves an analysis of the literature review by covering essential topics of cloud computing, cloud migration process and techniques, and process improvement modes. Next, Chapter 3 examines the literature required to answer the first two research questions. Next, Chapter 4 discusses the case analysis answering the research's first four research questions, focusing on the use case of Rabobank. Then, Chapter 5 establishes the groundwork for solving the fifth research question by summarizing the case study findings. Finally, Chapter 6 reflects on the thesis by discussing different aspects of research.

2

Research Methodology

This chapter explains the different research methodologies used for this research. Section 2.1 discusses the literature review, and section 2.2 focuses on the case study as a research design, along with different methods of data collection. Section 2.2 also explains the motivation of choosing the use case and the introduction to Rabobank. Finally,Section 2.3 summarizes the research design for the study.

2.1. Literature Review

The building block of academic research is to build the research on the existing knowledge [71]. But the knowledge is growing at an exponential rate and is fragmented and interdisciplinary, which makes it challenging to keep track of cutting edge research [71]. This paves the way for the literature review as a research methodology and would be the best tool to answer a few research questions. The literature review is conducted to evaluate the shape of knowledge in a specific research area [71]. It can be used to develop hypotheses, determine research gaps, or a theory/concept development.

Cloud computing was introduced two decades back, and since then, various researchers and academics have analyzed and explained various aspects and ways to exploit this technology. It is also the central point of this research; hence, a literature review to understand cloud computing as a concept and the various variables researchers consider when choosing a cloud service provider (CSP) is essential. Furthermore, the research objective is to analyze the diverse challenges in cloud migration; hence, understanding the migration process and the various stakeholders are crucial. Further, the existing research on the challenges and risks analyzed by researchers and organizations is essential. This will be used to validate the issues identified in this research.

The process of cloud migration and the stakeholders will vary depending on the organizational factors. Hence, to understand the problems in migration at an organizational level, a case study is considered a research methodology and discussed in the next section.

2.1.1. Search Criteria

The searches for literature review were performed in the many academic databases mainly, Scopus, Google Scholar, Science Direct, Emerald Insight and IEEE. In the following paragraphs, the search description and selection criteria have been explained in every research step.

The primary search was done using the keywords ”cloud computing AND security” to get an initial idea of the research published on cloud computing from a security point-of-view. However, since cloud computing is an advanced technology, many researchers have analyzed this technology from a security perspective. Therefore, the search was refined by adding more specific keywords like ”Cloud computing and security challenges” to understand the concept of cloud computing and its various challenges.

Multiple combinations were searched mainly on Google Scholar to understand the various aspects of cloud migration, leading to keywords like ”cloud migration AND process”, ”cloud migration AND strategies”, ”cloud migration AND challenges”, and ”cloud migration AND security risks”. These queries provided sufficient literature to understand the various methods researchers have considered migrating to the cloud and identify the research gap.

A few articles and blogs were also considered to understand the services provided by various cloud service providers like AWS and Microsoft Azure. The blogs were also referred to understand the definition of a few terms and get the latest statistical numbers for the study.

2.2. Case Study

The research layout has been developed using the methods of a case study. A case study is used as a research strategy when there is an investigation of a ”particular contemporary phenomenon within its real-life context using multiple methods of data collection [78]. The research questions for the case study has been defined in Section 1.4. The case study of Rabobank is done using various methods to gather information about the organization, its cloud journey and the migration process.

This is qualitative research, and a multi-method data collection approach has been used for data collection, including documentation, group interviews and semi-structured interviews.

2.2.1. Use Case - Rabobank

Rabobank is a Dutch banking and financial services company located in Utrecht, Netherlands. Their primary focus is on food and agriculture financing, and sustainability-oriented banking [62]. The mission of Rabobank is to ”grow a better world together”, and they have close to 9.6 million customers. As a banking company, Rabobank also understands the impact they have on the country’s economy. With an active workforce in thirty-eight countries, they provide a range of financial services worldwide [62]. The supervision of Rabobank is done by the European Central Bank, De Nederlandsche Bank (DNB) and the Financial Markets Authority (AFM) [62].

As an organization, Rabobank invests its resources in building better products for its customers. The bank has created an Innovation Board to prioritize the strategies concerning digitization and innovation [35]. Rabobank has also set up a Tech Lab to take initiatives with the state-of-the-art technologies like quantum computing and blockchain, and research into the four pillars, trend-watching, research, support and advice [35].

As mentioned earlier in Chapter 1, security is the biggest concern of organizations, along with these exponential developments. Similarly, Rabobank, a financial institution, has significant concerns about the security risks caused by these advanced technologies. Therefore, as a part of the organization, I analyzed one of these technologies and the challenges and security risks associated with them. As a result, I observed that Rabobank uses cloud computing and migrating its current infrastructure to the cloud.

With their decision to migrate to the cloud, they also faced challenges in the process. One of the biggest challenges in designing an effective process and strategies to migrate their infrastructure is the various regulations and compliance a bank must follow. The other challenges occur with the implementation of the migration process, as there are multiple stakeholders involved. The migration process has to be monitored responsibly as this could lead to business discontinuity for Rabobank. After initial observations, I found out that multiple teams faced challenges; hence, the scope of the research was decided to analyze those challenges and security risks triggered by them, with Rabobank being the use case.

2.2.2. Research Methods

Documentation

The documentation includes multiple sources of information like emails, memorandum, letters, minutes of meetings, reports of the events, administrative documents like proposals, progress reports, and internal records [78].

For this case study, the documentation specific to Rabobank has been analyzed. Furthermore, various reports concerning the cloud journey of Rabobank, its cloud migration process and strategies have been analyzed and used in this research. These reports can be viewed repeatedly, are unobtrusive, and provide a broad overview of the events and settings at Rabobank [78]. Hence, this method will be used to answer the third research question.

Group Interviews
Group interviews consist of several participants, and various points are raised concerning the central matter of research [65]. This is beneficial for such an exploratory study, where a dynamic group can generate numerous concepts and evaluate them, thus explaining and exploring different ideas. Another reason is that various researchers have analyzed cloud migration from other aspects, including security, in the literature review. Therefore, the interviews will provide a clear picture of Rabobank as a use case of this case study, and the answers will be focused on organizational context.

Interview method and content

Group interviews will be conducted using a video-conferencing technology for data gathering (Microsoft Teams). The interviews are scheduled for approximately 30 to 60 minutes. The technique used for the group interviews was Appreciative Inquiry. This technique is prevalent at Rabobank for conducting exploratory research interviews.

Appreciative Inquiry (Ai) is a process ”inquires into, identifies, and further develops the best of what is in organizations to create a better future” [20]. The process analyzes the organizational challenges and issues by looking at what is working well, instead of studying the problems directly [20]. This method has been criticized for not addressing issues in an organization adequately. However, it does address the problems by asking the participants what is going well and what more they want from the organization to improve the working or a process [20]. Hence, the main aim of group interviews is to understand the current state of cloud migration at Rabobank and analyze the challenges and risks in the ongoing process. Additionally, gather the requirements to understand participants expectations from the organization. This will be used to answer the third and fourth research questions.

This method starts with a topic introduction and then revolves around a central question. For this research, the central question was, ”*What opportunities and possibilities do we see to mitigate security-related risks in cloud migration?*”. Table 2.1 below describes the various steps in this process, questions, and the output.
Interviewee selection

To shortlist participants for the interview process, a selection criterion was developed. Since the main focus of the research is on understanding the challenges in the cloud migration process at Rabobank, the different factors and resources at Rabobank need to be considered. The stakeholder analysis, which will be done as a part of the case analysis, will help identify the candidates for the interview.

The participants will be selected based on their varying technical skills and different academic backgrounds and study fields. This is done to establish a difference in how they perceive the existing process and technology. This also reveals their level of understanding and their grasp of knowledge on adopting this new technology.

Different teams will be considered to participate in the group interview process. The teams will be chosen with specific criteria, like teams that migrated to the cloud and are currently in the migration phase. The teams or participants for group interviews are not related directly to cloud usage, as they are participating in the migration process to achieve the organization’s collective goal. The number of participants will vary from 2 to 10, as this would provide a vast amount of information about the process and the challenges.

Steps	Question	Expected output
Define	What is the first thing that comes to your mind when you look at the central question?	Innovative measure and socio-technical tools to secure cloud migration
Discovery	Elaborate your experience with the associated word or text regarding the central question.	Experiences with the current cloud migration process
Dream	What would be the ideal situation in your dream if there were no obstacles?	Gather requirements about the new possibilities
Design	Who and what is needed to realize this dream?	Translate the requirements into actionable tools and measures
Deploy	What is the first step that can be taken to create an impact?	Feasibility and distribution of tools and measures

Table 2.1: Feasibility and distribution of tools and measures

Method of Analysis

Since this is a multi-method qualitative research approach, a coding analysis will analyze the results. It is the most extensively utilized method of analysis for exploratory research. Qualitative data analysis is done by following three steps – data reduction, data display, and concluding [67]. The data is reduced in three stages by coding analysis [16]. The first step is to process the data, i.e. the interview transcripts being coded, into than getting combined into groups with similar codes using axial coding [16]. Then, these categories are analyzed and abstracted into theories, hypotheses and concepts. The research study involves a deep understanding of the data; hence, a line-by-line analysis will be performed.

The initial phase of developing codes and categories will be done deductive, and then the inductive process will be done. Therefore, the initial list of codes will be generated from the literature review and keywords, and then these specific codes are used to analyze the data for Rabobank. The advantage of adopting existing codes and categories is that it allows you to build on what you already know. Therefore, a similar approach is followed for the analysis of this research.

Structured Interviews
Structured interviews are conducted when the requirements and needs of the research are known beforehand. The questions are designed with the format, introduction, a set of topics and suggestions for probing questions [67]. These interviews will be conducted to evaluate and validate the data gathered from the research. This method will also convene feedback from involved stakeholders concerning the solution presented in further chapters. Hence, this will be used to answer the last research question.

Interview method and content

Structured interviews will be conducted using a video-conferencing technology for data gathering (Microsoft Teams). The interviews are scheduled for approximately 30 to 60 minutes. The participants will be shown a presentation summarizing the information from data analysis like the research question to provide context to the research, identified challenges, security risks caused by those challenges, the requirements prioritization, requirements to solution mapping, and lastly, the description of the solution.

The main aim of these interviews is to capture the input of the participant teams regarding the research objective. Another objective is to fill in the missing information that participants might add to the data presented. These interviews will also ensure participants had any queries or additional requirements

for designing and implementing the solution.

Interviewee selection

These interviews will be conducted with the primary stakeholders in the migration process at Rabobank, for example, the teams that participate in the migration process. 1 to 2 participants from each group will be interviewed for feedback.

Method of Analysis

The collected data from the interviews will be transcribed into scripts. Since the participants will be asked about the feedback and additional comments on the solution and the research overall, relevant feedback will be highlighted and categorized using applicable codes and categories. The categories are pre-defined; for example, if the participant agrees with the identified challenges, the category would agree. Similarly, the defined types are: agree, disagree, suggestion and feasible.

2.3. Research Design

This study is an exploratory qualitative case study, with Rabobank being the use case. Different research methodologies will be applied to answer the well-defined research questions in Chapter 1

The first step is to identify the various factors organizations considers to select a CSP and the multiple ways to migrate to the cloud. This can be answered using the literature review. The second step is to identify the stakeholders involved in cloud migration, which can be done by reviewing the documentation provided by Rabobank. The third step is to identify and analyze the security risks and challenges and gather requirements for the solutions. This will be done by conducting group interviews with the teams undergoing the migration. The next step would be to translate those requirements into actionable and feasible solutions and verify and validate those requirements with the experts at Rabobank. Figure 2.1 below shows the summary of the research methodology:

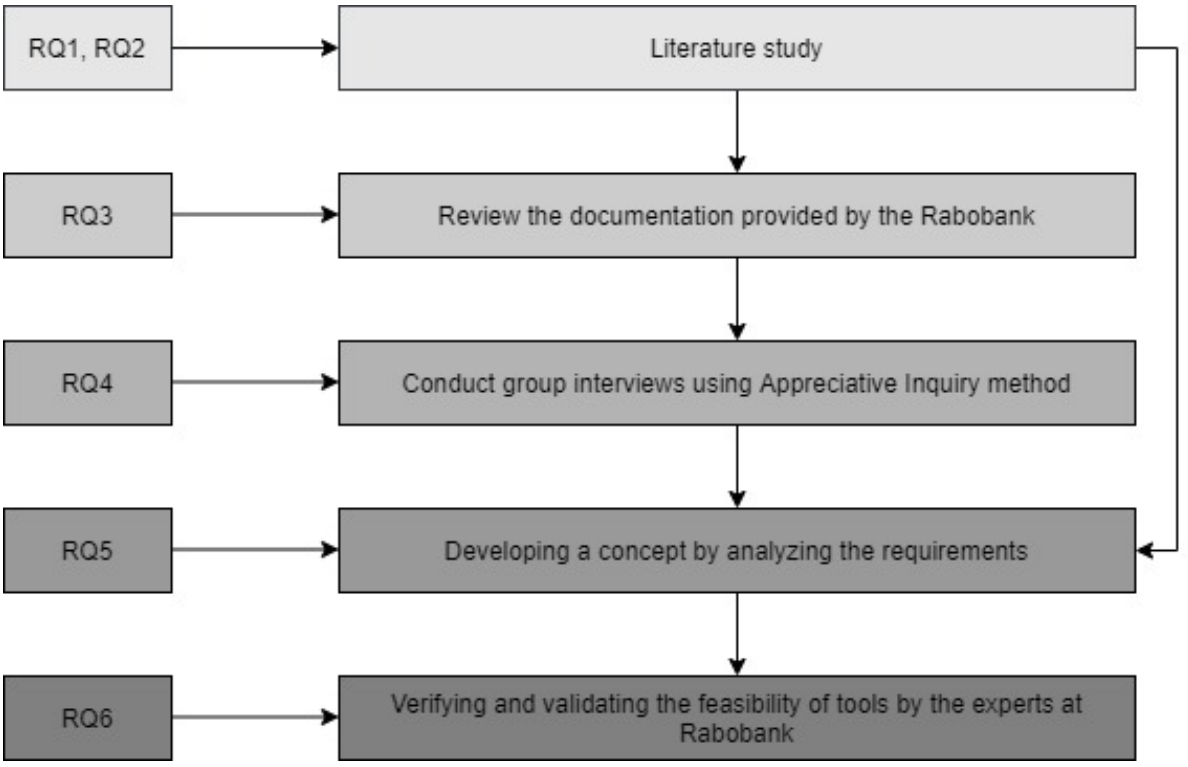

Figure 2.1: Research Design

3

Research Findings - Literature Review

In this chapter, the literature relevant to this thesis is reviewed. First, Section 3.1 discusses the basics of cloud computing, its benefits and service and deployment models. Next, section 3.2 discusses the various factors organizations consider for cloud service provider selection. Next, Section 3.3 discusses the process improvement model used to analyze the methods and strategies for the cloud migration process. This is followed by exploring and analyzing the different phases of cloud migration in section 3.4. Next, Section 3.5 discusses the numerous risks and challenges in the process of cloud migration. Finally, Section 3.6 summarizes the literature study and the research gap in the study.

3.1. Cloud Computing

3.1.1. Definition

Cloud computing has emerged as a new business model to provide a better computing environment in the digital era. It can be defined as 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” [26]. There are numerous benefits of using cloud computing as shown in Table 3.1:

Benefits	Description
Cost	Defeats the purpose of buying hardware and software and setting up on-site data centres, thus reducing the capital expenses for an organization
Speed	Services are provided as self-service and on-demand so that numerous resources can be allocated with a few clicks
Global-scale	Scaled elastically, which means the bandwidth of services can be set as per the requirements, and the services can be accessed from any geographic location
Productivity	Various tasks for setting up and maintaining the on-site data centres done by the IT department can be reduced
Performance	A global network of computing services running in secure data centres helps organizations reduce network latency for applications
Reliability	Data backup, data recovery, and business continuity are more accessible as data can be mirrored to multiple sites on the network

Security	Set of policies, technologies, and control to strengthen the data's security, applications and services running on the cloud

Table 3.1: Benefits of Cloud Computing [77]

3.1.2. Service Models

Cloud computing has been categorized into three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), as shown in Table 3.2. These services are generally differentiated based on the control a user has on the service. For example, SaaS is entirely managed by the cloud service provider, whereas in PaaS, the end-user has authority on the application and data layer.

Service Model	Description	Example
Software as a Service (SaaS)	A hosting environment where cloud consumers release their applications, which can be accessed through networks from various clients (e.g. web browser) by end-users	SalesForce, Google Mail, Office365
Platform as a Service (PaaS)	A development platform imitating the software lifecycle, providing cloud consumers with the freedom to develop and deploy their applications. It consists of infrastructure, including programming environment, tools, and configuration management	Google App Engine and AWS Elastic Beanstalk
Infrastructure as a Service (IaaS)	Infrastructure like processing, networks, storage, and computing resources virtually, using virtualization	AWS S2, EC2

Table 3.2: Service Models in Cloud [23]

3.1.3. Deployment Models

Cloud services can be deployed in four ways based on the demands and requirements of an organization: Private cloud, public cloud, community cloud, and hybrid cloud. Table 3.3 summarizes the four deployment models:

Deployment Model	Description
Private cloud	Operated within a single organization and managed by a single party, either the organization or a third party. It provides complete control to the organization regarding resource utilization, data privacy and trust.
Public cloud	Available openly to all the cloud consumers, and cloud service providers (CSPs) have full ownership of the resources, policies, profit, costing and charging model
Community cloud	When multiple organizations collaborate and share the same cloud resources, policies, requirements, values and concerns to form into a degree of economic stability and democratic equilibrium
Hybrid cloud	Combination of two or more clouds (private, public or community) and is bound together by standards to enable the use of technology and data portability

Table 3.3: Deployment Models in Cloud [23]

3.1.4. Shared Responsibility Model

It is made clear in the problem statement that security is a significant concern of organizations. The traditional model or legacy system relies on the end-user for the complete security of the infrastructure, which puts a considerable responsibility on the end-user. The cloud providers have highlighted this concern. Cloud service providers (CSPs) are the companies that provide a cloud-based platform, infrastructure and various services on the cloud. They understand that complete security of the infrastructure is a massive responsibility for the organizations; hence, they proposed a shared model between the CSP and the customer, called the shared responsibility model. Different CSPs have a clear, defined picture of this model for their customers. The prominent CSPs Amazon Web Services (AWS) and Microsoft Azure have developed their versions of the shared responsibility model, discussed below.

AWS divides the concept of security into two categories, security ”of” the cloud and security ”in” the cloud, explained in Figure 3.1 [72]. The security of the cloud is the responsibility of the CSP, and it protects the infrastructure that runs on the services provided by AWS. On the other hand, security in the cloud is the customer responsibility and will be determined by the cloud services that a customer selects [72].

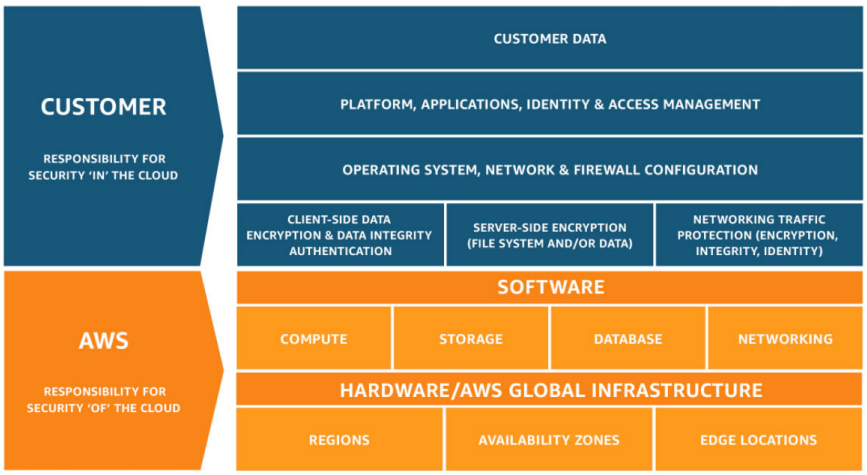

Figure 3.1: Shared responsibility of AWS [72]

Similarly, Microsoft Azure has divided the responsibility of the security of the services based on the customer's model, IaaS, SaaS, or PaaS, as shown in Figure 3.2. The customer always has the responsibility of their data, endpoints, account and access management in Azure [46].

Putting this model in practice means that the end-user and the CSPs do not have control over the responsibility of each other when it comes to security. But the end-users can access the CSPs audit reports to verify that their systems are secure and complying with the latest regulations [19].

3.2. Selection of Cloud

3.2.1. Cloud Service Providers

There are CSPs in the market that offer multiple services with similar functionalities like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Salesforce, IBM Cloud Services, Oracle Cloud, Dropbox etc. [1]. These CSPs provide numerous services in different categories like AI and Machine learning, Management & Governance, security, blockchain, compute, containers, storage, databases, identity, Internet of things etc. Table 3.4 shows two major cloud service providers, AWS and Azure, in a few categories. These CSPs keep developing new categories based on the dynamic customer requirements.

Figure 3.2: Shared responsibility model of Azure [46]

3.2.2. Selection Process

As cloud service is becoming popular amongst enterprises, organizations, and small & medium businesses, choosing the right service provider is a practical issue. As a result, several researchers have designed frameworks and parameters to select the right service provider.

In the research of Li et al. [50], various cloud services have been discussed, like elastic compute clusters, persistent storage service, intra-cloud network, and wide-area networks for a generic online computation platform. The authors found multiple metrics to measure the performance of each component, as shown in Table 3.5.

In the research of Lang et al. [47], authors used the Delphi method to explore the quality of service (QoS) attributes to be considered for selecting a CSP. The authors found numerous attributes and categorized them into two categories, technical and managerial, as shown in Table 3.6. The authors also found out that the QoS attributes have evolved based on the following significant changes in the cloud market: the importance of increasing data protection, cloud customer's pursuit of value co-creation with CSP, the possibility of a decrease in CSP's opportunistic behaviour, and product uncertainty [47].

