Universiteit Leiden

ICT in Business and the Public Sector

A GDPR cloud migration risk strategy for retail banks

Name: Jousuf Mohamed
Student-no: s2479540

Date: 04/05/2021

1st supervisor: Prof. J.B. Kruiswijk
2nd supervisor: MSc. Mohammed Atef Ibrahim

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgements

First and foremost, I convey my gratitude for the support, feedback, and continuous guidance of my first and second supervisor, Prof. J.B. Kruiswijk and MSc. Mohammed Atef Ibrahim. They have been essential for this research project. Without their patience and involvement, the outcome of this research would not be as it stands.

Secondly, I would also like to convey my appreciation to the interviewees, most importantly Marcel Brakeboer, Daniel Rademaker, Steve Rackham, Ivo Verhaeghe, Massoud Houssein, Simon Janssen, Mauro Meeuws, Sriya Badloe and all other interviewees. They offered me the primary source of qualitative data whilst conducting this research study.

Lastly, I would like to thank my family and friends who have personally provided me with supportive discussions and guidance throughout the essential moments of this research's writing process.

A GDPR cloud migration risk strategy for retail banks

Jousuf Mohamed

Leiden Institute of Advanced Computer Science (LIACS), Niels Bohrweg 1, 2333 CA
Leiden, The Netherlands

June 28, 2021

Abstract

This research study explores what GDPR risks are barriers to cloud data migrations in retail banking, whilst offering strategies on how to navigate these barriers as well. Within this study the definition cloud data migration is identified within the context of retail banks. The specific type of cloud migration relevant to the study will be defined, and this definition will serve as a scope for the research. The risks and risk strategies regarding GDPR compliance in retail banks when conducting the defined cloud migration in the scope are identified as well. The data sensitivity and the risk of adoption regarding regulatory requirements are the main factors that are considered when conducting this research.

The nature of the research was qualitative; therefore, the data gathering was completed by literature reviews and semi-structured interviews. To conduct the research study, a literature review was completed to research existing literature regarding cloud migration, GDPR laws and risk strategies. To gain qualitative data from the retail banking sector, interviews were conducted with industry experts from retail banks and IT (consulting) companies such as NetApp, De Nederlandsche Bank, ABN AMRO, NIBC Bank, Ordina and Capgemini.

The main research question is: “What are the retail banking cloud migration risk management strategies in compliance with GDPR regulations?”
Sub-research questions include the following:

1. What defines a cloud migration in the context of retail banking?
2. What are GDPR compliancy risks within a retail bank related to cloud migration?
3. What are the risk management strategies in response to the GDPR compliancy risks?

The major results indicate that there are six main GDPR risks: fines, data leaks, reputational damage, cyber security threats/ hacking, losing the banking license, and the cloud provider selling data to external parties for profit. The risk management strategies are described in Chapter 5.1 and 5.2. Strategies include data privacy assessments, GDPR software usage, deploying a GDPR policy mitigation team, reviewing cloud provider certification and more. This research is important and benefits the academic and corporate world because it offers a guideline of risk management strategies for data privacy officers and CISO’s in retail banks making decisions regarding GDPR related policy upon assessing cloud migration possibilities.

Table of contents

List of figures

List of tables

List of abbreviations

PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
IaaS	Infrastructure-as-a-Service
GDPR	The General Data Protection Regulation
AWS	Amazon Web Services
NIST	National Institute of Standards and Technology (U.S. Department of Commerce)

Chapter 1 Introduction

For the creation of my final master's thesis, I have set sight on offering a risk strategy for banks who have not yet fully adopted cloud technology but are planning on taking this leap of faith by making investments in their IT-infrastructure and migrating their (on-premises) data to the cloud. The aim of this research study is to identify risks and risk strategies for retail banks adopting cloud computing services, with focus on the specific risks regarding GDPR compliancy. The study was undertaken to gather data on GDPR compliancy risks and strategies when migrating data to cloud computing providers in retail banks.

1.1 Problem statement

Migrating data to an external cloud service provider as a retail bank has its benefits, downsides, and risks, despite these often-complex factors influencing the decision-making of banks, McKinsey predicts that more banks will be migrating their data to the cloud in the future (McKinsey, 2016).