3.3. Process Improvement Model

It is clear from the research objective that the research involves analyzing challenges and risks in the migration process from an organization's view, rather than a generic perspective. Thus, the migration process improvement starts from the people, including analyzing stakeholders, communication and knowledge skills, then process, including identifying the gaps in the migration process and then defining technology to mitigate the gaps and challenges. According to this workflow, the framework suitable for this research would be the People, Process & Technology framework. It involves finding the right balance with the three aspects of this framework [59]:

- **People**
  - People know what and how to execute tasks, leading to identifying the key stakeholders and their responsibilities
  - Ensure that people have the proper knowledge & skills
  - People are motivated and engaged, leading to identifying the interest of stakeholders
- **Process**
  - Identify the processes to solve the problem
  - Identify the key steps, process variations, exceptions, inter-dependencies, and supporting processes

Category	AWS	Azure	Description
AI & Machine Learning	Sage Maker	Machine Learning	To train, deploy, and manage machine learning models regarding resource utilization, data privacy and trust.
Big Data & Analytics	RedShift	Synapse analytics	Enterprise Data Warehouse to run complex queries
Compute	Elastic Compute Cloud	Virtual Machines	Virtual servers to deploy and manage OS and server software
Containers	Elastic Kubernetes Services	Kubernetes Services	Deploy and manage containerized applications with Kubernetes
Database	RDS	SQL Database	To manage relational database services
Internet of Things	IoT	IoT Hub	Gateway to manage bidirectional communication with IoT devices
Identity	Identity & Access Management	Azure Active Directory	To create and manage users and groups and to control access

Table 3.4: Example of Services offered by CSPs [63]

  - Identify the key steps, process variations, exceptions, inter-dependencies, and supporting processes

- **Technology**
  - Identify the tools and measures to communicate and develop efficient processes
  - Understand the problem and solution requirements to finalize the right measure

The people, process, technology model will be used to analyze the requirements, design the solutions, and evaluate the feasibility of the solutions, as shown in Figure 3.3. The people aspect deals with stakeholder analysis and stakeholder management discussed in Chapter 4. The process aspect deals with analyzing cloud migration, strategies and the gaps, i.e. challenges and security risks triggered by those challenges in Chapter 4. Finally, the technology aspect deals with the requirement analysis and conceptualizes those requirements into a prototype, further validating the prototype's feasibility and scalability.

Service	Metric
Elastic compute cluster	Benchmark run time Cost per benchmark Scaling latency
Persistent Storage	Operational legacy Operational throughput Cost per operation Time to consistency
Intra-cloud Network	Path latency Path capacity
Wide-area Network	Wide-area network latency

Table 3.5: Cloud performance metric [50]

Technical Attributes	Managerial Attributes
Functionality	Legal compliance
Flexibility	Contract
Integration	Geolocation of servers
Control	Transparency of activities
	Monitoring
	Support
	Deployment model
	Test of solution
	Certification

Table 3.6: QoS attributes for selection of CSPs [47]

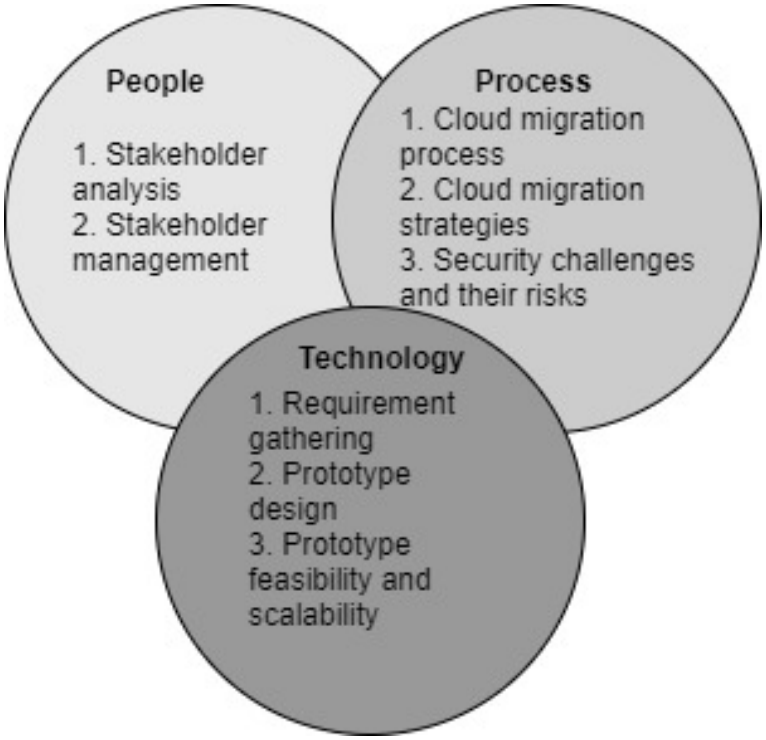

Figure 3.3: People, Process Technology for the analysis

This framework has been used as a primary tool to design the thesis structure, i.e. analyze the stakeholders, understand the process, identify gaps, and then provide a solution to rectify those gaps. It will be used to analyze the literature review and derive the observations in the later research phase.

3.4. Cloud Migration

3.4.1. Cloud Migration - Process

Cloud migration can be defined as ”a set of migration activities carried to support an end-to-end cloud migration” [29]. This process could lead to business discontinuity; hence, organizations need a plan for organizational and technological change. Therefore, various researchers, as well as organizations, have explored the process of cloud migration.

In the systematic literature review of [39], the authors found out that operational cost saving, application stability and efficient utilization of resources are the main motivational factors for organizations to move to the cloud. They also discussed the different ways to move to the cloud, like replacing data

and business layer to cloud stack, partially migrating a few components to cloud, migrating the whole application stack, and cloudify where an application is completely converted to cloud-enabled service. In addition, they have listed various steps of migration based on the type of migration [39]. The authors considered operational factors the drivers of migration; hence, the migration steps have been designed to focus on the data and business layer.

In the research of Zhao and Zhou [79], the authors discuss the various migration strategies for different service models of cloud, IaaS, PaaS, and SaaS. With IaaS, the plan would be to port legacy systems to the cloud using IaaS. For PaaS, the legacy system will be refactored as per the PaaS platform. Three sub-strategies have been devised for SaaS, replacing by SaaS, revising based on SaaS, and re-engineering to SaaS. The authors also compared the various strategies based on the migration workload and complexity, adaption and effect [79]. The migration strategies suggested by the authors are based on cloud service models, i.e. on the technology aspect of migration. However, these strategies do not consider the people and process aspect of *People, Process, & Technology* framework.

The banking sector is one of the most regulated sectors; hence, moving to the cloud needs to consider the involved stakeholders' regulations, compliance, and standards. In the research of Frațilă [27], the author described a framework to migrate from legacy model to cloud model. This framework accounts for the organization's governing policies, standards and regulations, and correlations between various organizational frameworks. It combines designing, implementing and operating a service migration from legacy to cloud [27]. This process does not consider the organization and individual readiness and is more focused on bringing organizational change.

In the research of N. Ahmad et al. [6], the author has defined five stages of cloud migration, namely, business assessments, technical assessments, migration strategy, migration planning, and execution and optimization. Table 3.7 shows the different steps discussed by the authors in the research:

Business Assessments	**Technical Assessments**	**Migration Strategy**	**Migration Planning & Execution**	**Monitoring & Optimization**
Workload assessment	Portfolio discovery	Rehost (IaaS)	Architecture recovery	Service monitoring
Compliance Assurance	Map dependencies	Replatform (PaaS)	Dependency check	Application monitoring & optimization
Security concerns	Cost-benefit analysis	Repurchase (SaaS)	Provisioning	Cloud resource optimization
Quality of Service levels	Decision on providers	Refactor (cloudify)	Pilot migration	Cost optimization
Performance predictions	Pattern-based approach	Rebuild (Cloud-native)	Data migration	Business continuity
Cost Analysis			Application migration	
Effort estimation			Integration	
Organizational readiness			Validation	

Table 3.7: Different steps in cloud migration

The framework suggested by [6] involves numerous aspects of an organization, and it mentions workload assessment and organization readiness. As it has been made clear from the literature review on cloud migration that the process leads to significant organizational changes like process changes, business model transition, governance model changes, and revision of regulations and standards for an organization. These procedural changes should start from people as per the *People, Process, Technology* framework as discussed in Chapter 2. Unfortunately, the frameworks or processes suggested by the researchers do not follow the flow of the improvement model.

People include both the individual who operates the technology and the process and the entire organization that bases the individual (Sorensen & Ing, n.d.). This aspect includes not the operation of technology but essential factors like role, job definitions, initial training, knowledge requirements, personnel development, skill requirements, reporting mechanisms, and knowledge, skills and attitudes (Sorensen & Ing, n.d.). These aspects are missing in the processes suggested by researchers, pointing to the research gap mentioned in Chapter 1. Instead, researchers and organizations jump directly to design a well-defined process and technology for the organizational change, which triggers risk for the organization.

3.4.2. Cloud Migration Strategies

Organizations begin to ponder about the migration strategy during the second phase of the migration process. The process involves determining their current environment, inter-dependencies in the present scenario, and the level of difficulty they would face in the migration [56]. The complexity of migrating existing infrastructure varies, depending on numerous factors. Hence, organizations need to come up with a strategy to migrate applications. Organizations like Gartner and AWS have come up with a list of migration strategies.

As mentioned in the research of N. Ahmad et al. [6], the migration strategies are called 5R's, and this is Gartner's strategy for organizations to migrate applications to the cloud [9]. The 5R's (Rehost, Replatform, Refactor, Retire, Retain) are summarized in Table 3.8:

Method	Description
Rehost	Moving applications from on-premises to cloud without modification (Lift & Shift)
Replatform	Moving the applications as it is, without a small amount of up versioning
Refactor	Transformation of non-cloud applications to a cloud-native application
Retire	Closing the redundant applications
Retain	Conditional migration as required, otherwise retain applications on-premise

Table 3.8: Migration Strategies, 5R's [9]

In the research of Orban [56], the author discusses the migration strategy suggested by Amazon Web Services (AWS), known as 6R's (Figure 3.4), which is an extension of Gartner's process. In addition, the author suggested an extra step in repurchasing (moving to a different product or platform) along with the 5R's of Gartner.

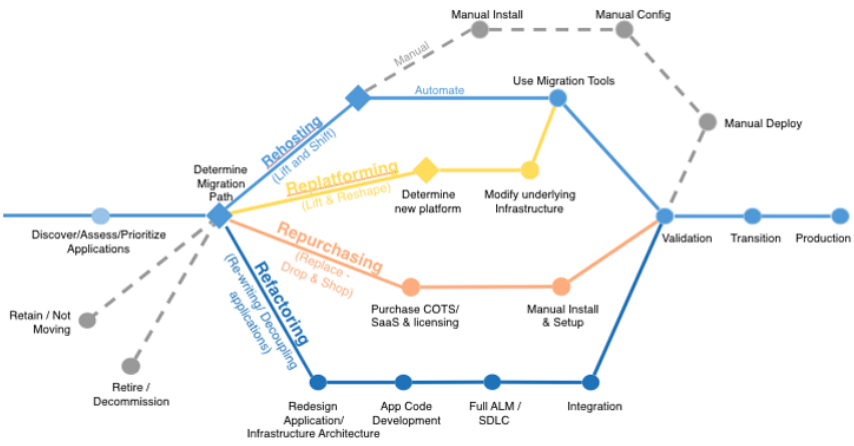

Figure 3.4: Six common application migration strategies [56]

3.5. Challenges & Risks in Cloud Migration

3.5.1. Operational Risks & Challenges

Cloud migration is the suggested solution to move out from the legacy infrastructure for the organizations. But this infrastructure has some unique characteristics, which introduces risks and challenges in the migration process. Many researchers have analyzed these issues, risks and challenges and provided solutions to reduce these risks, which has been summarized in Table 3.9:

Research Paper	Challenges	Suggested solutions
[29]	Resource elasticity, multi-tenancy, interoperability and migration over multiple clouds, application licensing, unpredictable environment, and legal issues	Framework to classify and characterize approaches based on the deployment model
[37]	Choosing the right vendor, adaptability amongst the employees and process change, lack of trust in cloud services, the extra cost to pay for system acquisitions, management and additional benefits	5R's process
[43]	Lack of knowledge, confusion about regulatory compliances in cloud contracts, concern over data and security, blocking of data sharing on shared infrastructure	3 stage framework; cloud requirement stage, cloud preparation stage, and cloud migration stage
[30]	Drivers and barriers in the adoption of cloud in the banking sector in EU: data breaches due to new and complex systems, risks of non-viable migration due to high migration cost, service discontinuity due to the multi-cloud system, and authorization and authentication issues	

Table 3.9: Summary of operational challenges in cloud migration

These operational challenges could lead to security risks like cyber-attacks, data breaches, insecure cloud environment, data and service unavailability and monetary threats. According to IBM, cloud-based applications open an easy way for hackers to exploit the cloud environment and account for 45% of cloud-related cyber threats [75]. The other threats are as follows: ransomware, data loss, malware, legal/compliance issues [75]. Hence, the operational risks and challenges will affect the security of the organization.

The solutions suggested that the researchers are more focused on tackling the operational challenges in the migration process and the features of the cloud. Therefore, the solutions aren't presented concerning an organizational perspective. Non-technical challenges like lack of knowledge, choosing the right vendor, adaptability amongst the employees and process change have been included by [37], [43]. But the solutions are designed to highlight the technical challenges like blockage of data security, business discontinuity, and authorization and authentication issues ([43], [30]). This points to the second point of the research gap, i.e. the researchers mainly consider technical challenges while analyzing the migration process.

3.5.2. Security-related risks & challenges

Cloud migration is a big step for any organization. However, along with operational risks, an organization also faces security-related risks and challenges. Researchers have analyzed those as well and presented a few solutions to mitigate the impact of such risks.

In the research of Islam et al. [38], the authors have proposed a risk management framework for supporting the cloud migration decision-making process for an organization. The authors identified a list of security risks in cloud migration, including lock-in, malicious insider loss of governance, compliance challenges, loss of business reputation, and service failure. They mentioned that these risks act as a barrier to the adoption of cloud computing within organizations.

In the research of Kelf [41], the author has discussed the security risks faced by cloud migration and how to mitigate them. First, the significant risk acknowledged was downtime. Because if the cloud service leads to discontinuity, it could expose the applications and data stored on the cloud to cybersecurity threats. But the probability of downtime with cloud services is low. Next, the author discussed the shared responsibility model, focusing that businesses need to trust their CSPs concerning the various security protocols. Finally, the author mentioned the harm caused internally by the employees if they fail to follow the organization's security protocols.

Under the investigation of [53], the author listed and discussed a few security challenges such as shown in Table 3.10:

Challenge	Description
Data loss, exposure & external attacks	Happen because of incomplete, corrupt or missing files during migration. Also, phishing emails spread malware leading to data loss.
Misconfiguration	Happens when users grant permissions to other users during migration and provide unauthorized access to the organization's network.
Insider threats and accidental errors	Employees might corrupt or expose the business data, share files and confidential information during the migration process.
Lack of resources	It happens in an organization when resources lack the skill to handle cloud demands. A well-defined migration plan might require a budget, tools and people with the right skills.
Regulatory compliance violations	Happen during migration when organizations fail to follow the regulations while moving the application from on-premise to cloud.
Shortcutting security during the migration phase	Happens because creating a service is a click-button operation in which the user might miss the security configurations of the service.
Migrating everything at once	Would lead to a chaotic migration without prioritizing data and applications.
Insecure APIs	Could lead to open lines of connection for attackers, leading to data theft.

Table 3.10: Security risks of cloud migration [53]

Mutune [53] also discussed mitigation measures for the risks mentioned above, like baseline security before migration, apply adequate security during migration, proper setups and protection of user identities, ensuring cloud services comply with security regulations, establish appropriate logging and monitoring, data backup before migration, a phased migration strategy, and employee awareness.

The risks of data tampering, data leakage and unauthorized data intrusion is a primary concern in several domains like the health and financial sector. For example, the banking sector stores and processes confidential customer information, which is being resolved using the security approach of encryption and authentication [7]. But even with these vigorous measures, the cloud-based attacks rose 630% in 2020 [73].

In discussion with OWASP (Open Web Application Security Project) and OccamSec, [68] listed a few

risks and challenges and ways to mitigate them in the cloud. The author mentioned misconfigurations in cloud services as one of the primary causes of data breaches in organizations. He analyzed the lift and shift operations in the four common areas summarized in Table 3.11:

Services	Attacks	Defences
Identity (Identity Access Management (IAM))	Account takeover Brute force attempts Password spraying Social engineering Social engineering Privilege escalation Resource allocation Persistence	Single-sign on Multi-factor authentication No root user API keys User key rotation Role-based access Least privileged IAM policies Disable unused regions
Data Storage (S3, RDS, DynamoDB)	Bucket enumeration Data exfiltration Resource tampering Payload staging	S3: Turn on block public access Strict policies No public access, encrypt snapshots No public queues, encrypt messages Strict IAM controls
Networking (Virtual Private Cloud (VPC))	Service discovery Data exfiltration Security group backdoor Traffic monitoring	Network segmentation Strict security groups and NACL rules Use VPC endpoints for internal traffic
Compute (EC2)	Service enumeration Application exploit Post exploit Instance metadata access Lateral Movement Cryptojacking Unencrypted volume access	Server hardening Remove default users Load balancers Encrypt volumes Protect instance metadata

Table 3.11: Attacks and defences in Cloud services [68]

The security attacks and defences discussed in Table 3.11 are particular to services. These can be used by altering the configurations of the service and map to the *technology* element of the people, process & technology framework. These are also very specific to AWS. Such attacks and defences will be beneficial if organizations like OWASP present generic defences which can be applied to all the CSPs.

Section 3.5.2 discusses security-related risks like data loss, insecure APIs, service discontinuity, lock-in and data breaches. These risks are triggered by technical challenges like compliance, downtime, human error, lack of resources, misconfiguration, and migration strategies. [68] discussed the attacks and defences of various categories of cloud services like identity, networking and compute. This shows that the researchers and organizations overlooked the non-technical challenges and their impact on their security.

3.6. Conclusion

The literature review contained various topics and concepts related to cloud migration. The literature review has been done to understand the different factors an organization considers for choosing a CSP. The literature review showed that various researchers had suggested that a phased cloud migration process and well-planned strategies can mitigate their operational challenges. These operational challenges provoke security risks related to data integrity and security, application security or even business discontinuity for an organization. These risks could be scaled down with deliberate processes and strategies based on different cloud service and deployment models.

But the literature study also revealed that the researchers mainly focused on technical challenges like misconfiguration, social engineering, malware and outsider attack. These challenges come in the concluding phase of migration when the services are deployed. An organization faces numerous non-technical challenges during the planning process and during the migration, i.e. lack of resources, knowledge and skills level of resources, proper planning and resource allocations from involved stakeholders. These non-technical problems are overlooked. These issues are primarily relevant to the people aspect of an organization. Further down the migration process, these issues cause security threats for an organization, causing other issues like loss of reputation. In conclusion, using *people, process, & technology* framework, researchers and organizations neglect the people aspect when planning an organization-wide change.

4

Research Findings - Rabobank

In this chapter, the literature and analysis specific to the use case, Rabobank, is studied. First, Section 4.1 discusses the innovation management model used by Rabobank. Further, the sections are designed similar to *People Process & Technology* framework. Section 4.2 starts with the stakeholder analysis and, Section 4.3 to understand the cloud journey of Rabobank. Then Section 4.4 discusses its cloud migration process and strategies considered by the organization for cloud migration. Finally, the chapter is concluded by discussing the observations and findings from the group sessions in Section 4.5.

4.1. Innovation Management Model

The migration to the cloud from legacy infrastructure seems like a radical innovation. However, the introduction to the cloud in Rabobank has disrupted the existing business model of the bank and led to the formation of a new model [45]. Adopting a new technology like the cloud would alter the existing processes, team structure, and business strategies and standards. The source of this innovation is that most of the organizations in the banking sector are slowly migrating to the cloud, and every organization needs to catch up. Rabobank has been working hard in the field of innovation. They have an Innovation Board to design strategies for digitization and innovation along with an Innovation Factory to accelerate the process of innovation in-house [35].

There are various models to categorize, understand and manage innovation in an organization. Multiple researchers have discussed different models, like Innovator's dilemma, jobs-to-be-done-framework, technology adoption life cycle, the three horizons of growth, and the 70-20-10 rule [45]. Rabobank, as an organization, decided to manage the innovation in close collaboration with different business units [14]. Another reason to do it in-house, it because most of the innovations spin out and incorporate innovation. Therefore, different aspects like strategy, politics, the market should be connected. Hence, the business line is in the lead, and they follow a lean start-up process. Therefore, the bank developed a framework called Innovation Road-map shown in Figure 4.1, a "funnel process in which the hypotheses are validated from Problem fit to Scale" [14].

The five phases of the Innovation Roadmap are:

1. **Discovery:** This phase deals with understanding and generating strategically relevant ideas from different aspects like data, technology, trends and market.
2. **Problem Fit:** This phase deals with analyzing and exploring customer problems that Rabobank could solve.
3. **Solution Fit:** This deals with developing feasible and desirable solutions for the customers. The solution design could be done internally, collaborating with external partners; hence, the decision must be made to "buy, collaborate or build" [14]. This also open doors for the bank to explore open innovation.

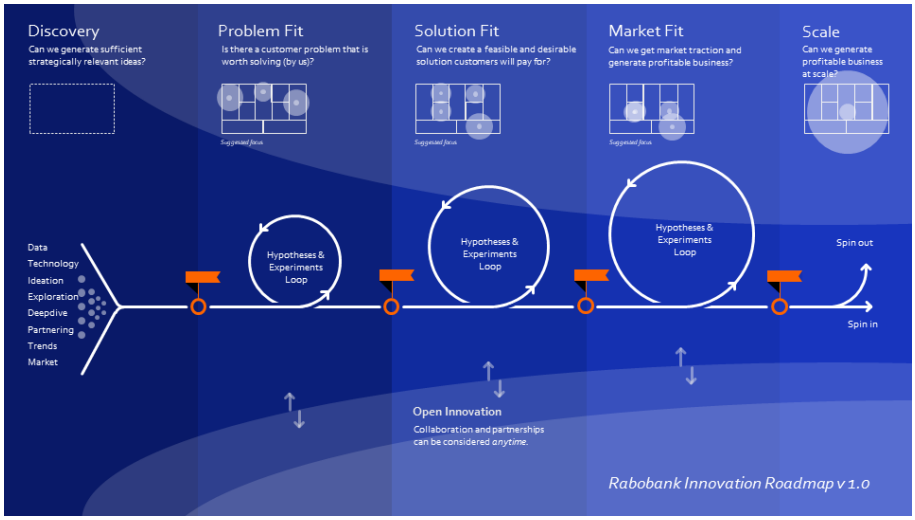

Figure 4.1: Innovation Road-map at Rabobank [14]

4. **Market Fit:** This phase deals with the solution's attractiveness, whether it will get market traction and generate profits for the organization.

5. **Scale:** This phase deals with the solution's scalability, i.e. if this solution could be expanded for other business lines.

The Innovation model Rabobank follows implies that the different business units are small start-up companies working autonomously. Each department or team follows the five steps of the roadmap and construct innovative solutions. Since the organization follows an in-house innovation strategy, Rabobank needs to make sure that the skills are accessible within the organization. Hence, the bank needs to ensure that all the stakeholders have been identified in the migration process. Different teams play specific roles, and they have skills and knowledge as per their stand in the migration process.

4.2. Stakeholder Analysis

Cloud migration can be defined as "a set of migration activities carried to support an end-to-end cloud migration" [29]. This process involves stakeholders with different backgrounds. At first glance, it would appear that there are three major stakeholders involved in the process of migration, cloud service provider, cloud service aggregators, and consumers [64].

In the research of Sabharwal [64], the author discusses cloud service providers or creators as the organizations involved in creating cloud services and infrastructure like Amazon, Microsoft, Google, etc. Cloud service aggregators are enterprises that provide solutions for the planning, implementation and monitor of cloud services. Consumers are the individuals or organizations that buy and utilize cloud services. They purchase either from a provider or aggregator based on their requirements. But for Rabobank, there are more stakeholders involved in the process. There are organizations outside Rabobank responsible for setting up laws and regulations to adopt such advanced technology. Within the organization, there are multiple units accountable for the design and implementation of different phases of the cloud journey, as shown in Section 4.3. Therefore, the stakeholders can be divided into two categories: external stakeholders and internal stakeholders.

The Power/Interest matrix is used to identify and assess the two categories of stakeholders [55]. This matrix identifies stakeholders in an organization based on their interest and ability to influence decision-making in a process or project. The stakeholders are divided into four zones based on their level of power and interest, as illustrated in Figure 4.2:

- *External Stakeholders*

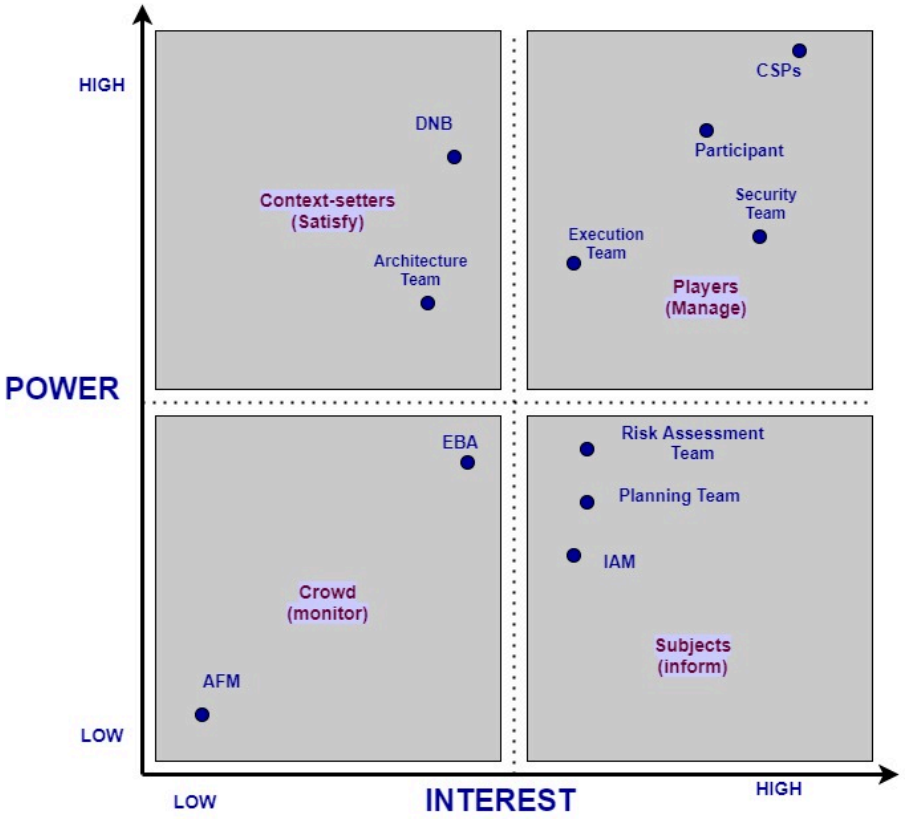

Figure 4.2: Stakeholder Analysis

– **Autoriteit Financiele Market (AFM):** The Dutch Authority for the Financial Markets is an independent governing body appointed by the Minister of Finance in the Netherlands [76]. This organization is responsible for supervising the responsible of financial market and determines and implements monetary policies. AFM also supervises Rabobank and other financial institutions in the Netherlands. They are directly not interested nor have the power to affect the cloud migration process at Rabobank.

– **De Nederlandsche Bank (DNB):** The Central Bank of the Netherlands or DNB is a public limited company governed by Dutch law. The main tasks involve designing and managing monetary policies, payment transactions, and foreign exchange market operations [57]. Therefore, DNB plays an essential role in formulating laws and regulations for the banks in the Netherlands. Furthermore, DNB mentioned strict supervision and a regulatory framework with new technologies like a cloud in the financial market [24]. Hence, DNB influences the overall cloud migration process and has power if their policies violate.

– **European Banking Authority (EBA):** It is an independent EU authority responsible for effective regulation and supervision across the European banking sector [4]. They play a significant role in designing rules for substantial organizational changes in the financial market in Europe; hence they have a considerable influence in cloud migration.

– **Cloud Service Provider (CSP):** Numerous companies like AWS, Microsoft Azure, Google Cloud Platform (GCP) are the major cloud service providers. Rabobank uses all three of them depending on their requirements. They have the most significant interest in the process of cloud migration. The constant updates in the design and configurations of cloud services like EC2, Virtual machines by CSPs influence the process considerably.

• *Internal Stakeholders*

- **Participant Team:** These teams are the ones that are currently migrating their infrastructure to a cloud environment. They provide their requirements, and then the following steps are decided. They have a significant interest and influence in cloud migration, as their needs affect the planning of the process.

- **Planning Team:** This team is responsible for enabling and accelerating cloud migration and having integrated planning, monitoring progress, and addressing the pre-migration issues for the numerous groups (Personal communication, July 12, 2021). They have a significant interest and influence in the process, as their main task is to accelerate the cloud migration process at Rabobank.

- **Risk assessment Team:** This team is responsible for performing the risk assessment of the cloud services and creating a decision tree to decide on the cloud environment (Personal communication, July 12, 2021). This team significantly influences cloud migration by evaluating the risk and security measures regarding the various cloud services.

- **Execution Team:** This team assists other stakeholders in the execution of the cloud migration. They help develop a business case for a participant team and provide access to cloud services as part of the onboarding process (Personal communication, July 12, 2021). They have a significant influence and interest in the process, as they are also an essential point-of-contact for the participant teams during the migration process.

- **Identity & Access Management:** This team is responsible for creating users and ensuring that the users have correct and secure access to buildings, data and applications. They are responsible for developing and provisioning access to users depending on the cloud service. They are the front door to the users through which they are granted access to applications; hence, they significantly influence migration.

- **Architecture Team:** This team is responsible for designing the architecture for groups when they migrate to the cloud. They have defined architectural principles concerning the cloud, keeping in mind the security, integration, and governance support needed to run and monitor the cloud applications at Rabobank (Personal communication, August 28, 2017). They influence the process and assist the participant teams, but they don't significantly interest the process.

- **Security Team:** This team is responsible for defining security standards for the numerous operations and protocols at Rabobank. Being a bank, Rabobank needs to follow various regulations and compliances, like PCI-DSS, ISO, GDPR and the rules set by external stakeholders like AFM and DNB. Therefore, this team influence the process majorly and has a significant interest as well. Moreover, their interest is substantial as they have to update the standards and policies if the external stakeholders make any change.

These stakeholders formulate the *people* aspect of the complete migration process at Rabobank. Therefore, they play essential roles in the different phases of the migration process, which will be discussed in the next section. One crucial point to be noted here is that any organization migrating to the cloud would have stakeholders on a similar level; hence, these stakeholders will be used to make generalized observations for any organization in this research.

4.3. Cloud Journey

Rabobank is one of the biggest banks in the Netherlands and manages assets of around EUR 48.9 billion [63]. Rabobank prioritizes its customers and provides them safe and secure banking services 24x7. Therefore, its priority is to build robust and scalable infrastructures to keep the business running.

Rabobank started using the cloud with SaaS-based applications and, moving forward, adopting a multi-hybrid integration of services. They are exploring the other service models and other cloud service

providers as well. This means a significant percentage of infrastructure moves to the cloud, and the remaining stay on-premise. Multiple CSPs are being considered based on their features and services and as per the teams' requirements. As an organization of 43,000 employees, the bank designed its cloud journey in three phases, with several sub-phases as shown in Figure 4.3.

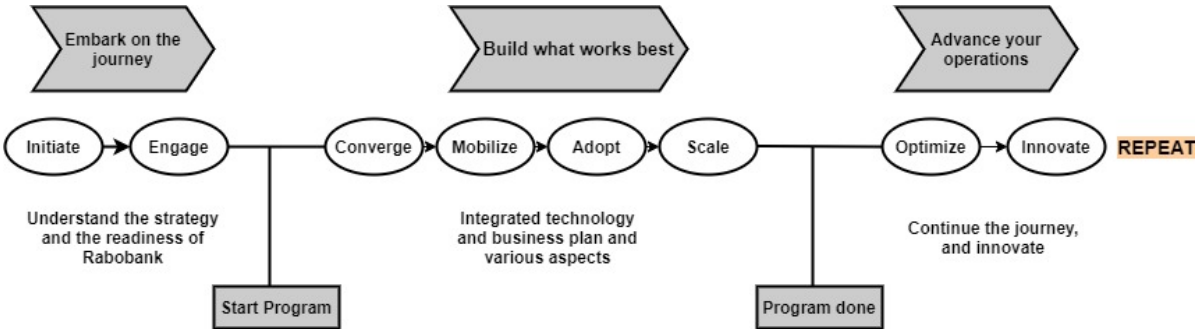

Figure 4.3: Cloud Journey at Rabobank (Personal Communication, July 12, 2021)

Each phase and sub-phase has specific objectives, which are listed below (Personal communication, July 12, 2021):

1. *Embark on the journey*
   The main objective is to understand the strategy and the fitness and preparation of the organization.
   (a) **Initiate:** Understand the importance and added value of the cloud to business and the organization
   (b) **Engage:** Enable early adopters to take the initial steps
2. *Build what works best*
   The main objective is to start an integrated technology and business plan, keeping in mind the various aspects like governance, control framework and operating models.
   (a) **Converge:** Establish that the major stakeholders have a common goal and are aligned on the same path
   (b) **Mobilize:** Detail the operating model and keep track of organizational readiness
   (c) **Adopt:** Enable the operating capability of Rabobank
   (d) **Scale:** Drive the adoption of cloud organization-wide and make use of all the powers of cloud
3. *Advance your operations*
   The main objective is to continue the journey, disrupt the process and transform the existing scenario.
   (a) **Optimize:** Continuous optimization of the cloud services as per the strategic plans
   (b) **Innovate:** Challenge the operating model and the existing knowledge of resources to foster continual ongoing innovation

Correlating the cloud journey with *people, process & technology*, the journey is more focused on the process and technology aspect of the framework. The journey will be used to map out the cloud migration process further. Hence, a lack of concentration on the *people* element might provoke issues in the migration process.

4.4. Cloud Migration

4.4.1. Process

In the research of Khan and Al-Yasiri [43], and Mutune [53], the authors suggested a phased framework or process for cloud migration to avoid numerous operational challenges and security risks. As a critical player in the financial sector, Rabobank also followed a phased approach and designed a five-step process to migrate their legacy systems to cloud applications. Each step or phase consists of multiple sub-steps leading to the successful cloud migration. The five stages have been described in detail with the involved stakeholders and their significant objectives (Personal communication, July 12, 2021).

1. *Migration engagement promotion*
   The primary stakeholder involved in this process is the planning team. The main objectives of this track are:
   - Increase the business support for cloud migration goals and prioritize the business goals following the common goal of successful migration
   - Promotion of the added values of the cloud-like decreased cost increased productivity and security
   - Discuss initial challenges and impediments with the participant team
   - To convince the participant to participate and grow with the innovative technology
2. *Acceleration migration pre-requisites*
   The key stakeholders involved in this process is the planning team, participant team. The primary objectives of this track are:
   - To identify blocking issues for cloud migration and remediation for these issues
   - To identify processes and technology and push owners of IT services to get on board with cloud migration
   - Enable the shared service teams to accelerate their cloud architecture implementation
3. *Planning, monitoring reporting*
   The key stakeholders involved in this process are CSP, assessment and execution team. The main objectives of this track are:
   - Categorize applications according to the requirements and methods
   - Redefine and standardize domain migration road-maps
   - Compile integral roadmaps, cloud migration planning and align dependencies
   - Prioritize migration movements across the different IT chapters to meet the common goal of Rabobank
   - Monitor and chase progress, and define and report key performance indicators (KPIs)
4. *Cloud organization, technology process design*
   The primary stakeholders involved in this track are the participant team, execution team and CSP. The leading objectives of this track are:
   - Develop a straightforward design of IT landscape and services from the intermediate to the end state
   - Push to define and design a target operating model for the IT
   - Ensure cost management on cloud resources
   - Develop clear designs and architectures for the participant teams
5. *Benefit tracking optimization*
   The major stakeholders in this track are the execution team, and they monitor and keep track of the migration and the status of cloud services at an organizational level. The main objectives of this track are:
   - Report the business benefits of cloud on an organizational level
   - Tracking the cost and the utilization of the cloud services

- Steer cloud migration priorities to maximize business benefits

The cloud migration process described above is a well-defined process with objectives defined corresponding to the cloud journey discussed in section 4.3. Correlating the migration process to the *People, Process & Technology* framework discussed in section3.3, it is clear that the function defined by Rabobank, as an organization, focuses on the change in process and value-added by the technology, i.e. cloud computing. The first phase consists of convincing the participant teams and businesses to understand the benefits of the cloud and get them onboard. The steps in the later stages jump directly into finding the blocking issues for cloud migration, identifying processes and technology, and develop architectures for those processes. The migration process nowhere considers the *people* component of the organization. The whole mechanism does not include stakeholder analysis, bringing stakeholders to the same page concerning new technology adoption, or the knowledge management for the adoption and migration process. Hence, the migration process will trigger challenges for involved stakeholders. These challenges will provoke security risks and threats to the organization, signifying the research gap mentioned in the literature review.

4.4.2. Strategies

The process of cloud migration could lead to business discontinuity; hence, organizations need to have a plan to perform this task. The technique discussed in the last section would ensure the continuity of the running services. But migrating different applications to the cloud depends on the type of service model it is transforming to.

Rabobank analyzed multiple strategies amongst the 5R's suggested by Gartner [9]. The planning team did the benefits and challenges of different approaches based on the service model summarized in Table 4.1.

Description	Benefit	Challenge	Service model
Refactor is rebuilding an application entirely with cloud-native components	Application is made fit for the future and will reap the full benefits of the cloud, like scalability, flexibility etc.	Refactoring each application will require a higher initial investment. In addition, legacy and cloud will co-exist, leading to additional costs.	Platform-as-a-Service
Replatform is when the application is moved from the infrastructure to platform services when needed base platform services	Reduce operational costs; Infrastructure acquisition and maintenance are transferred to CSP; Advantages of basic cloud functionality like auto-scaling, containers etc.	Change in application architecture could lead to incomplete utilization of the cloud; Maintenance of some components would be the responsibility of the application owner	Platform-as-a-Service
Rehost is moving the application one-on-one from on-premise to cloud	Reduce operational costs; Infrastructure acquisition and maintenance is transferred to CSP.	Change in application architecture could lead to incomplete utilization of cloud; Infrastructure maintenance needs to be done by application owner; Integration will become more complex, leading to hybrid integration	Infrastructure-as-a-service

On-premise cloud is moving the application one-on-one from on-premise to cloud-ready infrastructure	Reduce migration effort for participant team when they decide to go to the cloud	Application architecture is not cloud-native; there is incomplete utilization of cloud benefits; Infrastructure maintenance is heavy	On-premise infrastructure-as-a-service

Table 4.1: Comparison of different cloud migration strategies (Personal communication, July 12, 2021)

These strategies come in the second phase of migration, acceleration migration pre-requisites when the teams identify processes and technology. The planning and participant teams define the requirements and decide the type of strategy they want to choose. The groups generally decide to refactor, also known as lift and shift, to migrate their infrastructure [9].

After understanding the stakeholders and the process, the next crucial step would be to understand the opinions of the primary stakeholder, i.e. participant team, on the design and implications of the process and identify and validate the gaps and challenges in the current process. Therefore, the following section talks about the Ai method's analysis with two groups of participant teams.

4.5. Group Sessions

Group sessions, as discussed in chapter 2 were conducted with the employees of Rabobank to achieve the research objective. The sessions were done with two teams of Rabobank, one group that is in the initial phase of migration and another team that has already migrated to the cloud. The following subsections discuss the results of data analysis done on the scripts transcribed from the interviews. The scripts from the group sessions have been transcribed in Appendix A and Appendix B. Furthermore, the method of data analysis, coding analysis, has been explained in chapter 2.

4.5.1. Results - Initial Phase Migration

This group session was conducted with seven people from the team in the initial phase of migration. Table 4.2 shows the codes and categories recognized from the first group session.

The data analysis revealed that all participants shared a similar set of challenges and experiences encountered in the initial phase of migration, which led to the *feelings* category in the table 4.2 i.e. similarity in ideas. The first question of the Appreciative inquiry method revealed the first impression of participants concerning the central question, "*What opportunities and possibilities do we see to mitigate security-related risks in cloud migration?*" Participants mentioned measures to keep the cloud safe including "version control", "role-based access", AI as an opportunity, "access control", "data encryption to transfer the data from on-premise to cloud". Only one participant mentioned issues with cloud migration, i.e. "Missing or weak authentication leave organizations exposed to security risks". This shows that participants have risks and issues in mind, so they came up with these solutions.

The participants elaborated and shared their personal experiences related to their first impression with the central question as to the answer to the following question of the Ai method. These answers revealed the issues participants' experienced or might experience with their current knowledge of the cloud. The issues were categorized into data risks and security risks. The codes were defined for the specific type of risks.

Starting with the risks in the data, three out of six participants mentioned the lack of encryption and concerns about the type of encryption while migrating data to the cloud. Participants also worry about the security of the data in the cloud. For example, they were concerned that there is a lot of confidential data in a financial institution like Rabobank. While migration, the security of such data should be taken care of when moving to AWS and Azure. The participants were also worried about data risks like data breaches, data leakage, and unauthorized access to data. Similar issues were also discussed by researchers under operational and security in the literature study. [30], and [53] also listed data breaches

Codes	Categories
Data breach Data encryption Data leakage Data security Access	Data risks
Attacks Authentication Authorization Vulnerabilities Lack of communication Lack of information Advisor	Security risks
Assessment team Execution team Participant team Artificial intelligence	Stakeholders
Automation Checklist Good communication Cost of management Expertise Guidance Implementation Knowledge sharing Metrics Monitoring Reporting Tool Security maturity	Requirements
Similarity in ideas	Feelings

Table 4.2: Codes and categories after data analysis

in the complex cloud systems and data loss as a risk in the process of migration.

The other security risks mentioned by participants were related to authentication and authorization. Four out of six participants mentioned the access related to identity management in the cloud. This was also the first thing that participants could relate to the central question, and they described it as ”standard role-based access”, ”implement access control”, ”identity access”, and ”safe user access”. This shows that the participants were worried about the user access rights in the cloud environment and suggested ways to overcome their concern with role-based access. In addition, authorization and authentication issues have been categorized as barriers to adopting the cloud in the banking sector [30]. Hence, this was also covered by the researchers in the existing literature review.

A lack of communication amongst the different stakeholders like the participant team and execution team was observed in the first interview. The participant team was in the initial phase of migration and needed continuous assistance from the execution team during the service deployment concerning the different security settings of the cloud. Participants mentioned it as ”we have good communication during the migration process, and when the issues pop-up, everyone will be informed instantly.”, ”Getting a clear picture about the security, what level we need to apply for which application”, and ”for the security part, we can have more guidance”. These statements showed their concern regarding the lack of communication from the execution team. Such a lack of security information could lead to shortcutting security during the migration phase [53].

With the third question of the Ai method ”dream”, participants opened up about the requirements for a tool or solution to mitigate the risks and concerns in cloud migration. This phase revealed the primary concern of the participants, i.e. lack of communication and lack of information. A recurring requirement from the participant team was an advisor or a ”go-to person” for their queries and concerns regarding the security of the applications in cloud migration. The team members mentioned that they do not have adequate experience and knowledge about the cloud. They described their concern as ”we don’t need to put up a lot of time to find out the best way, what is the correct way and how to redo the things we already do”. The suggestion was mentioned as ”more of an onsite advisor”, ”it will be nice to have some go-to person that we can ask for, any question concerning security or architecture of the cloud”. These concerns point to a critical non-technical and planning-based challenge, i.e. participant teams do not access cloud and security expertise when needed.

The other critical concern is that the participant teams do not have adequate knowledge about cloud technology. The lack of information was also observed, majorly with three stakeholders, the participant team, CSP, and execution team. There were more than 15 instances where this was displayed as a concern and requirement from the participant team during the interview. The primary concern for the participant team is the lack of information about the risks different types of data carry. One participant mentioned that other groups that provide their data should inform them of the risks, such as whether the data is sensitive or regular. This would assist them in a secure migration of data to the cloud. Another participant mentioned that risks like data leakages could be prevented if the information about the security settings, existing systems, and security principles have been provided to them. This points to one of the operational challenges pointed out by [43], i.e. lack of security knowledge and concern over data and security. This also brings out other challenges, i.e. limited communication between the stakeholders.

Lastly, one observation from the data analysis was made about the indirect relations of a few codes to their categories. Codes like ”lack of communication” and ”lack of information” were not directly mentioned by the participants as a challenge. When asked about the risks in the current scenario, the major points were data-related risks and access and authorization. The participant team did not see this as a significant issue. But, the lack of knowledge and information in the migration process could lead to an insecure cloud environment and other risks like data breaches. Multiple participants also discussed it in numerous instances, putting it up as a critical non-technical challenge for the organization. This also proves the inefficiency of the cloud migration process is not considering the *people* aspect in the migration process. These issues were also missed out by researchers, clearly showing that researchers do not consider these non-technical issues alarming. These issues can trigger security risks for an organization, which will be explored further.