Considering that retail banks will invest their budgets into migrating to the cloud, a vulnerability in data security and privacy is created due to an increased dependency on cloud providers when granting access to client data.

Problem statement: Retail banks require guidance on how to migrate their data to the cloud whilst being GDPR compliant.

Cloud migrations require corporate data to be migrated to an external cloud service providers' IT-infrastructure environment. Migrating corporate data with an external party to benefit from the advantages of cloud services serves the corporate interest of a retail bank. Yet, multiple categories of risk ought to be managed before a migration can successfully and safely be conducted in compliance with corporate and legal regulatory requirements. Including risks of security breach, legal risks, and data privacy risks. These risk categories can prevent retail banks from migrating their data to the cloud. This research study explores the data privacy risks and focuses on the regulatory compliance regarding GDPR.

Retail banks process different types of data, regarding the aspect data sensitivity, their data could be categorized as non-sensitive and sensitive personal data. Non-sensitive data can be defined as data that does not contain personal information and therefore will not affect an individual person's privacy (Directive (EU) of the European Parliament and of the Council, 2015).

Personal data however is defined by the GDPR document Art. 4 "Definitions" as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Directive (EU) of the European Parliament and of the Council, 2015)

The European Commission defined several conditions for organizations/companies regarding accessing sensitive personal data such as "the explicit consent of the individual being obtained" and "an EU national law or collective agreement requiring you to process the data for employment, social security etc. to comply with its obligations and rights". Sensitive data is protected under the data protection law (European Commission, Directorate-General for Communication, 2020).

Certain banks are not moving their data to the cloud or only migrate non-sensitive data to the cloud because of the risks regarding regulatory compliance. Which means that they are not reaping the benefits of cloud technology. GDPR compliance risks can be categorized based on the GDPR "principles relating to processing of personal data" from Art. 5 GDPR:

1. Lawfulness, fairness, and transparency,
2. Purpose limitation,
3. Data minimization,
4. Accuracy,
5. Storage limitation,
6. Integrity and confidentiality,
7. Accountability (Directive of the European Parliament and of the Council, 2014).

Offering risk management strategies for the privacy risk aspect of cloud migration leads to risk strategies to remain GDPR compliant. Therefore, the following research questions arise:

Main research question: "What are the retail banking cloud migration risk management strategies in compliance with GDPR regulations?"

Sub-research questions:

1. What defines a cloud migration in the context of retail banking?
2. What are GDPR compliancy risks within a retail bank related to cloud migration?
3. What are the risk management strategies in response to the GDPR compliancy risks?

1.2 Research gap

The main research gap that is addressed is that there is limited research exploring how the cloud can be adopted whilst being GDPR compliant and managing risks of not meeting the GDPR requirements, including fines and reputation damage. Especially focusing on a specific domain within the banking industry such as retail banking. Therefore, the study tends to explore the adoption of cloud computing services with whilst considering risk management strategies based on several risk categories in GDPR. Financial regulations, data sensitivity and security needs are to be considered by the banking sector when making decisions. Yet, strategies on how banks should manage the risks of not meeting compliance requirements are not directly retraceable in current literature. This research study aims to fulfill that gap in literature.

1.3 Research approach

The research approach will be outlined in further detail in Chapter 3, which is the methodology. In the following outline, an overview will be given on the main objective per research question and through which method these objectives ought to be achieved.

“What are the retail banking cloud migration risk management strategies in compliance with GDPR regulations?”
This is the main research question, which will be answered lastly, to answer this question, sub-research questions were made. A plan for the collection of data to answer every sub-research question was constructed. Afterwards, an objective per question regarding the quality and relevance of the data and conclusions per sub-research question was used to ensure if the question was answered properly. The structured approach of:

- determining the question,
- the research objective per question,
- the data collection method,
- the data quality review/discussion,
- the data analysis or interpretation
- and the conclusion.

Eventually, every single conclusion and data interpretation is combined to answer the main research question. The research approach is divided into three phases which each contain one sub-research question. This would be the:

- The exploratory phase,
- The cloud migration definition & GDPR risk identification phase,
- and the GDPR risk strategy phase.