4.5.2. Results - Post-migration

The second group session, consisting of two participants, was conducted with a participant team that has already migrated to the cloud. This team choice is essential to understand and validate the challenges in the previous cloud migration projects at Rabobank. Table 4.3 shows the codes and categories for the post-migration data analysis.

The data analysis revealed that both the participants shared a similar set of feelings towards the cloud migration process, which they shared via their experiences encountered in the process of migration. This participant team revealed diverse challenges like difficulty in architectural integration, lack of in-depth knowledge, and inefficient risk assessment process. They also presented multiple examples to support their relationship with these challenges. Examples like ”do not use IP whitelisting, so taking away a security layer” are the participant’s view that removed a security layer and clashes with the in-depth security concept used during cloud architecture design. Another example is ”I experienced a lot of procedures and questions, and security-related questions”. The participant mentioned this concerning the questions related to the cloud in the migration process. According to the participants, these questions were asked during the risk assessment phase of cloud migration and should be answered by relevant teams rather than the participant team.

The other challenge that participants discussed was a lack of overview in the architecture design and

Codes	Categories
Architecture integration High-level overview Lack of in-depth knowledge Inter-dependencies Risk assessment process Lack of communication Lack of information Temporary solutions	Challenges
Insecure APIs	Security risks
Advisor Assessment team Execution team Participant team Security team	Stakeholders
Architecture integration Communication Evaluation Design Expertise Guidance Implementation Knowledge sharing	Requirements
Similarity in ideas	Feelings

Table 4.3: Codes and categories after data analysis

various inter-dependencies between numerous components in the architecture. Such inter-dependencies are adequately known to the participant team. During architecture design, a lack of communication between the two stakeholders leads to complex and insecure systems. This team also pointed to the critical non-technical challenge, i.e. lack of communication leading to an insecure system within the organization. This shows that technical challenges along with non-technical challenges can cause alarming threats to an organization. Hence, overlooking such challenges is itself a considerable challenge.

The participants also discussed components or methods in cloud migration that are generic to most teams. However, at times, the participant team has to develop their tools for these methods. In addition, a lack of knowledge about security standards leads to the design and development of insecure APIs and a critical security risk pointed out by [53]. Therefore, participants suggested that an assigned team develop such generic methods; hence, only one team needs to comply with the changing security standards at the organization.

The participants made multiple suggestions regarding the challenges they faced in cloud migration. Their recommendations included getting a team with a sound vision of architectural integration and security together, proper communication within different stakeholders, hands-on expertise and guidance about security and cloud environment, knowledge sharing and evaluation and review of previous projects that have migrated to the cloud to analyze and optimize the resource distribution. The first team also made similar suggestions, showing that the participant teams have identical requirements, which can be considered a crucial finding from the analysis and the identified challenges.

4.6. Conclusion

The analysis of the use case showed the cloud journey of Rabobank, the cloud migration process & stakeholder analysis. The investigation was presented following the *people, process & technology* framework. The cloud journey of Rabobank displayed a high overview of how the organization would adopt cloud computing. Further, the stakeholder analysis demonstrated the external and internal stake-

holders of external organizations responsible for setting up regulations and policies on the bank. The internal stakeholders mainly consisted of the teams or units participating actively in the migration process within the organization. Finally, the Innovation Management Model showed that the organization adopts a start-up model and treats each team as an autonomous unit, taking responsibility for their infrastructure.

The cloud migration process adapted by Rabobank is five-phased, and it resolves around *process & technology*. The first step towards an organizational change begins with *people*, but the process does not show strategies concerning stakeholders and knowledge management. This is also pointed out as a research gap in the literature study. Group sessions were conducted with the teams that have participated/are participating in migration, and the sessions showed similar results. The data analysis also revealed participants concerns with the current migration process and the requirements and expectations participants have from the organization. These two findings have been summarized in Table 4.4. The analysis also revealed that participants mentioned various security-related risks, which showed that participants are aware that the identified challenges can trigger security risks.

Challenges	Requirements
Data migration-related issues	Access to a well-experienced advisor
Architectural design	Proper planning
Lack of monitoring & reporting	Recommendation about the application's risk & vulnerabilities
Lack of knowledge of security	Architecture design aligned with the security
Lack of resources	Knowledge sharing between teams
Limited communication between stakeholders	Real-time monitoring of the maturity and health of applications
No inter-team knowledge sharing	Automatic mapping of on-premise security setting to cloud security
Inefficient risk assessment process	Evaluation of previous cloud migration projects
	Artificial intelligence to scan for vulnerabilities and attacks in the migration process
	Good communication during migration
	Recommendation system for the cost management
	No border between on-premise and cloud services way of working
	Time in between sprint planning

Table 4.4: Challenges & Requirements from the analysis

5 Findings

This chapter deals with the findings of the group interviews. First, Section 5.1 elaborates the challenges identified in the data analysis and discusses them in more detail. Second, Section 5.2 discusses the risks analyzed by the organization and from the data analysis. This section also presents a correlation between the challenges and risks triggered by them. Next, Section 5.3 discusses another critical finding from the data analysis, i.e. the requirements of the participants and prioritizes and categorizes those requirements. Finally, the chapter is concluded with the idea of the first step or a concept that organizations should consider dealing with the challenges and security risks in Section 5.4. This section consists of the various features of the concept, along with the evaluation of the concept.

5.1. Identified Challenges

5.1.1. Categorization

The main objective of this research is to determine the challenges and security risks an organization faces in the cloud migration process. The literature review summarized several operational and security-related challenges, which the participants also mentioned. In addition, several new challenges surfaced up in the data analysis as well. As mentioned in the introduction, the challenges can be categorized as technical and non-technical challenges. Table 5.1 below shows the categorization of identified challenges as technical and non-technical ones.

Technical	Non-technical
Data migration-related issues	Lack of knowledge of security
Architectural design	Lack of resources
Lack of monitoring & reporting	Limited communication between stakeholders
	No inter-team knowledge sharing
	inefficient risk assessment process

Table 5.1: Identified Challenges in Cloud Migration

The table clearly shows that non-technical challenges are more in number than technical ones; hence, it would be helpful for the organization to prioritize non-technical challenges over technical ones. Most of the non-technical challenges are related to the people aspect of the organization. As per the People, Process Technology improvement model, people are the critical asset of any organization. Lack of communication and skills in people would lead to an inefficient process [59]. The other two aspects, process and technology, are also enabled by people, showing the importance of the *people* element in

an organization.

Out of these eight identified challenges, the literature study discusses only three of them, which validates the research gap described in the literature study, i.e. the organizations and researchers overlook the non-technical challenges. Still, these are the primary concern of teams participating in the migration process. Figure 5.1 displays the overlapping between the numerous challenges discussed, indicating that the data analysis has challenges specific to Rabobank. The figure also shows the research gap, that researchers have analyzed generic issues in the process, rather than focusing on the non-technical problems an organization faces. The identified challenges have been discussed in detail now, along with the security risks triggered by them.

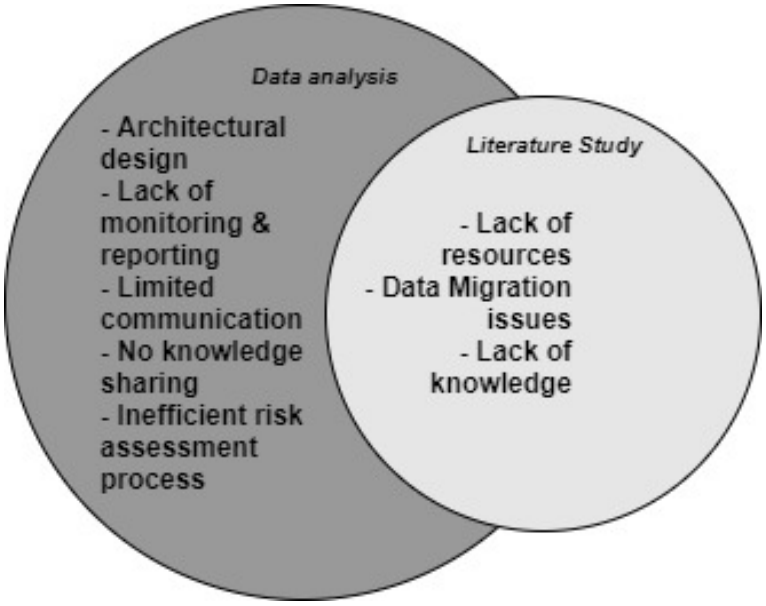

Figure 5.1: Challenges in cloud migration

5.1.2. Description

The identified challenges have been described in detail as follows:

- *Lack of resources:* The analysis clearly showed that there are no professional cloud advisors to ask questions about the security settings of different services and the system architecture. This could be because of various reasons like experienced advisors are not available or inefficient planning of resources. This challenge puts up teams in a difficult spot, where they have to make the decisions concerning sub-processes of migration. Furthermore, not every team is cloud expertise; it could lead to insecure deployments, misconfiguration of services, data loss, and unauthorized system access.
- *Data migration issues:* Data migration is one of the critical and complex steps in cloud migration. A decisive strategy, mapping data from legacy to cloud, is needed, along with an analysis of the problems faced during data migration like unexpected downtime, data loss, and compatibility issues [3]. The study pointed out that data security is of utmost importance during cloud migration for an organization; hence, the Lack of measures and strategy is significant. The investigation also acknowledged that it is essential to know the risks different data types have. Although, CSPs have classified data into various categories based on the associated risk with the data. For example, AWS recommends data classification in three categories unclassified (low-high for public cloud), official data (moderate-high for public cloud), and secret and above (moderate-high for private/hybrid/community/public cloud) [10]. Lack of such information could lead to misconfiguration and affect the security of the services and data.
- *Lack of knowledge related to security:* The analysis revealed that primary stakeholders like participant teams have acknowledged that security is not their area of expertise, and cloud migration

brings new aspects of security for them. The knowledge pool of the cloud is vast, and the teams are not aware of where to start. They are not skilled, and this leads to the development of systems with fragile security. This includes the Lack of knowledge of different security principles and controls put up by CSPs and adopted by the organization.

- *No inter-team knowledge sharing:* This was pointed out as the newest challenge in the analysis. Groups that have successfully migrated to the cloud could descriptively share their success stories so that the other teams could avoid the issues and mistakes. This would also help optimize the various resources like people, money, and time used in cloud migration.
- *Lack of monitoring and reporting of cloud migration:* It is vital to monitor applications' health and security maturity during migration. Numerous key performance indicators can be set up to quantify concepts that are hard to measure, like security is an advantage of the cloud, and can be used to convince teams to promote cloud by the planning team; still, it is challenging to measure [25]. The analysis revealed the need for a tool to continuously monitor the risks in the cloud environment and report these risks and vulnerabilities. This way, stakeholders would have a visual representation of the security level of the organization's applications. It is essential as lack of such a tool would lead to a higher presence of security risks and vulnerabilities in the cloud environment and expose them to higher risks like data loss.
- *Inefficiency of risk assessment in the migration process:* The analysis showed that the risk assessment process involves understanding the requirements of the teams and assessing the services they need. The current process is manual and involves the teams filling a survey to understand their understanding of cloud services and the security aspect of the cloud. Unfortunately, these questions are not relevant to the participant team, and further information about these questions is not presented in a concise and structured manner; hence the process becomes inefficient. In addition, the incompetency in the risk assessment process could lead to additional use of resources like money and time for the organization.
- *Architecture design:*The analysis pointed out that the architecture design is performed at a macro-level, and a high overview is presented to the teams, which leads to complex integration of services. The architects are not aware of the various interdependencies between services, leading to complex systems design. This delays the process for the teams migrating to the cloud. Further, the analysis also revealed that the architecture is not aligned with the organization's security standards, as they are not aware of different benchmarks. This also leads to the development of systems with weak security.
- *Limited communication between stakeholders:* This challenge was pointed out by multiple participants that there is little communication between primary stakeholders like the execution team, architecture team, assessment team, security team, and participant team. This limited communication leads to disorganized and inefficient processes. The Lack of communication could be the inadequacy of groups to access the existing knowledge at the organization or unavailability of resources. Therefore, continuous feedback and open communication between stakeholders are needed for a successful and secure migration.

5.2. Identified Risks

The threats and challenges discussed above lead to numerous risks to an organization. These risks could be security-related like data loss, data breach, insecure systems, or other dangers like monetary loss and reputation loss to the organization. Therefore, these challenges affect an organization collectively. Thus, the risks have been classified into two categories, i.e. security risks and other risks.

5.2.1. Security Risks

This section explains the various security risks that the identified challenges could trigger. These risks could impact the security of the infrastructure consisting of a network of services, devices and data. These risks were also pointed out in the data analysis and literature study; hence, it is crucial to discuss them in detail.

- *Data loss:* When migrating the data and applications from legacy systems to cloud environments, the data could go missing in the target system, called data loss [3]. Organizations deal with confidential and sensitive customer data, i.e. name, date-of-birth, address, sexual orientation, religious views, payment and transaction data. Therefore, this will be a significant security risk for the organizations.
- *Data breach:* This is also known as data spill or data leakage and can be defined as ”an activity which involves the unauthorized viewing, access or retrieval of data by an individual, application or service” [13]. It can be caused by internal factors like employee misuse, human errors, system glitches, and external factors like malicious attacks, intrusions, and online cyber theft [13]. A data breach is one of the critical security issues for financial institutions like banks because they store and process confidential customer data.
- *Insecure systems:* When deploying a service in the cloud environment, the developer needs to keep in check numerous security configurations. If these checks are missed, the service is not entirely secured and prone to malicious attacks. For example, Azure has defined certain security checks to protect the network, like protecting azure resources with virtual networks, denying communications with known malicious IP addresses, recording network packets, and deploying network-based intrusion detection/intrusion prevention systems (IDS/IPS) [12]. However, if these security checks are not fulfilled, attackers can access the services deployed in an insecure virtual network.
- *Unauthorized access:* Access management is a critical aspect for an organization when migrating to the cloud. This includes access to the complete system, including the applications, network and data. Unauthorized access to one aspect, for example, network, can halt the entire system. This also includes access to what type of data and what privileges have been defined for different users. If failed, internal data leakage will be a significant hazard of this risk.
- *Service discontinuity:* Cloud computing offers ”as a service” features like Software-as-a-service (SaaS), platform-as-a-service (PaaS), and Infrastructure-as-a-service (IaaS). These services together run the business flows, and downtime or blackout could discontinue services [48]. Therefore, service discontinuity can surely lead to business discontinuity and bring the entire organization to a standstill.
- *Insecure APIs:*This was a critical security risk revealed in the data analysis. There are generic functions that can be used by various teams in the process of cloud migration, and these functions need to comply with the security standards followed by the organization, like transferring files and data from on-premise to cloud. However, since teams are not aware of the security standards, it would lead to the development of functions and APIs that are not secure, opening these channels for data theft and data loss.

5.2.2. Other Risks

- *Monetary loss:* The number of cyber-attacks has been increased by 630% in cloud-based environments between January and April 2020 [51]. With such a massive number of cyber-attacks, the monetary losses will be gigantic. For example, Accenture estimated the cost of cyber-attacks in the banking industry to be $18.3 million per company [22].
- *Reputation loss:* This is not a security risk but the impact of the security as mentioned above risks. If these risks take effect, they will negatively affect the organization that cannot secure its systems and data. The damage is difficult to predict, as it is dependent on multiple factors, but the company can be associated with the security-related incidents [15].

To further understand the severity of the identified challenges and security risks triggered by them, mapping each challenge to the risks has been done. This correlation shows that the result is a many-to-many mapping. It means that multiple challenges lead to various security risks, and all the security risks lead to monetary loss and reputation loss for the organization, as shown in Figure 5.3. It is clear from the figure that the non-technical challenges have a massive impact in triggering the security risks and should be considered in the initial phase of migration. Therefore,this correlation clearly shows the emergency of highlighting the non-technical problems in an organization.

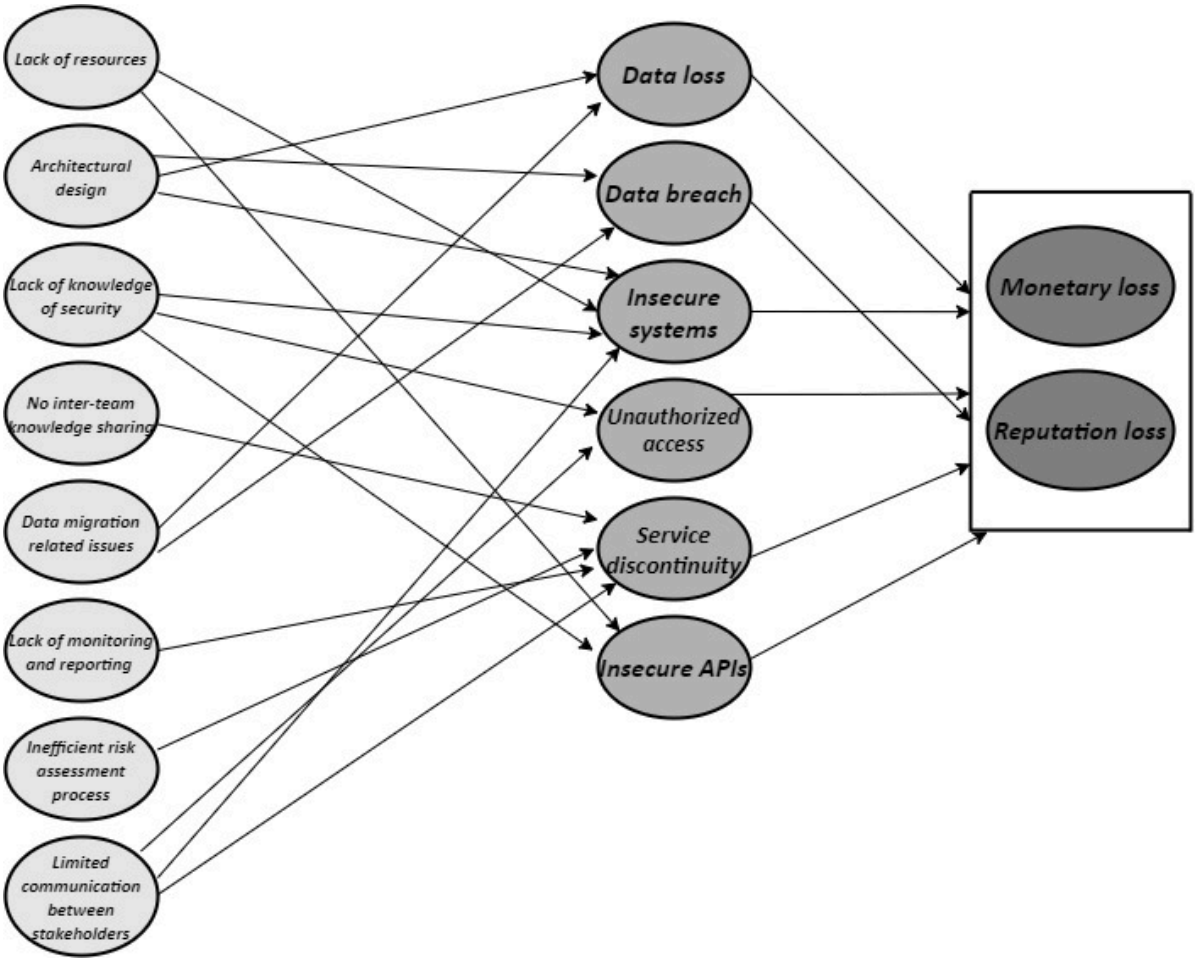

Figure 5.2: Mapping of Challenges and Risks

5.3. Identified Requirements

The last two questions of the Ai method were there to understand what teams need from the organization concerning the migration process; hence, requirements are also the critical finding of the analysis. Multiple requirements were gathered from the interviews, and it is essential to understand and process them to develop a viable solution. This is similar to the approach followed in a software development cycle, where requirements are gathered, understood, analyzed and translated into tools and measures.

It is important to prioritize and categorize the requirements because that would help understand the requirements from the solution perspective, as in which ones to deliberate first.

5.3.1. Requirements Prioritization

Requirements prioritization is a critical step in developing any software or tool, as it provides the proper implementation order of requirements. This order will help decide the solution's features, and the resource planning can be done correctly. The prioritization of the needs will be done using the MoSCoW method. This method is used to rank the requirements in a collaborative manner [33].

According to MoSCoW method, the requirements can be divided into four categories as discussed below and shown in Figure 5.3.

The method was applied to the list of requirements gathered from the data analysis, and summarized in Table 5.2.

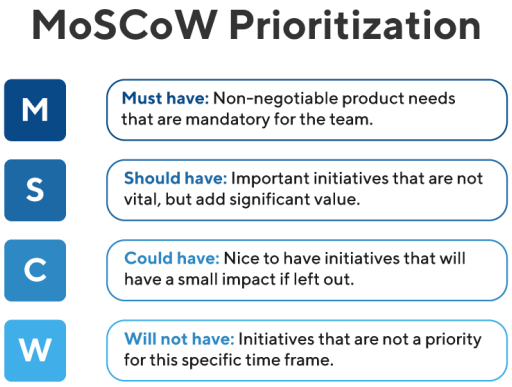

Figure 5.3: MoSCoW Prioritization [60]

Must haves: These serve as non-negotiable needs for the concept design [33]. This concept design should provide access to a well-experienced advisor who would bridge the stakeholders and clarify security-related queries. This advisor can enable the bi-directional information flow for both the stakeholders, i.e. requirements for service deployment from participant team to execution team and knowledge of security controls from execution team to participant team. The process will be finished with temporary fixes without the appropriate migration planning with the team's current workload. Since migration is an organization-wide goal, different groups should plan their resource allocation accordingly to avoid a confusing process. Knowledge sharing between teams and evaluation of previous cloud migration projects should be done adequately. When one team goes through migration and records their journey with an accurate description of the challenges and solutions, it would benefit the other teams.

Should haves: These requirements are essential to the prototype development but not critical [33]. Good communication between the teams is vital for a process to happen in an organization. Since most of the methods are manual, limited or lack of communication could misuse information. The other requirements in the should haves category are related to monitoring and reporting the security maturity and health of the applications, which would make the concept of security transparent to everyone in the organization. Proper metrics and KPIs would provide a visual awareness of the security maturity of different teams and the organization.

Could haves: These are the requirements that are not necessary to the product's core function, and they have a more negligible impact if left out [33]. Automatic mapping of on-premise security settings to cloud security is a dream because legacy infrastructures' features vary significantly with the cloud environment. The second and third requirements in this category relate to artificial intelligence as a defensive mechanism and use it to scan for vulnerabilities and attacks in the migration process. Various organizations like IBM and VMWare have worked on AI as a tool for cloud migration [44]. This tool optimizes the different phases of migration like discover, design and migrate using automation and AI [44]. The fourth point in this category is already implemented by various cloud service providers like Microsoft Azure and AWS. The Azure Cost Management and Billing service monitors cloud spending, improve accountability in an organization by implementing governance policies to manage the cost-effectively, and optimize cloud efficiency by improving returns on the cloud investment [18].

Won't haves: These requirements are the ones that are not the priority in a specific time frame. The two conditions mentioned in this category are related to the planning of the sprints suitably to accommodate the cloud migration as a part of regular tasks for the teams. The last requirement in the won't haves category is the indifference to working with both types of infrastructure. Teams expected that the systems were designed to make no difference with legacy systems moving forward with the cloud. This requirement points towards an experience rather than a tool, which might be out of the bounds of this research project.

Must-haves	Should haves	Could haves	Won't have
Access to a well-experienced advisor	Recommendation about the application's risk & vulnerabilities	Automatic mapping of on-premise security setting to cloud security	No border between on-premise and cloud services way of working
Knowledge sharing between teams	Real-time monitoring of the maturity and health of applications	Artificial Intelligence as a defensive mechanism	Proper internet connection
Proper planning	Real-time metrics for the security maturity	Artificial intelligence to scan for vulnerabilities and attacks in the migration process	Time in between sprint planning
Architecture design aligned with the security	Good communication during migration	Recommendation system for the cost management	
Efficient risk assessment process			
Evaluation of previous cloud migration projects			

Table 5.2: Requirements for the solution

5.3.2. Requirements Categorization

After gathering the requirements, it is essential to translate the requirements into a feasible business case. As inferred from the literature study, the two major cloud service providers are AWS and Microsoft Azure. The translation output contains the mapping of requirements to AWS and Azure's security controls and terminologies. Requirements from the teams can be categorized like the shared responsibility model, security of the cloud (CSP) and security in the cloud (customer) (Figure 5.4). In this case, the CSPs are AWS and Azure, and the customer is the organization migrating to the cloud. The relevance of this model is there because the CSPs came up with the shared responsibility model to enable the security practices from both sides. Similarly, the requirements should be divided between the two primary cloud stakeholders if responsibilities have been shared with the two primary cloud stakeholders. The cloud offers IT efficiency and flexibility to enable swift development in organizations [66]. But organizations need to understand that they have to adopt an agile way of working in this competitive market to respond to dynamic business demands [66].

- *Customer – Responsible for security "in" the cloud*
  - These requirements will be analyzed deeply to design a concept or solution for the organization.
  - The current knowledge sharing method is limited to sharing the success stories with no proper description of actual issues and challenges. Therefore, the teams should have a good knowledge transfer session planned in the initial phase of migration, which other stakeholders can put in the planning phase of migration. Knowledge sharing also includes sharing security knowledge between different stakeholders regarding the principles and controls provided by the CSP and the organization.
  - Proper planning of the migration for each team should be done by enabling communication channels amongst the key stakeholders like the planning, execution, and participant teams. This also includes allocating resources from each team to assist the teams in different phases of migration.
  - Each team should have access to a well-experienced advisor who can advise and guide them through the process of migration.

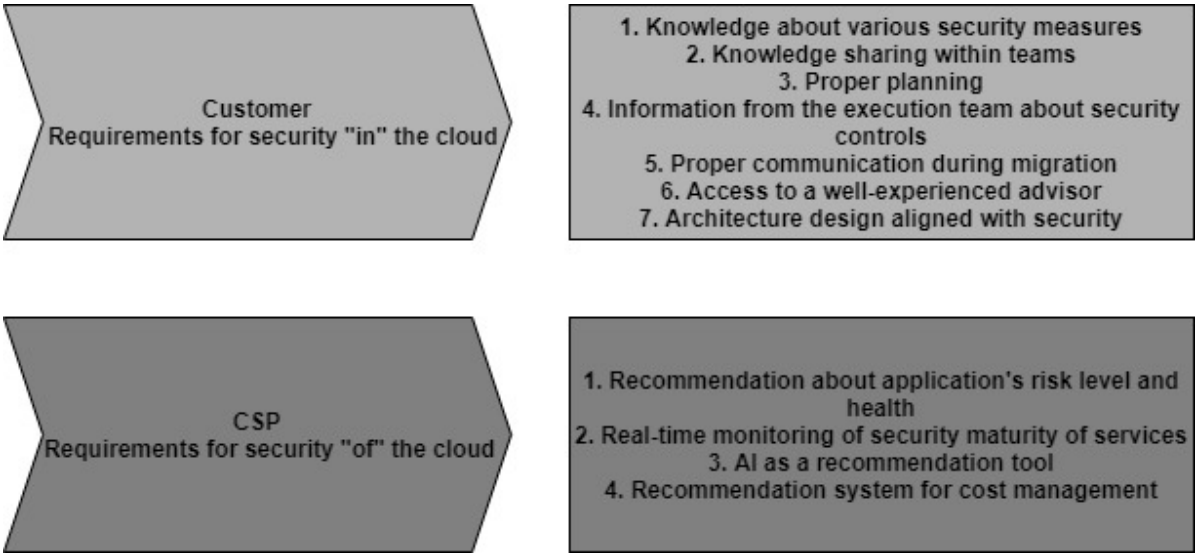

Figure 5.4: Requirements Segregation using Shared Responsibility Model

  - The architecture of the infrastructure has to be designed following the security regulations of the organization. The design should be done with continuous feedback to resolve the inter-dependencies between the sub-systems.

- *CSP – Responsible for security ”of” the cloud*
  - The cloud service providers have different tools to monitor the services that are being deployed and recommend security controls to the users. For example, Azure has a separate service called Azure security centre to assess the security state of the resources, visualize and improve the security posture by working on the security score [11]. In addition, AWS has a service known as AWS security hub that provides a comprehensive view of the security posture of your services and prioritizes findings and conducting security checks [36].
  - Azure security centre also uses AI and automation to identify threats, inform the users, and streamline threat investigation [11]. Similarly, AWS has an Amazon Inspector to perform an automated security assessment of the applications deployed in your AWS account, check the security compliance and enforce security standards [8].

With this model, the end-user or the organization will be able to develop tools and measures from their side to maintain security in the cloud. However, the analysis mentioned that the organizations focus mainly on technical problems rather than organizational problems like resource allocation, knowledge sharing, and management to maintain the organization’s security. Hence, the solution or concept should be more focused on the customer requirements presented in the analysis.

5.4. Initial Concept - Solution

In an organization, the cloud migration process would be similar for all the teams on a macro-level but moderately different on a micro-level. The requirements, strategy and resource distribution would depend on team size, current infrastructure design, knowledge level and qualification of the employees, current workload, and the budget for a particular team. The better way would be to turn the requirements into a business case and proceed with further steps. When a business case is created for a team, respective resources from different groups will be assigned to this business case. It will be their responsibility to ensure the fulfilment of all the requirements of a team.

Keeping this in mind, the initial concept was designed. The idea is named ”Cloud Catalyst”, with the primary intention of assisting the critical stakeholders during cloud migration at an organization. The concept can be designed as a platform that acts as a single interface for essential stakeholders to communicate, analyze, plan and execute cloud migration to achieve the goal. In addition, this platform will

help streamline cloud migration and be developed in collaboration with the execution and assessment team. The research analysis shows that limited communication, Lack of resources and an experienced advisor, and Lack of knowledge lead to security risks in an organization. Hence, the streamlining of the process would disable such issues, leading to a secure architecture and system design.

The following subsections describe the features of the concept and the evaluation of the concept with the various stakeholders.

5.4.1. Features

The requirements mentioned above has been translated into features, as shown in Figure 5.5, which will resolve the critical challenges analyzed in Section 5.1.

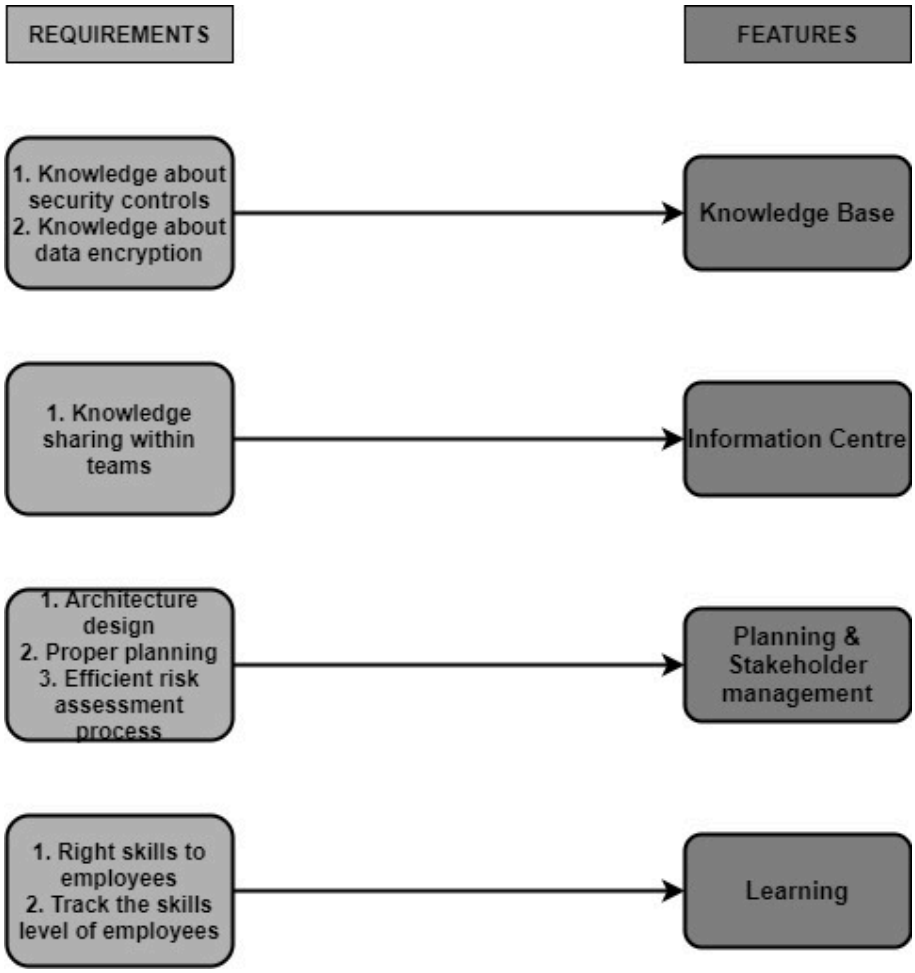

Figure 5.5: Requirements Features translation

Knowledge Base

The literature study mentioned a lack of knowledge about security and cloud computing and revealed it during data analysis. There are multiple sources of knowledge in an organization. Cloud migration is a complex process with numerous stakeholders, as shown in the study, and these stakeholders also act as a knowledge source. With this much knowledge flowing in an organization, it is crucial to managing it; otherwise, it won't be put to the correct use.

With multiple CSPs, and each CSP providing different services, there are numerous security configurations and controls concerning the secure deployment of these services. Therefore, the requirements

were to provide insight into these controls to mitigate the security risks triggered by insecure systems.

To solve the above difficulties of the teams in an organization, a knowledge management system (KMS) needs to be created as the first step to improve the migration process. According to the research of Pee and Kankanhalli [58], it is also a critical feature because knowledge management is essential for organizations to enable an agile business environment. Knowledge management is a complex process and involves the three aspects of the improvement model, people, process technology. Therefore, the system should have defined objectives and practices for the three aspects and help organizations achieve their goal. The authors have defined five stages of knowledge management, i.e. aware, defined, managed, and optimizing [58].

In the current scenario, the security controls and other information have been managed on different platforms and tools, which creates difficulty for teams to find such knowledge. However, this shows that the organization is in the second phase and is aware of developing expertise and are managing it in a complex way [58]. Furthermore, the multiple platforms show that they have defined a basic level of infrastructure supporting knowledge management [58].

But knowledge management is not tightly incorporated as an organizational strategy and not supported organization-wide [58]. This is clear from the identified challenges in Section 5.1. Cloud Catalyst can act as a knowledge management platform, where different teams can contribute by developing knowledge in a structured way. For example, the execution team can generate knowledge about security consisting of existing security controls and principles concerning the different cloud services used at Rabobank. The security controls can be further categorized corresponding to the categories provided by the CSPs, as mentioned in Table 4. The security controls will include the rules provided by the CSP and the authorities designed to keep the organization's security standards in check. The participant team can identify and access the type of controls needed for their scenario. In addition, the organization can optimize knowledge management by supporting institutionalized knowledge-sharing culture; organizational members are motivated to contribute valuable knowledge to improve the organization's performance [58].

Information Centre
Knowledge sharing between teams was an evident requirement from the data analysis, and it is also essential. The groups that have successfully migrated to the cloud can record their requirements, strategies, and steps to fix the migration problems. The evaluation and analysis of old projects will help the other teams understand the chosen plan and actions. It will also help understand the mistakes made in the past and help other teams not repeat them. Therefore, another feature of this concept would be to act as an information centre.

Cloud Catalyst can act as an information centre and assist in analyzing the requirements and show similar business cases of previous projects. The teams can also request sessions with the groups related to previous projects; hence, the platform will enable knowledge sharing within different teams. This would also help the teams understand the reasoning behind choosing a particular strategy for the migration process or a combination of security configurations for the services. In addition, the platform will also contain information about the different migration phases and an essential guide to the teams thinking of migration.

Planning & Stakeholder Management
Another visible challenge revealed from the data analysis was improper cloud migration planning for the teams and no go-to person for numerous security-related queries. Participants presented requirements like proper architecture, proper planning and an efficient risk assessment process. Hence, the next feature which will be essential to consider would be planning.

Cloud Catalyst can act as a common ground for the teams to provide their requirements concerning architecture design and enable continuous feedback. Furthermore, the teams could track the architecture design's progress and provide input and feedback regarding various components' inter-dependencies. Thus, cloud catalyst can act as a platform where different stakeholders can interact and provide feed-

back on the ongoing process. This continuous knowledge sharing and feedback with associated stakeholders would lead to a better migration process [49].

Another aspect of planning would be continuous communication between the stakeholders and managing them. The platform can assign individuals from different teams like the execution team, assessment team, planning team for the participant team. These individuals would be point-of-contact for the teams and ensure their queries related to security controls and their implementation are resolved to ensure timely infrastructure migration.

This feature would facilitate proper planning of the migration at a micro-level and continuous communication between stakeholders. In addition, this would lead to the design of secure systems complying with the standards and regulations set by the organization and external stakeholders.

Learning
Learning is the first and utmost important step when an organization goes through a significant technological change. Learning and skills refinement of the employees is very critical while adopting new technology. This is also the first aspect of the People, Process & Technology framework that has been adopted for this research analysis. It is essential to make sure that the human resources have knowledge about various aspects like what is cloud, why cloud, and how cloud. The first question on why the cloud is already done in the first phase of cloud migration explains the organization's mutual benefits to the cloud. The second question is what is cloud has to be done by the teams by exploring the different certifications program. The CSPs provide numerous certifications to get hands-on experience. This tool will help track other teams' skills levels and ensure that teams have sufficient knowledge before starting the migration process. The third question, i.e. how cloud has been answered via the other tool features as a knowledge base and information centre.

5.4.2. Evaluation

The evaluation is intended to observe and understand how the stakeholders perceive the concept, Cloud Catalyst, and the data analysis and findings leading to this concept. Another objective of this evaluation is to validate the data collected regarding the migration process and make the various stakeholders aware of gaps and challenges. The assessment will be carried out using the research methodology, structured interviews, as discussed in Section 2.2.2. Participants from the previous group sessions were asked to participate in the evaluation process. The interviews were one-on-one, and two-on-one based on the availability of the participants and the transcripts can be found in Appendix C, Appendix D and Appendix E

Mixed feedback was recorded from different stakeholders. Participants presented their opinions regarding the data collected and provided additional information regarding the findings, i.e. identified challenges, risks and requirements. The participants also gave valuable feedback on the initial concept to tackle the identified challenges. This feedback will be implemented in the recommendations for the organization.

They agreed on the identified challenges and further elaborated that Lack of experts because of resource shortage or Lack of planning in the process points to the inefficiency of the migration planning and could be taken care of by the planning feature of Cloud Catalyst. They further explained that there are multiple channels to gather the needed information; hence, it is difficult to clarify a single query in the process. They highlighted an important aspect of stakeholder analysis: business units should be included as internal stakeholders and explain the business risks to the developers. This could be solved with the stakeholder management feature of Cloud Catalyst. They further added that several initiatives had been started as part of the organization, but the teams are unaware of such actions. These initiatives could be made available at a common platform acting as an information centre.

The participants agreed on the security risks triggered because of the analyzed challenges. They suggested that other than monetary loss, these risks would also affect its reputation if the news of such security incidents goes out to the media. They also added that these security risks are interrelated. This showed that people within the organization are aware of such security risks and are open to a tool

or a platform to mitigate those risks. This makes it clear that the concept, Cloud Catalyst, would be helpful for an organization.

The participants agreed to the inefficiency of the current migration process by stating that ”the process is all over the place” and that Cloud Catalyst, as a tool, could streamline the process. In addition, they mentioned that the CSPs have a common standard of security, which should be customized by the organization, rendering to its security standards. They too said that ”Customer – Responsible for security ”in” the cloud” should be done by the different teams involved in the process.

Lastly, the participants suggested the features of the prototype. They recommended that the information centre be presented as a channel to answer the queries regarding the migration process. They also indicated that the information centre could be a promotional aspect for knowledge sharing and motivating other teams based on their story. To further encourage the knowledge process, the participant also suggested a points system for knowledge sharing. Additionally, they suggested creating a prioritization order to implement the feature based on their order in the migration process. The participants supported knowledge sharing by stating that members of teams that have already migrated to the cloud could assist other groups in the migration process. However, the participant mentioned his doubts about implementing one platform, as different stakeholders are responsible for providing knowledge about different migration phases.

The participants disagreed with the learning aspect of the concept. They stated that the certification courses of different CSPs are based on working with additional services. Still, the teams are looking for knowledge on the integration of various services. In addition, integration and networking affect the security aspect of migration, and hands-on learning is needed.

The mixed feedback made it clear that it is impossible to develop one platform to cater to all the requirements. Instead, the organization can implement the designed features in phases. In phase 1 focuses on knowledge management & resource allocation along with planning. Phase 2 would be developing a database of successful migration stories to build an information centre. Phase 3 could include creating a point system to motivate and enable the learning process in the teams and coming up with a new learning program that explains and assists in the integration of the services.

5.5. Conclusion

The findings of the data analysis were discussed in detail in this chapter. Identified challenges were classified into two categories, i.e. technical and non-technical challenges. Both the categories are equally crucial for safe and secure migration. Although, the study made it clear that the organization faces more non-technical challenges than technical challenges in the migration process. These non-technical challenges like lack of resources, lack of knowledge, and knowledge sharing are overlooked, and the organization fails to weigh in their impact. Multiple security risks like data loss, data breach, insecure systems, service discontinuity can be provoked because of these non-technical challenges. A correlation was done and presented in Figure 5.3, showing that multiple challenges lead to numerous security risks.

Another critical finding is the requirements of the teams concerning the migration process. These requirements were categorized and prioritized using various methods. The prioritization was done using the MoSCoW method to decide the ranking of the priorities and which ones to be considered first. The categorization was done using the shared responsibility model because cloud security is CSP’s and end-users responsibility together. The CSPs have adopted this model; hence the other stakeholder should also adopt a similar model to process the requirements internally.

Finally, the requirements were translated into features of an initial concept known as Cloud Catalyst. The four significant features are knowledge base, information centre, planning & stakeholder management and learning. These features were presented to the stakeholders, and they agreed on most of the features and their descriptions. In addition, they made suggestions and additional feedback, which will be implemented in the next chapter as recommendations.

The solution was designed after analyzing the data gathered from one specific organization, Rabobank, but other organizations can also adopt it. Furthermore, the literature study has validated identified challenges and risks; hence, the solution can be generalized and customized based on the organizational factors.

6

Discussion

Essential components of the thesis have been discussed in this chapter. The thesis is first reflected upon in Section 6.1. Following that, in Section 6.2, the contribution of such research are noted. After that, in Section 6.3, the thesis's limitations are examined. The future study focus and recommendations for Rabobank are then discussed in sections 6.4 and 6.5. In conclusion, Section 6.6 talks about the relevance of this thesis to the master's program.

6.1. Reflection

Cloud migration is an essential and complex process for any organization. Multiple stakeholders are involved in this process, dealing with numerous sub-processes, and driving those processes with advanced technology. The use case, Rabobank, was used to gather the data and analyze it. The analysis showed that an organization faces numerous challenges during cloud migration, starting from lack of knowledge about security principles and controls concerning cloud, lack of measures for data migration, lack of communication between stakeholders, and disorganized sub-processes like planning & risk assessment. Further, primary stakeholders like the planning team, assessment team, and security team are not aware of these challenges faced by the participant teams.

During the research, it was found out that these challenges are faced by multiple teams and also trigger security and other risks for an organization. Security risks like data loss, data breaches, insecure systems could lead to monetary loss and affect the organization's reputation. However, since there is a timeline planned to migrate the infrastructure, these challenges and security risks are ignored in the process.

The research also revealed multiple strategies to migrate to the cloud, and they differ from team to team. For example, if the team decides on the SaaS model, they would consider re-purchase, but if they choose IaaS, they will use re-host. In addition, the lack of knowledge within teams could make the decision-making process difficult for them; hence, they need a well-experienced advisor.

The requirements gathered from the data analysis also showed that teams in an organization want the management to focus on non-technical challenges. These requirements were translated into a conceptual solution for the organization focusing on four features, knowledge base, information centre, planning & stakeholder management, and learning. On evaluating the concept, it was found that there is a need for such a solution or a unique platform dedicated to cloud migration. This platform would open communication channels, enable proper knowledge management, and motivate teams to migrate to the cloud with adequate planning and learning. In conclusion, the idea of Cloud Catalyst as a platform could mitigate the crucial challenges faced in cloud migration.

Rabobank, as an organization, is investing considerable resources in the field of technological, organizational and business innovation. This thesis, in collaboration with them, has produced fruitful reflections for them as an organization. The identified challenges and requirements provided them with a

clear picture of the cloud migration process and its complexity. The designed concept was discussed with the recognized stakeholders at the bank and made them aware of the gaps and challenges in the current process from a security perspective.

6.2. Contributions

The literature review revealed that various researchers and organizations have improved and advanced the cloud migration process. Different processes and strategies were discussed based on the technical aspects of the cloud migration, i.e. type of deployment model, cloud service provider etc. Since migrating to the cloud is a substantial organizational change for any institution, technical and non-technical factors should be considered. Therefore, such a case study of a financial institution like Rabobank throws light on the importance of non-technical factors in the process of cloud migration.