The research approach for all sections is described in detail below.

The main qualitative data collection methodologies that were used for this research question consists of two methods, the literature review, and systematic semi-structured interviews. The results from the literature review will be descriptive in nature. The interviews on the other hand will be focused on collecting new information and be exploratory in nature. The semi-structured interviews consist of three phases displayed in the table below.

Interview phases	**Phase name**	**Interviews**
Phase 0	Exploratory	2 exploratory interviews
Phase 1	Cloud migration definition & GDPR risk identification	9 in-depth interviews
Phase 2	GDPR risk strategies	8 in-depth interviews
Total	Finalize transcriptions	19 interviews

Table 1: Interview phases

Phase 0 - Exploratory

To start of the interviews, two exploratory interviews were conducted with two experts in the industry (‘lead data scientist in IT consulting firm’ and a ‘cloud & banking senior solutions engineer at a cloud provider’). This gave the opportunity to test and review the question list, research approach, potential answers, understand the several fields of compliance, risk management, cloud data migration and banking correctly regarding the research questions with the assistance of two experts. The feedback received allowed the question list to be reviewed and improved. After gaining insights in the exploratory interview phase, the two in-depth interview phases could be started.

Phase 1 – Research question 1 and 2
Hereby, the cloud migration definition is explored in phase 1 together with the risk identification of GDPR risks. Which is why this phase is named "Cloud migration definition & GDPR risk identification", to showcase, that every in-depth interview involved questions starting the cloud migration definition and afterwards questions regarding GDPR compliance risks. The qualitative data collection methodologies for the second research question consists of two methods, the literature review, and systematic semi-structured interviews.

Research question 1: What defines a cloud migration in the context of retail banking?
The literature review for research question 1 was aiming to collect relevant literature on cloud computing infrastructure, cloud migrations, cloud migrations within retail banks, sensitive data and GDPR's cloud related aspects.
For the first research question, the 2 exploratory interviews in interview phase 1 and 7-8 in-depth interviews were conducted in interview phase 2 with GDPR, banking and consulting professionals. The aim with the interviews is to collect information on how cloud migrations are defined in the context of retail banks, whilst considering the type of migration (data, application, infrastructure), deployment models, cloud strategy and data sensitivity.

Research question 2: What are GDPR compliancy risks within a retail bank related to cloud migration?
The literature review for research question 2 aims to collect relevant literature on GPDR compliance, GDPR risks, sensitive data leaks, data privacy, GDPR in cloud migrations and GDPR in retail banks.
The semi-structured interviews consist of 8 in-depth interviews with IT banking professionals, data scientists, GDPR consultants, cloud consultants, privacy & cyber security professionals. The literature review ought to provide an overview of supportive literature material on GDPR compliance risks and consequences such as fines, data leaks and reputation damage. The interviews are conducted to understand what specific risks occur related to cloud migration within a retail bank.

Phase 2 - Research question 3
In the second phase, the third research question regarding the risk strategies is answered. This includes the classification and categorization of the individual risks found in the previous phase and studying the probability and impact of every risk whilst identifying suitable risk management strategies. The literature will be supportive in nature when categorizing risks and finding existing preventative, mitigating, avoidant or accepting risk management strategies. The interviews will serve to find the answer to the research question by questioning experts in the field whilst posing them risk management strategy options as well and see what (interview)data leads to effective conclusions answering the third research question.

Research question 3: What are the risk management strategies in response to the GDPR compliancy risks?
The main qualitative data collection methodologies that were used for this research question consists of two methods, the literature review, and systematic semi-structured interviews. The literature review for research question 3 is completed to collect relevant literature on managing risk, risk impact, risk probability, risk categorization, risk strategies for GDPR, risk strategies for GDPR in retail banks, risk strategies in cloud migration.
The semi-structured interviews consist of 7-8 in-depth interviews with cloud consultants, GPDR professionals, privacy officers, cyber security specialists and banking professionals.