Security is the key concern of organizations, and organizations innovate by developing numerous measures and actions to keep their infrastructure and data safe and secure. Different stakeholders are responsible and apply stringent laws and regulations to keep the data secure. When an organization decides to enable innovative technology like cloud computing, the apprehension of security rises. The significant threats and risks come with data migration, data security, authentication and authorization, integration of multiple CSPs, lack of resources etc. But other factors are shadowed by these process-related issues. By effectively focusing on the people, process, and technology framework, this research shows that researchers and organizations miss the first step, i.e. people aspect. This aspect focuses on the learning and skills of employees, communication between stakeholders and knowledge sharing. These issues fall under the non-technical category but affect the security of the infrastructure and data. Hence, this thesis provides a platform that focuses on the learning aspect of people and knowledge sharing in a technological change.

This concept can be used as a single platform to enable a uniform migration process and facilitate open communication and knowledge sharing within an organization. Additionally, this thesis has made different stakeholders aware of the concealed challenges and their security risks in the migration process. Therefore, it would better support the participating teams during migration, leading to a successful and secure migration.

6.3. Limitations

The research methods, literature, and concept design all contributed to the limitations of the thesis.

- Because of the current covid-19 problem, the research approach had to be changed. The approach needs to be adjusted from a typical study to virtual group interviews with team members. The current working environment prevents scheduling interviews with multiple teams at once. While there could be some drawbacks in analyzing data from similar groups with similar ideas, the research pointed out the impact of non-technical factors on security.
- The research was also confined because of the small sample size. This may or may not be crucial to an exploratory study on cloud migration problems. However, it can be a drawback during the evaluation process as all the stakeholders could not be consulted, leading to better conceptualization and visualization of the solution.
- The sample size was limited to people from a specific background at the company. The teams were chosen to keep in mind their affiliations to the legacy and cloud infrastructures. This would lead to pointing out the obvious security risks in the process.
- The data collection, analysis and validation was done within the settings of one organization. The identified challenges, risks and requirements would have impacted more if more organizations could contribute to the analysis.
- The concept was designed keeping in mind the requirements of one stakeholder, i.e. the participant team. Even though this team is affected the most and has the most significant interest in migration, the concept should consider the needs and requirements of other stakeholders like the planning team, assessment team and execution team.

6.4. Future Research

The thesis is concluded by providing some suggestions and recommendations for further development of the concept and streamlining of the cloud migration process:

- The research study revealed a big gap in the research, i.e. overshadowing non-technical factors concerning security of the infrastructure & organization. This was pointed out in the literature review, as well as in the organizational study. The researchers need to change their perspective from technical to organizational factors while assessing any organizational change.
- The framework used in this analysis was *People Process & Technology*, which is considered as a process improvement model. Here this model was used to study technology adoption and migration, which many researchers do not use. In addition, this model provided impacting results; hence, the researcher would recommend using such models for analyzing organizational changes.
- To conduct a similar study with other organizations in different industrial sectors. Security is one of the primary concerns of all industrial sectors, and such non-technical factors might be overlooked and impact the security of other sectors. Like the security team, the other identified stakeholders can play an essential role in drawing a better correlation between non-technical and security risks.
- The concept's features could be developed and automated efficiently using innovative technologies like machine learning. For example, as soon as a team registers to migrate to the platform, the knowledge base can show relevant content to understand in the initial phase, like knowledge about different CSPs and their services.

6.5. Recommendations

- The development of the concept into a platform could be done in different phases as suggested in Chapter 5. The organization need to include all the teams in the loop and take continuous feedback during the prototype development. This would ensure the feasibility and scalability of the prototype.
- To make the current migration more secure, stakeholder management and knowledge management should be taken care of by the organization as a priority. Stakeholder analysis is an important aspect of an organizational change, and knowledge management is essential when an organization shifts to new technology.
- The organization could evaluate the previous projects and report the challenges faced and solutions provided. This would ensure proper planning and resource allocation from involved stakeholders. It would also make sure that the new teams do not repeat the mistakes made in the past.
- An organization should focus on the people aspect of the improvement model and invest more into the learning and knowledge management within and between different teams. Multiple stakeholders are responsible for the knowledge sharing, but they are not aware of their roles and responsibilities in the process.

6.6. Relevance to MOT Program

This thesis was completed as part of the TU Delft's Management of Technology (MOT) MSc. program. This course focuses on the ways students can investigate and understand technologies leading to better processes, productivity, and competitiveness in an organization. The thesis specifies cloud computing as technology and explores the challenges and security risks an organization faces in the transition phase to cloud, with Rabobank as the use case for the case study.

The thesis weighs in on the relevance of mitigating non-technical factors as they also trigger security-related risks in an organization. The analysis has been done by applying knowledge gained from the MOT courses such as Leadership and Technology Management, Digital Business Process Management, Research Methodology, and I & C Service Design. As a result, a research study like this is critical for the MOT program because it directly relates to its primary goals.

7

Conclusion

Cloud computing is one of the state-of-the-art technologies that has led to considerable transformations in an organization. Its numerous benefits like scalability, cost-efficiency, security, robustness are making many organizations migrate to the cloud. However, the process of migration is complex as it involves migrating the infrastructure and triggering process and organizational migration. This is followed by numerous technical and non-technical challenges that impact the security of the organization. This research study has explained the concept of cloud computing, cloud migration process and strategies, the various challenges an organization can face in the migration process, the security risks posed by those challenges, and finally, a concept or proposal to mitigate those challenges.

Along with this concept, this study also revealed a considerable research gap in the research methodology using the people, process& technology framework. The gap revealed that researchers and organizations focus mainly on technical challenges and weigh in the security risks triggered by them. The non-technical challenges like lack of resources, knowledge sharing, limited stakeholder management are overlooked. This study showed that these issues could also cause security risks like data loss, vulnerable systems, and unauthorized access to systems and data in the migration process. Therefore, the concept was designed by prioritizing the requirements from these non-technical challenges. Four essential features were discussed as a part of the solution: knowledge base, information centre, planning & stakeholder management, and learning. The suggested concept was evaluated and showed that organizations need to enable knowledge sharing, open feedback and stakeholder management in the initial phase of migration to mitigate security risks from the beginning.

Bibliography

[1] 5 Top Cloud Service Providers Companies in the World. (2018). https://data-flair.training/blogs/cloud-service-providers-companies/#:%7E:text=Services%20Provided%20by%20Cloud%20Providers%20%20%20Name,%20SaaS%20Products%20%201%20more%20rows%20

[2] A. Ojeniyi, J., O. Edward, E., & M. Abdulhamid, S. (2019). Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study. *International Journal of Education and Management Engineering*, *9*(2), 1–14. https://doi.org/10.5815/ijeme.2019.02.01

[3] Abdou Hussein, A. (2021). Data Migration Need, Strategy, Challenges, Methodology, Categories, Risks, Uses with Cloud Computing, and Improvements in Its Using with Cloud Using Suggested Proposed Model (DMig 1). *Journal of Information Security*, *12*(01), 79–103. https://doi.org/10.4236/jis.2021.121004

[4] About us. (n.d.). https://www.eba.europa.eu/about-us

[5] Ahmad, A., & Babar, M. A. (2014). A framework for architecture-driven migration of legacy systems to cloud-enabled software. *Proceedings of the First International Conference on Dependable and Secure Cloud Computing Architecture - DASCCA '14*. https://doi.org/10.1145/2578128.2578232

[6] Ahmad, N., Naveed, Q., & Hoda, N. (2018). Strategy and procedures for Migration to the Cloud Computing. https://ieeexplore.ieee.org/abstract/document/8629101?casa_token=1F8R7US3Ha4AAAAA:FS-7Puj52mIFAICJrPn5V__i14sXiceKjjgUn_w8Dv2f0WD26HT5xuel7c2Zs_LvupfI6Q9tPSY

[7] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, 1–1. https://doi.org/10.1109/access.2021.3073203

[8] Amazon Inspector. (n.d.). https://aws.amazon.com/inspector/

[9] Avinash, G. (2020). 5R Strategy for Cloud Migration. https://www.agiliztech.com/2020/05/21/cloud-migration-5r-strategy/

[10] AWS Recommendations - Data Classification: Secure Cloud Adoption. (n.d.). https://docs.aws.amazon.com/whitepapers/latest/data-classification/aws-recommendations.html

[11] Azure Security Center. (n.d.). https://azure.microsoft.com/en-us/services/security-center/#features

[12] Baldwin, M. (2021). Azure Security Control - Network Security. https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-network-security

[13] Barona, R., & Mary Anita, E. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. https://ieeexplore.ieee.org/abstract/document/8074287?casa_token=KR3BcGunXM0AAAAA:9hjxyOduq09E_2f6lDAnEYhj3t5JS_Azs2gGUaRGW0VUFCMr2YEBccj8V_E8M1tb-05B0fGlebY

[14] Berghuis, G. H. (2020). Innovation Factory. Klinkt goed, wat is het? - Gert Hans Berghuis. https://gerthansberghuis.medium.com/innovation-factory-klinkt-goed-wat-is-het-307ca099b4ac

[15] Bernstein, E. (2019). The Reputation Impact of Data Breach. https://www.bernsteincrisismanagement.com/the-reputation-impact-of-data-breach/

[16] Bryman, A. (2012). *Social Research Methods, 4th Edition* (4th). Oxford University Press.

[17] Carmeli, A., Gelbard, R., & Gefen, D. (2010). The importance of innovation leadership in cultivating strategic fit and enhancing firm performance. *The Leadership Quarterly*, *21*(3), 339–349. https://doi.org/10.1016/j.leaqua.2010.03.001

[18] Cloud Cost Management. (n.d.). https://azure.microsoft.com/nl-nl/services/cost-management/

[19] CloudPassage". (2020). Shared Responsibility Model Explained. https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/#:%7E:text=In%20the%20AWS%20Shared%20Security%20model%2C%20AWS%20claims,ownership%20of%20%E2%80%9Cphysical%20hosts%2C%20networks%2C%20and%20data%20centers.%E2%80%9D

[20] Coghlan, A. T., Preskill, H., & Tzavaras Catsambas, T. (2003). An overview of appreciative inquiry in evaluation. *New Directions for Evaluation*, *2003*(100), 5–22. https://doi.org/10.1002/ev.96

[21] Crumpton, M. A. (2012). Innovation and entrepreneurship. *The Bottom Line*, *25*(3), 98–101. https://doi.org/10.1108/08880451211276539
[22] Dautovic, G. (2021). Top 25 Financial Data Breach Statistics | Fortunly.com. https://fortunly.com/statistics/data-breach-statistics
[23] Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. https://ieeexplore.ieee.org/abstract/document/5474674?casa_token=oYssxf3f_0kAAAAA:8Q9cm5uWLM9nfZ9c3ooA9PD2no86ASEBZmMfiQ874B4wc4wHMisvsYfW2oMigxeqhudiOphQdNI
[24] DNB". (n.d.). Rise of BigTechs in financial services sector requires adjustments in supervision. https://www.dnb.nl/en/actueel/dnb/dnbulletins-2021/rise-of-bigtechs-in-financial-services-sector-requires-adjustments-in-supervision/
[25] Essential KPIs to measure cloud migration services. (2019). https://theblackchair.com/essential-kpis-to-measure-cloud-migration-services#:%7E:text=KPIs%20are%20an%20essential%20part%20of%20cloud%20migration,protect%20data%29%20and%20infrastructure%20%28to%20support%20their%20operations%29.
[26] Final Version of NIST Cloud Computing Definition Published. (2018). https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published#:%7E:text=Final%20Version%20of%20NIST%20Cloud%20Computing%20Definition%20Published,Definition%20of%20Cloud%20Computing%20%28NIST%20Special%20Publication%20800-145%29.
[27] Frațilă, L. (2020). ENTERPRISE ARCHITECTURE AND CORPORATE GOVERNANCE – A COHESIVE APPROACH TOWARDS CLOUD MIGRATION IN THE... https://www.researchgate.net/publication/341480560_ENTERPRISE_ARCHITECTURE_AND_CORPORATE_GOVERNANCE_-_A_COHESIVE_APPROACH_TOWARDS_CLOUD_MIGRATION_IN_THE_BANKING_INDUSTRY
[28] Ganesan, A. S., & Chithralekha, T. (2016). A Survey on Survey of Migration of Legacy Systems. *Proceedings of the International Conference on Informatics and Analytics*. https://doi.org/10.1145/2980258.2980409
[29] Gholami, M., 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
[30] Hon, W., & Millard, C. (2018). Banking in the cloud: Part 1 – banks' use of cloud services. *Computer Law Security Review*, *34*(1), 4–24. https://doi.org/10.1016/j.clsr.2017.11.005
[31] Hosseini Shirvani, M., Rahmani, A., & Sahafi, A. (2017). An iterative mathematical decision model for cloud migration: A cost and security risk approach. *Software: Practice and Experience*, *48*(3), 449–485. https://doi.org/10.1002/spe.2528
[32] Howarth, F. (2017). What Are the Risks of Legacy Infrastructure? https://securityintelligence.com/what-are-the-risks-of-legacy-infrastructure/
[33] Hudaib, A., Masadeh, R., Qasem, M. H., & Alzaqebah, A. (2018). Requirements Prioritization Techniques Comparison. *Modern Applied Science*, *12*(2), 62. https://doi.org/10.5539/mas.v12n2p62
[34] Hussein, N. I., Hashem, M., & Li, Z. (2013). Security Migration Requirements: From Legacy System to Cloud and from Cloud to Cloud. https://www.researchgate.net/publication/266642754_Security_Migration_Requirements_From_Legacy_System_to_Cloud_and_from_Cloud_to_Cloud
[35] Innovatie bij Rabobank. (n.d.). https://www.rabobank.com/nl/about-rabobank/innovation/design-en-innovation/how-we-innovate.html
[36] Introduction to AWS Security Hub (2:34). (n.d.). https://aws.amazon.com/security-hub/?aws-security-hub-blogs.sort-by=item.additionalFields.createdDate&aws-security-hub-blogs.sort-order=desc
[37] Iqbal, A., & Colomo-Palacios, R. (2019). Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review. *Procedia Computer Science*, *164*, 48–55. https://doi.org/10.1016/j.procs.2019.12.153
[38] Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Decision Support. https://www.mdpi.com/1911-8074/10/2/10
[39] Jamshidi, P., Ahmad, A., & Pahl, C. (2013). Cloud Migration Research: A Systematic Review. https://ieeexplore.ieee.org/abstract/document/6624108?casa_token=ijQWnGOxcwAAAAA:647pBr2kEb82I84ipP1zRF1JJj4h_gCLywEZKijV9Im0DCEPAjZ_bGHP2Xgoe8nh63LnRf2X6Pw

[40] Kampen, M. (2020). Trends and developments in the ICT sector |. https://www.rabobank.nl/kennis/s011077850-belangrijke-trends-en-ontwikkelingen-voor-ict
[41] Kelf, S. (2020). The security risks created by cloud migration and how to overcome them. *Network Security*, *2020*(4), 14–16. https://doi.org/10.1016/s1353-4858(20)30044-1
[42] Kepinski, W. (2018). Rabobank kiest voor Pivotal Cloud Foundry platform | Dutch IT-channel. https://dutchitchannel.nl/608737/rabobank-kiest-voor-pivotal-cloud-foundry-platform.html
[43] Khan, N., & Al-Yasiri, A. (2015). Framework for Cloud Computing Adoption: A Roadmap for Smes to Cloud Migration. *International Journal on Cloud Computing: Services and Architecture*, *5*(5/6), 01–15. https://doi.org/10.5121/ijccsa.2015.5601
[44] Kowta, R. (2020). IBM and VMware Transform Cloud Migration Through AI-Powered Smart Operations. https://cloud.vmware.com/community/2019/09/12/ibm-vmware-transform-cloud-migration-ai-powered-smart-operations/#:%7E:text=Our%20AI-powered%20cloud%20migration%20%28AIM%29%20solution%20will%20optimize,services%20from%20discovery%20data%2C%20using%20AI%20community%20algorithms.
[45] Kylliäinen, J. (2019). Key Innovation Management Models and Theories. https://www.viima.com/blog/innovation-management-models
[46] Lanfear, T. (2021). Shared responsibility in the cloud - Microsoft Azure. https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[47] Lang, M., Wiesche, M., & Krcmar, H. (2018). Criteria for Selecting Cloud Service Providers: A Delphi Study of Quality-of-Service Attributes. *Information Management*, *55*(6), 746–758. https://doi.org/10.1016/j.im.2018.03.004
[48] Lee, K. (2012). [PDF] Security Threats in Cloud Computing Environments | Semantic Scholar. https://www.semanticscholar.org/paper/Security-Threats-in-Cloud-Computing-Environments-Lee/ad9493adbdb0b26d5b5b69ae7aa5f269e73727df
[49] Lee, S., Oh, H. Y., & Choi, J. (2020). Service Design Management and Organizational Innovation Performance. *Sustainability*, *13*(1), 4. https://doi.org/10.3390/su13010004
[50] Li, A., Yang, X., Kandula, S., & Zhang, M. (2011). Comparing Public-Cloud Providers. https://ieeexplore.ieee.org/abstract/document/5731587?casa_token=j05IA-5kEv8AAAAA:Sf6XZI4NjRXC0u4yXnfZ7XqJO2zWOMrKWbXaz1gv8kuqJu0Iq4bpc9EehZLpFobDgcOfcsCj9Y4
[51] Mangat, M. (2021). 89 Eye-Opening Data Breach Statistics for 2020. https://phoenixnap.com/blog/data-breach-statistics
[52] Morrar, R., Arman, H., & Mousa, S. (2017). Technology Innovation Management Review. *Technology Innovation Management Review*, *7*(11). https://doi.org/10.22215/timreview/1114
[53] Mutune, G. (2021). Cloud Migration Security Challenges and Mitigation Strategies. https://cyberexperts.com/cloud-migration-security-challenges-and-mitigation-strategies/#:%7E:text=Cloud%20Migration%20Security%20Challenges%20If%20a%20business%20is,files%20because%20of%20incomplete%2C%20corrupt%2C%20and%20missing%20files.
[54] Nelson, O. (2019). Cybersecurity Threats in the Banking Sector. https://cyberexperts.com/%EF%BB%BFcybersecurity-threats-in-the-banking-sector/
[55] Newcombe, R. (2003). From client to project stakeholders: a stakeholder mapping approach. *Construction Management and Economics*, *21*(8), 841–848. https://doi.org/10.1080/0144619032000072137
[56] Orban, S. (2021). 6 Strategies for Migrating Applications to the Cloud. https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/
[57] Organisatie. (n.d.). https://www.dnb.nl/over-ons/organisatie/
[58] Pee, L. G., & Kankanhalli, A. (2009). A Model of Organisational Knowledge Management Maturity Based on People, Process, and Technology. *Journal of Information Knowledge Management*, *08*(02), 79–99. https://doi.org/10.1142/s0219649209002270
[59] Prodan, M., Prodan, A., & Purcarea, A. A. (2015). Three New Dimensions to People, Process, Technology Improvement Model. *New Contributions in Information Systems and Technologies*, 481–490. https://doi.org/10.1007/978-3-319-16486-1\{_}47
[60] ProductPlan". (2021). What is MoSCoW Prioritization? | Overview of the MoSCoW Method. https://www.productplan.com/glossary/moscow-prioritization/
[61] Puckrin, S. (2020). Legacy systems in banks explained. https://internationalfinance.com/legacy-systems-in-banks-explained/
[62] Rabobank - Particulieren. (n.d.). https://www.rabobank.nl/particulieren/

[63] Results reports. (2020). https://www.rabobank.com/en/about-rabobank/results-and-reports/index.html
[64] Sabharwal, N. (2013). Cloud Stakeholders and Value Chain. https://link.springer.com/chapter/10.1007/978-1-4302-4924-5_2?error=cookies_not_supported&code=d7d5d98f-6028-4f2d-983a-21ad71647751
[65] Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (4th ed.). Pearson Education.
[66] Scott, B. (2018). How a zero trust approach can help to secure your AWS environment. *Network Security*, *2018*(3), 5–8. https://doi.org/10.1016/s1353-4858(18)30023-0
[67] Sekaran, U., & Bougie, R. (2016). *Research Methods For Business* (7th edition). Wiley. https://www.academia.edu/39038902/Uma_Sekaran_Research_methods_for_business_a_skBookZa_org
[68] Sewell, J. (2020). OWASP London / OWASP Suffolk [ONLINE] Joint Chapter Meeting 7-October-2020. https://www.youtube.com/watch?v=Mp8RVCDYY38&feature=youtu.be
[69] Shivakumar, S. K. (2019). Transforming Legacy Banking Applications to Banking Experience Platfor. https://link.springer.com/chapter/10.1007/978-1-4842-4303-9_10?error=cookies_not_supported&code=2cf58197-dbe8-460b-b646-4b01699f261a
[70] Shuaib, M. (2019). Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challe. https://link.springer.com/chapter/10.1007/978-981-13-5934-7_35?error=cookies_not_supported&code=57d4591f-5dce-4071-b090-27412fd4575f
[71] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
[72] Software Engineering | Requirement Engineering - javatpoint. (n.d.). https://www.javatpoint.com/software-engineering-requirement-engineering#:%7E:text=Software%20Requirement%20Management%3A%20Requirement%20management%20is%20the%20process,a%20better%20understanding%20of%20the%20system%20is%20developed.
[73] The 2020 Cybersecurity stats you need to know. (2021). https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/
[74] The history of cloud computing. (2020). https://www.scality.com/solved/the-history-of-cloud-computing/
[75] Top 5 Cybersecurity Risks with Cloud Migration. (2020). https://www.tripwire.com/state-of-security/featured/top-5-cybersecurity-risks-cloud-migration/
[76] Wat doen wij? (n.d.). https://www.afm.nl/nl-nl/over-afm
[77] What Is Cloud Computing? A Beginner's Guide. (n.d.). https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/
[78] Yin, R. (2018). *Case Study Research and Applications* (6th ed.). SAGE Publications.
[79] Zhao, J., & Zhou, J. (2014). Strategies and Methods for Cloud Migration. *International Journal of Automation and Computing*, *11*(2), 143–152. https://doi.org/10.1007/s11633-014-0776-7

A

Interview transcripts – Interview 1

Researcher: As I mentioned I am the security innovation intern and my research deals with cloud migration and security. Today's session will be conducted in process with the Rabobank's AI method, i.e. appreciative inquiry method. So just a small introduction about the method as well. There are 5 steps in the Rabo AI Dialogue method. The first one is define, so I will give an introduction and you can associate with the topic, so everybody will have to type a word to show how they associate with the topic. And the second step is discover, everyone has to share a personal experience regarding the research question or the central question. The third step is dream, so this is where you have to visualize how do you see the future, how do you see the solution happening. The fourth step is design, as in what and who are needed to achieve the dream, basically who do you think could help with achieving the dream. And the fifth one is deliver, that is how do we make concrete plans regarding the topic. So there are few rules of conversation for Rabo's appreciative inquiry dialogue. These are the rules:

Allow the person to tell his or her story. We appreciate the story and we do not judge anyone, it's a discussion, not a debate. Ensure everyone gets an opportunity to speak. And be respectful and kind.

So moving down to the research objective, as we know it is Rabobank's strategy to move most of their services to cloud by 2023, and in the process there are so many risks and challenges faced by the organization and the different teams within the organization, so which brings to my research objective, "to investigate security-related risks and challenges faced by Rabobank in cloud migration and innovative measures and socio-technical tools to overcome these challenges." And this is the central question:

"What opportunities and possibilities do we see to mitigate the security-related risks in cloud migration?"

As per the process, I am supposed to put the question in the chat. This is the central question and now we move to the first phase, which is define. As we know this is the central question and we are aware of the research objective, you guys have 2 minutes to think what is the first thing that you associate with this question and at 1:13 pm everybody will type it and send it at the same time.

Okay, send.

Participant 1: version control ;standard role based access; easier rollback

Participant 2: opportunity : AI

Participant 3: Already discuss the migration with our source providers, and include it in the Data Delivery Agreement.

Participant 6: Implement access control

Participant 7: Ubiquitous security management

Participant 3: Ask the source data providers if they see any risks

Participant 4: Missing or weak authentication leave organizations exposed to security risks

Participant 5: data encryption and identity access; safe user access

Participant 3: Some encryption to transfer the data from on-premise to cloud

Researcher: Is everyone done with the association part?

Now we move to the next step, so you have to elaborate your experience with the associated text you mentioned or your personal experience concerned with the central question. Let's give 2 minutes of time to think about a personal experience and we will start at 1:16pm.

So any experience or incident which happened with the association you mentioned. If you have any incident regarding the associated word, or regarding the central question that is also fine.

Participant 5: The thing is that we, for example I mentioned data encryption and identity access management, that first pops in my mind when we talk about cloud. The cloud is in the public cloud so it means that it is quite vulnerable and can be easily manipulated or hacked. That's what raises concerns for any organization when you are moving your data to the cloud. It contains a lot of confidential data as well and if you are moving the data to a cloud provider like Azure or AWS, they are public cloud, so we are not the only organization putting our data there but there are other organizations as well. And of course it is in the public domain, it's on the public internet and all those things, so there is a quite good chance someone can breach and can access the data. So that is something that you know first came to my mind, what about the data security and user access management. Of course we are working with Rabobank, and with financial institutions, this become much, much important that the data is all safe and secure.

If I have to say about the real life or practical experiences, within our team I am not sure how much you are familiar with the progress of current cloud migration thing, but we are still starting with the migration, so we haven't started using the cloud platform. We are still in the process of migration, learning at the same time what are things we have there. I said this point because I see how this becomes more important to public cloud to have safe your data and have proper encryption of your data. So that there are less chances so we can mitigate the risks of breaching the data and also the proper user access so someone should only access the data only when they have proper authentication and authorization. So does this answer this question?

Researcher: Yes. So this session is for you guys to speak up, there is no right or wrong answer. Whatever comes to your mind, regarding the central question or the text you mentioned in the chat.

Participant 6: As to what Participant 5 was saying, I have something similar that popped up in my mind. When we were working on the hackathon for the team involvement, we were assigned in groups, so that directly links us to Rabobank. We had to encrypt the data if we wanted to do some testing in the cloud, so I think data encryption pops up for me as well.

Participant 3: Add on to that, I also talked about encryption, also something we already do to mitigate the risks like we are not the data owners, we are data warehouse, so the source provides data to us. So to already inform that we are doing cloud migration and also ask them the risks they see to get an overview of it.

Participant 4: Yeah the same way the data leakage problem when you go to the cloud, so I thought the authentication and everything should be well defined.

Participant 1: Ah yes, the question is basically migrating to cloud we encounter some security risks and what cloud tools can help us mitigate those risks. One risk that we encounter at the moment because we are in the phase of transition is to make the on-premise design with on-cloud design in sync, therefore we don't miss any alignment of the design. And how we try to mitigate these risks of missing something, try to share the knowledge into the group together. And it is based on the version control, the first topic that I mentioned. And we try to be really commitment to do that, as much as we can. And may be in cloud there will be some tools to help us to monitor in real time that how much you differentiating from the different times to detect in the migration phase much faster and much easier. And one point I mentioned about easier roll back because when there is version control then you can also mitigate the risk of doing a mistake or missing something so you can easily roll back and again it depends if we use version control in the cloud or not. This is actually what we are practicing.

Participant 2: I mentioned AI because I was triggered by the fact that you mention in your question what possibilities and opportunities do we have. Well we know hackers are weaponing AI and to hack the organizations it is also to know that AI can be used as defensive mechanism, so I saw that of course it is not the general way to do it. But it is a field that is growing and will be growing and that is an opportunity to learn about that as well.

Participant 7: Something we can think about is that eventually the boundary between on-premise infrastructure and cloud infrastructure would be blurry. I mean at some point you cannot say where on-premise ends and cloud starts. So as fast as you can think about the cloud, it is so convenient specially about the security of the data itself but when you think somehow deeper you understand that. On-premise you have a virtual machine at least this is our case, we have some virtual machines with some databases we work in them. So there can be some sort of cloud infrastructure and to be honest, I am not sure where on-premise begins even now and when on-premise ends and cloud begins and I am guessing that in future this boundary will be more blurry and eventually gone.

Participant 5: I can share something, within the Rabobank, because all these concerns about the same data access, encryption and from which network we are trying to access the things, the cloud has this concept called security in-depth concept where we have multiple layers of security for the cloud. So the thing is that, in cloud, I am talking about Azure because I know more about Azure. So in Azure we have this Azure Policy feature which means you are defining some policies which is going to be applicable for the whole organization. So one of the things which we can say when it is not allowed to move your production data to development environment in cloud because there you have other requirements compared to production. Production is more safe, production has more limitations, production has read-view and not the write-view. So there are a lot of other things that nobody who does not have, so anyone who does not have an access to make a modification cannot do the things in the production, so there are a lot of limitations when we see in the production environment and development environment in the cloud. Similarly, you cannot directly provision any resource like deploying let's say any SQL database or anything directly on a production machine. You have to go via pipelines because they are all under the audit things, so every pipeline is under audit and cannot delete or move the pipelines, and that's something I learnt that okay it is not allowed to delete any pipelines to provision a resource on the cloud because everything is under monitor, and is under auditing. So it is continuously monitored as in who is doing what on the production and what sort of data you are pushing to the production, and what sort of data you are pushing to the development. That's one thing and of course there are two ways like one thing is you can push the data from on-premise to cloud and the other thing is that you can push data from cloud to on-premise. So let's see you can see there are two paths and getting the data from cloud to on-premise, there are lot of security and restrictions, but when you move the data from on-premise to the cloud, there is a different set up. So those are the some of things that I came to know and I learnt in the process. That's how we are making sure we are doing every possible way to make the data safe and proper access management in a safe network environment so that you should not enter the network, with a machine or IP address that are not allowed or which should not be there in the network. So all these things I recently came to know in more details how things are happening within the Rabobank so that the data is safe in the cloud.

Researcher: The next step is dream, it's what you would think, given a chance there are no obstacles

or problems in your path, what would you think be the ideal situation? What would be the ideal situation in your dream, if there were no obstacles?

Participant 2: So I was dreaming of a self-running AI software, just scanning our access or infrastructure cloud or on-premise for vulnerabilities and attacks and that is just reporting those incidents or those warnings to human colleagues. They can decide, so it helps in their tasks and work. And in the same time it would do lot more checks, the human kind would be able to do. That would be my dream.

Participant 1: automatically mapping on-premise security setting to the cloud environment; receiving automated warning notification or recommendation for the security setting in the cloud; Have a real-time metric for the level of security maturity of our applications on the cloud Participant 3: When starting the migration we can work side by side in the same location, so we have good communication during the migration process. And when issues pop-up everybody will be informed instantly.

Researcher: It would be good if you could elaborate those solutions.

Participant 1: Similar or follow up to what Participant 2 mentioned. That could be also what you call a dream, that the cloud provider could provide us with some metrics and also recommendation to make our security risks more mature in our application in the cloud. And also it was kind of super dream that it can automatically map our security settings on-premise during the migration to cloud, so we don't have to again so that we don't have to again do it ourselves. May be it is too much request from the cloud provider, but yeah that would be a dream.

Participant 3: Yeah, I thought also when we start migration, we can work side-by-side, so we are in the same location. It would be really nice if it is a villa in Spain. That way we could have good communication and if something pops up, everyone will be informed instantly. It will be easier for us through the whole process.

Participant 7: I think the best ideal situation regarding the cloud is not to worry about the security issues. As most of the concerning points mentioned by our team are regarding security and data breach, so I think the most ideal situation, one can imagine with cloud is to work with it without worrying about too much complexity, and too weak security.

Participant 4: For me, getting clear picture from the cloud competence centre about the security, what level we need to apply for which application or which type of data very clear upfront before we start exactly our development. Then definitely it is a dream because we won't come into any problems later like data leakage or not applying the correct principles later. That's really a good thing, sometimes we do miss for few data or for few stuff, so everything going smooth is a good dream.

Participant 6: For me the ideal situation would be where we don't have to worry about any data related security from the cloud provider or also within Rabobank because they also have some restrictions to go, so then it will be great. So we can just do our thing with the data.

Participant 5: For me also, similar to the others, they mentioned. So for me like as a participant team, the ideal situation would be to focus on all the other things, and for the security part we can have more clear guidance. Also at the same time, it is not only okay to what you shouldn't do but also how can we do that, just a bit more guidance and support on that front. To understand all this security stuff around this cloud is quite vast and at the same time also keep letting us know where we are lagging or where we need to improvise more and getting a continuous support from them. So as a participant team, we can focus on other stuff as well.

Participant 6: In general when you are going to the cloud, by default we have to do some security settings, and also as an organization, within Rabobank, depending on the data you may have settings that we need to and also with respect to data, so if we don't have to worry about it too much, I think that will be great.

Researcher: Anybody else wants to share something else? Moving to the next phase, that is Design phase. In this phase you have to think of how your dream can come true. Who and what is needed to realize the dream of yours?

Participant 5: Yeah I think what I said for the last question that as a participant team, so the thing is that it becomes very much important, of course the security is of top most priority to any organization to have on the cloud but what I want to just continue from what I said for the last question is that it becomes very important for any team who let's say if I talk about our team we are not the security experts, we don't have that much of expertise in security domain because we are just a participant team. Let's say a team who is responsible for bring all certified BI and data warehouse stuff, just we are the team who wants to use the applications available on the cloud. So we have our expertise there, and may be not much on the security domain. So it becomes very important and would be helpful to get a support, to get a guidance from time to time, sort of a continuous guidance throughout the journey for the migration process, regarding the security, and what we have implemented and how it can be improvised, how it can be better. So, that as a participant team we do not have too much worry, or reinvent the wheel to figure out. Of course you can go to the internet and read the things, but when it comes to the practical implementation things are always different. So any team that has experienced implementing those security stuff, having expertise in the security, they know in and out of the concepts, having a support from them for sure help us a lot.

Participant 1: The AI monitoring and recommendation application will be created with assessment team to assists the migrating teams on following checklists and standards. Like an onsite advisor

Participant 3: Ask our Scrum Master too book a room for when we start the migration. Get enough dedicated time within the sprint to really focus on finishing the migration successfully.

Participant 1: My dream is also Participant 2's dream. Using AI, possibility of management, monitoring and also taking the burden off our shoulders when actually going to migrate to the cloud. Cloud monitoring tool and AI recommendation tool, may be can be created by assessment team or another team that help us in pace up migration. As Participant 5 already mentioned, we don't need to put up a lot of time to find out what is the best way, what is the correct way and how to redo the things we already do, because further may be we make a mistake or so, it would be not safe. So more of an onsite advisor, but if it can be automated or programmed based on the AI, which could be much more scalable. Because currently we have this challenge, that we don't have access to well experienced advisors in practice.

Participant 3: For my dream, I would want scrum master to book a room at Rabobank for when we start the migration, and get time in the sprints to finish the migration. And it will be good to have a good internet connection and things like that. From the Rabobank side, we don't have issue of the check point.

Participant 6: I think I will go next, so who and what is needed. From who perspective, it will be nice to have some go-to person that we can ask for any question with respect to security or architecture of the cloud. And what is needed as a team for us, more knowledge and information. There is always nice to have a someone to go-to.

Participant 7: I can go next, needless to say we no need to worry about security and complexity of the cloud. So I guess to reach that point, in my idea if we look into any product, your first found is complicated, not user friendly, so when you go on and in the back the product itself gets more complicated but the end-user, cannot feel it. So I guess, these things happen for the cloud, that the complexity or should move to the back and we as end-users of the cloud will be comfortable in working. I think the necessity is toying because eventually, or I hope the cloud will touch that point. And as Participant 6 mentioned, having someone who fully understands the cloud, can get you through.

Participant 4: Yeah I also completely agree with the team. We need to have the right point of contact of expertise person, and of course the planning and the coordination plays a key role during the time. Actually as a team what exactly we require is what is the data we have, what type of things we have,

we also as a team should be very clear. And we need to be able to explain what do we want to the point of expertise's person. Then yeah of course definitely, we can achieve our dream.

Researcher: This is the last phase of the session. This is deliver, here we talk about the first step which can be taken to achieve the dream we described.

Participant 1: Exploring the possibilities or existing of AI applications that help in monitoring and managing the cloud migration risk; Suggestion of this solutions to the assessment team

Participant 1: My dream was to have an automated, in a way that it suggests or recommends us steps, metrics for the security for the migration to the cloud. First it could be explored if such possibility exists with cloud providers to build that, or how to build that. And then suggest it to the main advisory team in the bank to the assessment team or also the security team. Participant 5 mentioned there is Azure Security Centre at the bank, and may be that's the best team for this suggestion.

Participant 5: It is a feature from the cloud provider. In Azure, we have security centre, which also to some extent integrates the AI capability, which gives you time to time recommendation as to why, which applications are at risk, which are vulnerable, things like that. Security centre and there is one more thing, Azure monitor or something, they have some capability.

Participant 1: Can I ask you question Participant 5? Are there features also then help in migration things?

Participant 5: These are open and available to any team to use. It's up to the team to how they would make use of these things but this is like one of the applications available to make use of, to continuously monitor your risks, health of your applications and everything.

Participant 7: I want to add to Participant 1's suggestion. It will be great to have some recommender systems for usage and picking of the web services in Azure, something about the cost management, so a recommender system for cost management. If they have some functionalities or the options you have in Azure and it can be based on your choices and give you some options or suggestions. I really think that can help.

Participant 3: The product owner and scrum master are going to need some dedicated time for the migration, considering the overall planning process like for the rest of the end-users. There is some form of expectation management during this time.

Participant 4: May for me, to know the existing source system, security principles, what they already applied because these source systems are already in the cloud, may be going forward also. So may be by knowing their already applied security principles, also helps us while migrating to cloud. So that our data can be in line with their security principles. So knowing that information as a first step I think helps us.

Participant 6: May be I can go now, so what I said for us one of the things would be knowledge of the cloud. Also if someone can be there as a go-to person, so the first step, would be getting more knowledge in the cloud and security aspects of it. Or already finding team or some dedicated person, we can reach out to.

Participant 5: Yeah I think for me as well the same like to get in touch with or having some sort of advisor to help us with the initial understanding of the security and what is expected from let's say from a participant team, who are just one of the let's say who are going to make use of one or the other application in cloud. And what are the different security recommendations, if those are defined at the application level. That would be something to start with.

Researcher: Thank you so much for your time. We will schedule another session, once we have a tool or prototype ready.

B

Interview transcripts – Interview 2

Researcher: So there are five phases in the Rabo AI dialogue method. The first one is define

Participant 1: I am not a technical person, but I work closely with EXECUTION TEAM and the security department to learn and to ask if the things are compliant. That's from my point of view, Participant 2 knows a lot more.

Participant 2: From my personal experience from a couple of projects, I would say, integrate the architectural and the security vision with each other.

Participant 1: And they should do it, probably the execution team and the security partners.

Participant 2: And a good example is, do not use IP whitelisting, so taking away a security layer, that is architecture, and security states security-in-depth, every additional layer should be there, so both are completely clashing.

Researcher: So this is like the first phase, to talk about the things that come to your mind when you look at the central question. The next phase is discover, so you have to elaborate your experience with the associated word or the central question. So whatever you mentioned in the first phase, provide an example of an experience with the associated word. Take time to think about the experience.

Participant 1: I experience a lot of procedures and questions, and security-related questions. As Participant 2 said most of them are general questions, to occur within every team, and I was wondering why do we have to answer those questions but it is also related to the thing Participant 2 said, integrated architecture and security. Because a lot of stuff was general cloud stuff and not individual project items.

Researcher: So the teams who were migrating to cloud, they generally asked you these questions.

Participant 1: No, from security point of view, we had to execute cloud risk assessment, and they asked us questions, about security, that in my opinion, were not project related but Rabobank related.

Researcher: So in general the security standards followed by Rabobank?

Participant 1: Yes, they should be applied to the whole Rabobank

Participant 2: I have a very good example with that one. When you have a SaaS application, software-as-a-service, one of the benefits for the team should be that they do not have to assess the vendor anymore because it is pre-decided. And you see the security officers ask me questions like what type of encryption is your vendor using. One this is not a question for a participant team anyways. The participant team do, is responsible for the type of software the vendor is running, and according to the assessment team process, that is being assessed, by security, legal, vendor management, these type

of teams, so you see a complete misalignment is there in the process. And operationally seeing, we run into a lot of headaches, because of the misalignment.

Participant 1: And I experienced, that not the execution team share their knowledge and also the security officers share what they know. But it was as Participant 2 said in the beginning not very click-and-go. You should expect we have a kind of easy way for old, general stuff that we can use, but that was not ready.

Researcher: Do you have something more to add to this, or should we go the next phase?

Participant 2: From my experience, it is the way Rabobank used to work for this, to make every team responsible for every aspect of application in the cloud, that means making general lists, and that means that you are never having in-depth experience on all topics, which security requires.

Participant 1: Yes, another example and it is also security related, we are a reporting team, they ask us to use anonymised data, but we are a part of a chain, and they ask it to every team. So we ask our source systems to provide us with anonymised data, otherwise, we have to do it in our source system. But our source system is dependent on other source systems, so what Rabobank should do it start with the source systems and give them a deadline and then all systems that retrieves data from their source system will get anonymised data at the time, but not make every team responsible. It is taking a lot of time in discussion, it is very ineffective if you do it like this.

Researcher: I will go to the next phase, so the next phase is dream. What would be the ideal situation in your dream if there were no obstacles? So what would be your ideal situation for a secure cloud migration would look like?

Participant 2: My ideal situation is that they think about intermediate architecture being in place. So you see we have a perfect architectural vision but there is no way of integrating all the components at the moment, when you follow it. So then you need to reach out to global architecture as a single team as to find out which solution few teams are using, so a more integrated approach within the infra team.

Researcher: So the architecture design, is it done by a participant team in the migration process or is there a separate team for that?

Participant 2: We have an infrastructure platform centre, they have a cloud architect and then they describe the architecture going forward. And creating architecture forward in place is like putting a dot on the horizon and it has and it has all sorts of dependencies. And not all the dependencies are in place yet. So you need to find a temporary solution to get your system up and running, which is delaying a lot of teams and causing security risks as well. Researcher: And are these architectures designed on the basis of requirements from the team or based on the high level overview that the cloud architect already have?

Participant 1: Yeah, a very high level overview and as Participant 2 said, no intermediate steps in between. So an endpoint to reach that in a couple of years, but we have to deal the current situation, functionality is not there, architecture, components are not there and what do we have to do then. If I can dream, I would like to have an architectural team with a Participant 1: Yeah, a very high level overview and as Participant 2 said, no intermediate steps in between. So an endpoint to reach that in a couple of years, but we have to deal the current situation, functionality is not there, architecture, components are not there and what do we have to do then. If I can dream, I would like to have an architectural team with a vision, but also a team that can create components, and handle. And not only from execution team but also from architectural point of view. Not only you can do this, or that or this works like this but also advice, because you have some types of applications, and it would be nice to tell an expert, that I have this type of application that he says well, concerning our components, use this, this or this. For example, all teams have to figure that out and in all teams you have the discussion as to what is best but you don't have the knowledge.

Participant 2: So we need more guidance, and hands-on guidance. For example, what would really help us if security officers doesn't give us a form to fill in without any guidance. And if you are looking into the informational section, the security assessment section that we do in a tool called Sherlock, if you look, it is a minimum of 96 questions including cloud. And if you have question on any of these questions, you can click on the "i", and then you are forwarded towards a sharepoint site with 90 pdfs. And there is no way anyone can keep up with all those pdfs because they change as well. So you really need a better guidance there. So to get more secure applications, the team needs to know what they need to answer for those questions. And over the years, I have seen the distance between the security and the teams is getting bigger instead of smaller.

Participant 1: And also for example, for a few projects we need to load files, to upload files to the cloud, so we built a solution for that. We had to add security measures of course, and kind of architecture, but it is very normal to load files especially in this phase, when not every application is in the cloud, to load files from on-prem to cloud, otherwise you won't get data in the cloud. So that the basic thing, that every project will need, and for those basic functionalities, they can create a general solution. For example, we also have to make corrections in the cloud, then we create a correction tool, and there seems to be a basic, generic correction tool and we have to use that. But we have to build our APIs ourselves, I am not sure if we can do that secure, but it is a basic functionality that all teams will need in one way or another. They are the generic components that can be provided. And I think that will help us in building faster and also being more secure.

Researcher: So you mentioned about transferring files from on-prem to cloud, so if such tools don't exist, is there a possibility that the files might get lost or file might get corrupted?

Participant 1: No, they won't get lost but we have to build our own solution, and that takes time. If we don't build them, it is a risk.

Participant 2: Because we are building the same wheel lots of times, the question is if they are built in the same, secure way?

Participant 1: And if security standards change, and they will change with time, every team will have to apply the changes to their generic functionality. And if you have generic components, only one team will have to do it.