Thesis overview

Chapter 1 presents an introduction to the research problem and approach, Chapter 2 follows with the literature study, Chapter 3 addresses the methodologies used to conduct this research. The fourth chapter brings forth the results of the research, Chapter 5 provides the conclusion and discussion. Chapter 6 is the last chapter where a critical reflection is given on the research conclusions and research process.

Chapter 2 Literature review

This chapter, containing the literature review, explores all the literature that was collected and utilized to enable the study. In other words, this would be the literature study itself that is required to answer the sub-research questions, and most of all gain an in-depth understanding of the concepts, theories, background, previous work, and relevant insights. It serves as the main set of theories that function as a guideline for the thesis and is divided into multiple subsections based on the three topics addressed in the research approach, which are cloud computing, GDPR risks identification and risk strategies.

2.1 Cloud computing

2.1.1 Why adopt cloud computing?

The adoption of cloud computing by banks is a topic that has been discussed in media frequently, Information Week wrote an article regarding the slow adoption of the cloud by banks. And Investment Executive wrote that banks are competing in tech innovation adoption yet are challenged by a slow adoption. An argument that is addressed by those opposing the usage of cloud technology in banking is the security concerns. If the security concerns can be resolved the technology can improve scalability, flexibility, and costs of the IT-infrastructure (Forbes, 2019).

However, a different challenge is occuring for banks regarding their financial services and internal operations. According to Accenture, managing the regulatory landscape and the increasing customer demands, banks are looking to optimize their legacy IT systems to more flexible, digital platforms to adapt to the needs of their customers and save costs (Calvet, 2017).

And lastly, retail banks are struggling with their approach as well, according to Capgemini, most banks have been digitizing the customer experience (front-office) and not their back-offices that often still use legacy systems, use manual, paper based processes and utilize siloed data sources. Manual efforts result in operational inefficiencies, which negatively impact the customer experience.
This can be optimized by digitization, by investing in cloud computing technology to improve the IT-infrastructure or the customer experience, including the internal operations which ought to be addressed as well (Capgemini Consulting, 2017).

2.1.2 What is cloud computing?

Cloud computing is in its essence the provisioning of computing resources over a network, which is delivered on a scalable basis serving a client's demands. Clients can be the government, small to medium-sized organizations and of course large organizations including financial institutions (Hon & Millard, 2013). There are multiple service models when speaking of cloud computing. The three main service models are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) (Cloudflare, 2021).

Cloud computing is known as the act of offering online computing services in the forms of storage, software, and servers through the practice of using networks of remote servers hosted online, replacing the traditional local server in organizations (Rountree & Castrillo, 2014), (Cloudflare, 2021).

Defining the field of cloud computing was done by the National Institute of Standards and Technology (NIST) who defines 'the cloud' as an outlining of five characteristics, four cloud deployment models and three cloud service models. The five key characteristics are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The four deployment models include public, private, hybrid and community cloud. Whereas the three service models consist of Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service (Rountree & Castrillo, 2014).

The first notable cloud characteristic is the on-demand self-service which refers to a consumer requesting and receiving access to services without the supervision of an administrator or support staff, which have become automated processes (Rountree & Castrillo, 2014).

The broad network access is a second characteristic referring to ability to accessing a wide range of client devices such as laptops, desktops, tablets, and phones that use different operating systems (Rountree & Castrillo, 2014).

Thirdly, resource pooling means saving costs and offering being resourceful with the storage space when allocating the usage of storage and other resources. For example, when resources are not being used by customer A anymore, they are used by customer B allowing cost savings for the cloud provider. Resource pooling is often conducted by utilizing virtualization, which is the act of allowing a single server to host multiple virtual systems such as operating systems in a virtualized environment. Broadening the density of what a provider can offer per system. An example could be hosting multiple virtual environments on one system (Rountree & Castrillo, 2014).

Lastly, cloud computing provides the measurement of the cloud service usage per client. The quantification of usage enables cloud providers to offer the pay-as-you-go cost model where you clients exclusively pay for the services that they used measured in servers amount, storage capacity, additional services and computer power consumed. Through the usage of this metric, whenever a service is not used, the client is not charged for it. This metric determines the rate that the client is charged by additional costs may still be billed, yet this payment module allows companies with limited information technology budgets to not have to invest in building their own data center's (Rountree & Castrillo, 2014).