Researcher: So what you are saying is a generic tool or component for the whole organization?

Participant 1: Yeah it would be better, more maintainable and cheaper. Sometimes it is very handy to have an expert that you can hire only for one week, if you have any big problem, they can help you hands-on, your teammates can help you hands-on. Well we have that, from Microsoft a guy, he is very busy, but it would be nice to have a specialist that can support a team, hands-on specialist, not the procedures specialist.

Researcher: So the next phase is design, you have to tell who and what is needed to realize your dream.

Participant 2: Let's first start with a what I guess, what is needed is a closer cooperation between the departments, not living in sidelines, and feeling a bit of responsibility for their sideline. That's when you get an integrated solution, instead of two solutions, remaining besides just pure of responsibilities. So who, you need to get management on-board with this one. The other thing is who is going to fund this, when you are trying to set up a generic team, it needs to be funded. Because they cannot cross-charge it to a single team, because a lot of teams are using it. There is no dedicated budget because it has to be requested for a purpose, and somebody has to pay the bill. So in the end we are paying a way higher bill, because of no alignment upfront.

Participant 1: I think I agree with Participant 2. I think budget is one thing, but a hands-on generic team would be nice. Atleast start now, with learning from the cloud projects that are already in the cloud and try to find the generic components. And try to make the plan, that the teams can reuse and lower their

budgets for maintenance.

Researcher: The last step is deliver, the first step which we can take to make an impact.

Participant 2: I would start evaluating some of the projects, which already went to cloud, and really listen to them, what they are experiencing. And then create a plan going forward or decide that we keep on doing the same way. So yes, I would start evaluating projects and see where they lose time, where they lose the money because of time.

Participant 1: And focus on hands-on security guys.

Participant 2: That's one of the bad parts as well. When we start requesting security people, they are Raboank's security people, they will be hired and they are not aware of the organization's that was in place. These people have a long learning curve because our infrastructure is not that easily set up after so many years.

Participant 1: And may be organize knowledge sessions for starting teams about the first steps, what are the basics of the security and really help the team with the practical knowledge, not theoretical, not telling what we can or cannot do, but really practical information related to Rabobank's security standards.

Participant 2: Provide solutions instead of advice.

Participant 1: Provide solutions and knowledge about the solutions.

Participant 2: We have really good people on the security side, but the knowledge is not transferrable, or it is being tested by asking the teams to fill in the security assessment questions. Believe me I can fill all sorts of things in the security assessment questionnaire, and nobody is actually testing it. I see that we have a pen test now, what they do is review but somebody will look into what's code and what's actually being deployed. That's a big way.

Participant 1: That's a step forward, just to review and evaluate the projects to discover generic functionalities. I think it covers smaller, bigger mistakes.

Researcher: Thank you so much for your time. We will schedule another session, once we have a tool or prototype ready.

C

Interview Transcripts – Feedback Interview 1

Researcher: Hello, the main aim of this session is to summarize the findings of my thesis, and get your feedback regarding the findings. Starting with the main research question, which is “How can Rabobank mitigate numerous challenges and security-related risks triggered in the process of cloud migration?” To answer this question, I have defined sub-questions to understand the current migration process at Rabobank, different stakeholders involved in the process, challenges faced by the stakeholders and innovative ways to mitigate these challenges.

These are the list of identified problems from the data analysis, no access to experienced cloud advisors, lack of information on data carriers, lack of knowledge related to security, no inter-team knowledge sharing, lack of measures for data migration, and the inefficiency of risk assessment in the migration process.

Participant 1: So for the first point, the teams didn’t where to go or they went to some people and they said we don’t have time or the availability to help you?

Researcher: Yeah so they mentioned that during the process of migration, there wasn’t one person available to them to whom they can go and ask all the questions.

Participant 1: Okay, and they didn’t find it?

Researcher: Yes, they felt that kind of cloud advisor is not available to them right now.

Participant 1: Okay because there are advisors available at Rabobank. We have a specific program and those guys are experienced engineers and you can reach out to them and say that you need help in the coming weeks or whatever in getting started with the whole migration. They don’t have a lot of resources, so that could be the reason. Or the information is not enough to support the team.

Researcher: Regarding the first point, team that has migrated to cloud, they said they didn’t have a go-to person to whom they could talk to about cloud related queries. They asked around and they received theoretical answers, rather than the practical ones.

Participant 1: Regarding the third point, the shift of responsibility is moving away from a centralized team. The teams need to step up their games regarding security part and the whole development process.

Regarding the fourth point, we have something called Cloud community, where we give presentations and it has been hosted to now 1500 people, that are all doing cloud migration. So if you have any

problem, you can put it up on Teams and someone will definitely answer your question.

Researcher: I think the teams are not aware of such initiatives being taken. And that's why such issues keep coming.

Participant 1: For the last point, I think a team member is assigned to a specific team from the assessment team and helps you go through the assessment team. And if some difficulty is faced or not cleared, they should reach out to that guy. May be it's not documented properly or not made aware to the teams.

Researcher: The next slide is security risks, containing security risks identified in the process like data loss, data breach, insecure system, unauthorized system access, service discontinuity, monetary loss, insecure APIs. The teams felt that there are generic tools to develop, and they are not aware of security standards completely, this lead to insecure functions.

Participant 1: So these are the security risks that the teams pointed out. Did they have a follow-up after that for insecure APIs?

Researcher: I am not sure. If they did, it wasn't part of this process.

Researcher: In the next slide, I have created a correlation between the identified challenges, and the security risks. It is clear that most of the challenges would lead to insecure systems, and that would lead to data loss, data breach, etc. and these in turn would cause monetary loss.

Participant 1: It's always about the money. But the other damage that the bank might face would be their reputation. If these things go to media, you get negative attention.

Researcher: In the next slide, I have prioritized the requirements using MoSCoW method. The must-haves are the ones to take care of immediately, should haves will be next, could haves, after that and then the last category. These requirements have been gathered from the two interviews that I conducted.

Participant 1: Regarding the one team to develop the generic components, we also discussed it sometime back. Rabobank, as a company, follows anonymity of growing their own systems, rather than going to a centralised team to create changes in their applications, because that would take a lot of time. And now the possibilities we have in cloud, the teams are responsible for their own security but also they can put up their own timelines to update or change the security of their applications. And when you look at the past, with on-prem, you have to put up an RC or a change request to change your application, and that could take 2-3 weeks. In that time they could get start the work on their own. It's like Spiderman, with great power, comes great responsibility. But this is the way of working Rabobank chose. If the team is not mature enough, then they should not go to cloud yet. They should invest time to gain some proper knowledge before they go to migration.

But it is interesting to see what teams have encountered.

Researcher: Next slide, is categorization of requirements which has been derived from the shared responsibility model used by CSPs. There are three categories, requirements for security in the cloud, which can be taken care by Rabobank as a customer, and then the requirements for security of the cloud for CSPs to take care of. One team had certain requirements using AI as a tool to make recommendations for the security controls and cost management. This is already been taken care by the CSPs in the form of new services like Azure has azure security centre. The ones which Rabobank can take care of, knowledge about various security measures, knowledge sharing within teams, transfer of knowledge from execution team and other. These are the ones that have been focused for the development of a solution. The common ones are safe and secure data and proper authorization and authentic measures, which can be taken care by both CSP and the customer.

Participant 1: Normally it's two layers in the shared responsibility model. So CSP is responsible that

nobody can access the data and store it in a secure way. But as a customer you can check if the data is stored in a secure way, if the data is encrypted. So this is a combined responsibility, but they are on different layers, like technical layer. The other one is where customer is responsible to check all the boxes.

Researcher: Okay, that's a good feedback. I will keep the two layers.

The next slide is, I have translated the requirements into features for the solution. So knowledge about security controls and data encryption can be translated into a knowledge base. Knowledge sharing within teams and information about migration process, it can act as an information centre. Then architecture design, proper planning and efficient assessment process as planning & stakeholder management. And the learning part of the teams can be translated into learning. The solution is still a concept with these features.

I am calling the solution Cloud Catalyst, first as knowledge base or knowledge management platform, teams can get access to different knowledge about security controls and principles, knowledge about Rabobank's security standards, and knowledge about different CSPs.

Participant 1: I think that's one of the key point you have put out there. The information is there, but teams find it difficult to access it.

Researcher: The second feature is information centre, when one team migrates to cloud, it is good to see what other teams faced in the process of migration, learn from their mistakes. It is similar to how you mentioned that resources like cost, time is wasted. The migration can be done properly if teams are aware of challenges they might face. So the solution will act like an information centre, and the new teams could see the stories of the old teams and contact them if anything pops up. This would enable knowledge sharing between the teams. It could also act as an information centre for the new teams planning to migrate.

Planning & Stakeholder management is there to streamline the process. So participant teams can put up their requirements, and different stakeholders like architecture team and execution team can assist them in developing an architecture aligned with Rabobank's security standard. It can open communication channels and enable feedback at every step of the process.

Participant 1: Before somebody goes to cloud, or they are on boarding to cloud, first they will get a presentation from the execution team explaining what is cloud, where to look for it. But I agree, it's all over the place. The team will get a presentation from the execution team telling them this is what you have to do. Then they have to go through the assessment process, without that they cannot go live with application. The assessment team members are supposed to help them.

But this is part of the process, that they can talk to the execution team and members are assigned.

Researcher: I agree, but this issue has come up again and again, so may be with this tool the process could be made clearer to the participating teams. At every step, the teams could ask questions and provide feedback and communicate properly regarding planning and availability of people.

Participant 1: Yes, that can be done. Because we don't have a lot of people in the execution team. And when teams migrate to cloud, after that they are responsible for their services. Then they cannot come back to us, to ask what's wrong with it. We can help them in the initial phase, but they need to know the a to z part of their system.

The last point learning is very important in this. They should have enough knowledge within their team to be self-sustaining.

Researcher: That's where the last part comes in, learning tab can handle the learning part of the teams, provide them information on different certifications, and learning programs at Rabobank. Teams starting to migrate can track their teammates' learning levels and proceed to migration process accordingly.

Participant 1: So from the planning team, they have a program that stimulates the teams to go to cloud. They call it a cloud wired licence, where the teams need to have a certification before they can go to cloud.

Researcher: My objective is to streamline the process, and ensure knowledge sharing by this tool. There are multiple platforms, that cause chaos during knowledge management.

Participant 1: Yes I agree with this. I think the whole information set up is not ideal right now. So if we have somewhere or someplace, where all this information is combined, that will be good. Multiple teams are involved in the process, so one place where all this information is possible or one page to redirect you to the right place should be there.

You get a good point on the problems of the team here.

Researcher: Thank you for your valuable feedback

D

Interview Transcripts – Feedback Interview 2

Researcher: Hello, the main aim of this session is to summarize the findings of my thesis, and get your feedback regarding the findings. Starting with the main research question, which is “How can Rabobank mitigate numerous challenges and security-related risks triggered in the process of cloud migration?” To answer this question, I have defined sub-questions to understand the current migration process at Rabobank, different stakeholders involved in the process, challenges faced by the stakeholders and innovative ways to mitigate these challenges.

These are the list of identified problems from the data analysis, no access to experienced cloud advisors, lack of information on data carriers, lack of knowledge related to security, no inter-team knowledge sharing, lack of measures for data migration, and the inefficiency of risk assessment in the migration process because the process involves filling multiple forms without any knowledge of what to fill.

Participant 2: Yes, this is similar to many processes. For a privacy related work, we had to fill many forms and we didn’t have much knowledge about those things.

Researcher: The next slide is security risks, containing security risks identified in the process like data loss, data breach, insecure system, unauthorized system access, service discontinuity, monetary loss, insecure APIs. The list has been updated as monitoring and reporting is being taken care by execution team via azure security centre.

Participant 1: Okay.

Researcher: In the next slide, I have created a correlation between the identified challenges, and the security risks. It is clear that most of the challenges would lead to insecure systems, and that would lead to data loss, data breach, etc. and these in turn would cause monetary loss and reputation loss.

In the next slide, I have prioritized the requirements using MoSCoW method. The must-haves are the ones to take care of immediately, should haves will be next, could haves, after that and then the last category. These requirements have been gathered from the two interviews that I conducted.

Next slide, is categorization of requirements which has been derived from the shared responsibility model used by CSPs. There are two categories, requirements for security in the cloud, which can be taken care by Rabobank as a customer, and then the requirements for security of the cloud for CSPs to take care of. Previous team had certain requirements using AI as a tool to make recommendations for the security controls and cost management. This is already been taken care by the CSPs in the form of new services like Azure has azure security centre. The ones which Rabobank can take care of, knowledge about various security measures, knowledge sharing within teams, transfer of knowledge from execution team and other. These are the ones that have been focused for the development of a

solution.

Participant 2: So a cloud service provider, who would be an example of that?

Participant 1: Microsoft

Researcher: Yes, Azure would be an example for that. So Azure with its various services takes care of monitoring and recommendation. But the first part is something which Rabobank can take care of.

Participant 1: I have one question regarding your problem statement. When you talk about security of migrating to cloud, I think every CSP have a general standard for security. It is not something which is choosable for its users. But I don't think we have any control over those services.

Researcher: Yes, so right now the kind of services they provide, we don't have a very much control over that. So security of the cloud is something which is their responsibility. Now security in the cloud is something which we can take care of by making use of security policies as per our needs. You can take care of your own services, and that's where you have the flexibility of maintaining and designing things on your own.

Participant 1: So the part that we can control is the customer part. And the CSP part, is something we need to accept what is provided by them.

Researcher: Yes, so for the design of solution, I have focused on the customer part.

Participant 1: Okay, that makes it clear.

Researcher: The next slide is, I have translated the requirements into features for the solution. So knowledge about security controls and data encryption can be translated into a knowledge base. Knowledge sharing within teams and information about migration process, it can act as an information centre. Then architecture design, proper planning and efficient assessment process as planning & stakeholder management. And the learning part of the teams can be translated into learning. The solution is still a concept with these features.

Participant 2: So the knowledge base, is something you can compare it as a book. The information centre can be seen as a channel or a telephone line where you can communicate with one another. The book is say is there for acquiring knowledge like a knowledge base.

Researcher: Yes, that's a good comparison. Moving on to the more description of the features, I am calling the solution Cloud Catalyst, first as knowledge base or knowledge management platform, teams can get access to different knowledge about security controls and principles, knowledge about Rabobank's security standards, and knowledge about different CSPs.

When one team migrates to cloud, it is good to see what other teams faced in the process of migration, learn from their mistakes. It is similar to how you mentioned that resources like cost, time is wasted. The migration can be done properly if teams are aware of challenges they might face. So the solution will act like an information centre, and the new teams could see the stories of the old teams and contact them if anything pops up. This would enable knowledge sharing between the teams. It could also act as an information centre for the new teams planning to migrate.

Planning & Stakeholder management is there to streamline the process. So participant teams can put up their requirements, and different stakeholders like architecture team and execution team can assist them in developing an architecture aligned with Rabobank's security standard. It can open communication channels and enable feedback at every step of the process.

Participant 2: I have an idea for the information centre. You said it could enable knowledge sharing. But I would say you could also say that it promotes knowledge sharing. So that t is interesting for

people that they find it interesting to share their knowledge somehow. Then otherwise it means it is enabled but it wouldn't mean a lot. But if people are motivated and remember that how easy or difficult it was when they started out but how easy it became when you received help. Well that's one line of motivation. Or there could be a point system like Stack overflow, where people get points, so they will motivated and encouraged to share their knowledge.

Researcher: That's a good idea of putting gamification in the process.

Learning tab can handle the learning part of the teams, provide them information on different certifications, and learning programs at Rabobank. Teams starting to migrate can track their teammates' learning levels and proceed to migration process accordingly.

Participant 1: For this solution, is there any order for the implementation? Or these are all at the same time or at the same level of implementation?

Researcher: This can be done as the first step of the implementation, to decide an order of implementation.

Participant 1: Yes, because at the migration phase, usually teams have mixed skill levels and at the same time they want to move forward with the planning, so there is no consecutive steps for this. At least in our team, we plan to learn things on the go, and also move forward. Because if you take time to prepare, you will left behind. This is something which could be challenging to define a very best practice for that. But the different components, they look fine.

Participant 2: So these four items, do they correspond to the features in the last slide?

Researcher: Yes

Participant 2: Okay, then the components look good.

Participant 1: May be one thing that can be added in this is that teams which that migrated to cloud successfully, people from those teams could join other teams and boost and help with that team. This could be added to the planning & stakeholder management.

Researcher: Yes, sure. Thank you for your valuable feedback.

E

Interview Transcripts – Feedback Interview 3

Researcher: Hello, the main aim of this session is to summarize the findings of my thesis, and get your feedback regarding the findings. Starting with the main research question, which is “How can Rabobank mitigate numerous challenges and security-related risks triggered in the process of cloud migration?” To answer this question, I have defined sub-questions to understand the current migration process at Rabobank, different stakeholders involved in the process, challenges faced by the stakeholders and innovative ways to mitigate these challenges.

These are the list of identified problems from the data analysis, no access to experienced cloud advisors, lack of information on data carriers, lack of knowledge related to security, no inter-team knowledge sharing, lack of measures for data migration, and the inefficiency of risk assessment in the migration process.

Participant 1: The second point is actually related to business side as well. One of the questions that business gets is to indicate the impact of data loss. This is not really an IT thing, it is for business. How can an IT team understand the risk, if business doesn’t understand the actual process. It is very hard to put a figure or rating to show if this data is lost, this is the exact behaviour.

Researcher: The next slide is security risks, containing security risks identified in the process like data loss, data breach, insecure system, unauthorized system access, service discontinuity, monetary loss, insecure APIs.

Participant 1: I was looking for business continuity, but that is related to service continuity. Also if you want to pull out more security risks, you can always do that.

Researcher: In the next slide, I have created a correlation between the identified challenges, and the security risks. It is clear that most of the challenges would lead to insecure systems, and that would lead to data loss, data breach, etc. and these in turn would cause monetary loss and reputation loss.

Participant 1: These are the ones that matter the most.

Researcher: In the next slide, I have prioritized the requirements using MoSCoW method. The must-haves are the ones to take care of immediately, should haves will be next, could haves, after that and then the last category. These requirements have been gathered from the two interviews that I conducted.

Next slide, is categorization of requirements which has been derived from the shared responsibility model used by CSPs. There are two categories, requirements for security in the cloud, which can be taken care by Rabobank as a customer, and then the requirements for security of the cloud for CSPs

to take care of. Previous team had certain requirements using AI as a tool to make recommendations for the security controls and cost management. This is already been taken care by the CSPs in the form of new services like Azure has azure security centre. The ones which Rabobank can take care of, knowledge about various security measures, knowledge sharing within teams, transfer of knowledge from execution team and other. These are the ones that have been focused for the development of a solution.

Participant 1: We see that now a days Microsoft is popping up with so many vulnerabilities that are not aligned with Rabobank's security standards. They say well it's just Azure popping up vulnerabilities. For example, a nice one would be that your data is not classified, there is no requirement that your data is classified on a sensitivity level within the databases. Rabobank's requirement is that it is classified, and the information is stored and your system is built accordingly. Now Microsoft popping up new stuff, just displays negative on the dashboard. People are like why aren't you picking this up. My first question is would we have to pick it up as per our standards or according to Microsoft standards, or are they trying to push new feature.

Researcher: The next slide is, I have translated the requirements into features for the solution. So knowledge about security controls and data encryption can be translated into a knowledge base. Knowledge sharing within teams and information about migration process, it can act as an information centre. Then architecture design, proper planning and efficient assessment process as planning & stakeholder management. And the learning part of the teams can be translated into learning. The solution is still a concept with these features.

I am calling the solution Cloud Catalyst, first as knowledge base or knowledge management platform, teams can get access to different knowledge about security controls and principles, knowledge about Rabobank's security standards, and knowledge about different CSPs.

When one team migrates to cloud, it is good to see what other teams faced in the process of migration, learn from their mistakes. It is similar to how you mentioned that resources like cost, time is wasted. The migration can be done properly if teams are aware of challenges they might face. So the solution will act like an information centre, and the new teams could see the stories of the old teams and contact them if anything pops up. This would enable knowledge sharing between the teams. It could also act as an information centre for the new teams planning to migrate.

Planning & Stakeholder management is there to streamline the process. So participant teams can put up their requirements, and different stakeholders like architecture team and execution team can assist them in developing an architecture aligned with Rabobank's security standard. It can open communication channels and enable feedback at every step of the process.

Learning tab can handle the learning part of the teams, provide them information on different certifications, and learning programs at Rabobank. Teams starting to migrate can track their teammates' learning levels and proceed to migration process accordingly.

Participant 1: The learning part I don't fully agree upon. Of course it is good that people have certifications. But one thing is something you don't get from these certifications. That's why I have never taken such certifications myself because the knowledge I am lacking is not given by these courses, which is really annoying. The courses Microsoft provides focuses on working with Microsoft Azure Data factory, working with Azure SQL, working with components. But the knowledge people are looking for is how to integrate the components. And that's a difficult course to create, but that is exactly the knowledge teams are looking for. That's where security comes up, that's where networking is popping up. While networking is new for the most of the development teams at Rabobank when dealing with infrastructure. So you see it is good to have such certifications, but the knowledge people need is you cannot gain from these certifications, but they do not give information on integrating the components. This is something I have experienced.

Researcher: It is a good feedback. Do you have specific feedback to te solution I proposed?

Participant 1: I like the solution you proposed. I see that it highlights the problems I face and I know the other teams are struggling with. If you look at the features, open communication channels for stakeholders. At times, for some issues, we need to raise ticket here and there, and then you wait for people to respond. And in that moment they are shifting their focus to something else, because a ticket is asynchonised and one time you will get contacted by the team, and the other time you see a response on the Azure Devops ticket, other times you see a response in other channel. All sorts of different information comes when asking a question. And we need to use all sorts of different systems for asking a question, which makes it difficult for people to find the correct answer.

Researcher: It is a relatable feedback and issue. So this platform can be used as a single place to raise questions regarding the cloud migration. If you have a particular question for assessment team, or execution team then the assigned person can answer the question.

Participant 1: The assessment process is a bit funny. So we have a cloud exit strategy here at Rabobank, and I asked them what would Rabobank do in total if we exit from Azure. So which steps will be taken care of and which ones will be generic, and which gaps does a team needs to fill in. These questions are asked by multiple teams, how am I supposed to be knowing what will be in place in whole of the Rabobank, which gaps I still need to fill in so regarding the cloud exit strategy, I see the most creative answers popping up there.

Looks like you had an interesting thesis topic there.

Researcher: Yes, thank you for your valuable feedback.