2.1.3 Benefits and risks

Benefits	**Risks**
• **Cost-effective**: Lowering upfront and overall IT infrastructure costs for firms, and dramatically for small to medium-sized firms with limited budgets for information technology budgets. • **Scalability:** Enterprises can easily scale their services based on the demand from their clients. There is not a need to invest in new datacenters or servers, whenever more or less capacity is	• **Reliability**: There is a dependency on the cloud providers' service availability. • **Global boundaries/ data location**: The processing of data, based on regulatory and legal boundaries, must be compliant and therefore the storage of certain data is restricted in certain areas. The restrictions are related to where the data is stored, accessed, and processed. Therefore, the technology might be

required regarding computing power and • **Cyber security:** Enterprises won't have to invest in cyber security regarding their IT-infrastructure since the cloud service provider, for example Microsoft Azure or Amazon's AWS Cloud. • **Innovation:** Lower barriers to innovation with access to cloud-based SaaS services such as analytics and artificial intelligence after cloud adaptation. This is to be witnessed in modern-day start-ups that start building their company based on cloud infrastructure and data services. Examples include Facebook and YouTube.	borderless, yet may still be limited based on regulations implemented in the future. Which may affect international organizations. • **Implementation costs**: The costs can be higher than initially expected or budgeted for due to complex IT infrastructure challenges occurring. • **Data security**: The data security may be at risk with cloud providers with penetrable security infrastructures. • **Existing infrastructure**: Legacy systems may be challenging to migrate to the cloud environment due to incompatible infrastructure.

Table 2: Benefits and risks of cloud computing technology usage (Avram (Olaru), 2014)

2.1.4 Cloud deployment models

The four deployment models include the public, private, hybrid and community cloud. The different deployment models are to accommodate differing requirements an organization has for their cloud environment. Considering that the differing deployment models can support different cloud strategies. A retail bank working with personal data can for example be challenged to comply with several privacy guidelines from the central banking institutions or the privacy law GDPR. Therefore, a public cloud environment could be suitable for a company working with data regarding agricultural activities since that data does not contain personal information. Yet a retail bank, managing sensitive personal data would most likely prefer a private cloud or hybrid cloud (mix between public and private cloud) to accommodate their security and privacy guidelines (Rountree & Castrillo, 2014).

2.1.4.1 Public cloud

The public cloud is a deployment model that allows customers to access their IT infrastructure, data, and software systems online through an external service provider. The public cloud is accessible online for other customers and companies to access. Also, the infrastructure that is being offered is also being used by other customers which are most likely other companies. This form of deploying cloud solutions is cost-effective. It also requires less server management by internal personal since it this activity is outsources and it also allows the cyber security to be of high quality even though small and medium sized businesses won't always have sufficient budgets to invest in IT infrastructure security improvement (Rountree & Castrillo, 2014), (Cloudflare, 2021).

2.1.4.2 Private cloud

The private cloud is a deployment model that allows a third-party cloud provider to offer a cloud environment with servers and infrastructure exclusively being used and accessible to the internal organization of a customer. Therefore, the private cloud is more expensive than a public cloud. The private cloud offers the cloud services through an intranet. In some organizations staff may be able to access the private cloud externally outside of the organization through a virtualized private network

(VPN), which is the act of encrypting all information communicated between the organization and employee. Private clouds are always deployed for an organization (Rountree & Castrillo, 2014), (Cloudflare, 2021), (Laszewski & Nauduri, 2012).

2.1.4.3 Hybrid cloud

The hybrid cloud deployment model is a combination between the usage of public and private cloud deployment, whereas private clouds are normally only run for one organization. Yet, governments and banks often require a combination of public cloud services to allow several organizations and customers access to the cloud services, yet also require private cloud deployment for the privacy of sensitive information (Rountree & Castrillo, 2014), (Cloudflare, 2021), (Gurkok, 2013).

2.1.4.4 Community cloud

The community cloud is a collaborative cloud computing environment for several organizations to use based on having similar requirements for the infrastructure and therefore share the digital resources together. The organizations having access to the computing service environment are limited, the community shares similarities security, performance, requirements, privacy, and organizations outside the community do not have access. The organizations gaining access may have similarities regarding their industry (banks, governments, trading firms). The community cloud may be regulated by a third party, but this is not a necessity (Rountree & Castrillo, 2014), (Cloudflare, 2021).

2.1.5 Service Models

2.1.5.1 Software-as-a-Service

When speaking of SaaS or Software-as-a-Service, it refers to offering clients online access to software applications installed by the cloud provider on their remote servers, allowing clients to use the software whilst outsourcing the of purchase and maintenance of servers (Mell & Grance, 2011). Software applications offered could for example be B2C, B2B, HR, accounting, productivity, document editing, email, or file sharing applications. SaaS services, companies use include Workday to support their HR services and Salesforce to support their customer relationship management processes (W. Kuan Hon, 2018), (Gurkok, 2013).

2.1.5.2 Platform-as-a-Service

The PaaS or Platform-as-a-Service service model includes the offering of hosting and deployment platforms to function as the foundation for the software application (SaaS) services. Clients gain autonomy regarding they design their platform and software applications (W. Kuan Hon, 2018). PaaS platforms allow clients to develop and deploy web applications, the cloud provider does not influence what is being developed, yet they can offer additional services such as analytics to review the usage of an application or support deployment with load-balancing services (Derrick Rountree, 2014), (Gurkok, 2013), (Laszewski & Nauduri, 2012).

2.1.5.3 Infrastructure-as-a-Service

The third service model is known as IaaS or Infrastructure-as-a-Service, which is the "technical layer" offering operating systems, virtualization, computing power, storage, networking, the PaaS, and SaaS environment can be created on top of this layer. The client's data is stored on the datacenters of the cloud provider (Derrick Rountree, 2014), (Gurkok, 2013), (Laszewski & Nauduri, 2012).

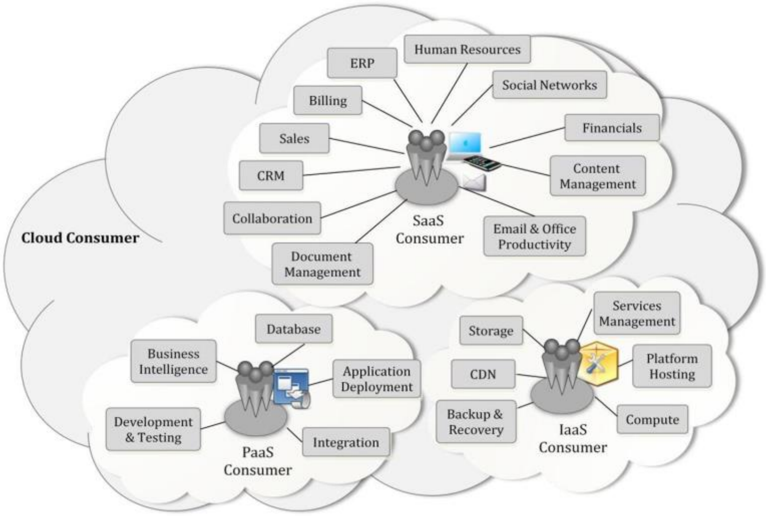


Figure 1: Examples of SaaS, PaaS, and IaaS cloud services from the NIST (Kearns, 2017)

2.1.6 Cloud infrastructure parties

The cloud computing infrastructure is relevant to review when analyzing how a cloud migration is conducted within the context of a retail bank. This is because the existing technology infrastructure of an organization influences which cloud migration approach is chosen when migrating data to the cloud provider. Therefore, the architecture background of a client organization and the cloud providers with its services offered is relevant. According to the NIST reference model the entities in the migration are five in total, which are:

- The service consumer, maintaining a relationship to use the cloud services provided,
- The service provider, ensures that the services are delivered to the service consumer,
- The carrier, guarantees that the connection between service consumer and provider is functional,
- The broker, an intermediary between service consumer and provider managing usage, performance, and delivery of cloud services,
- And lastly, the auditor, conducting independent assessments on the performance, operational functioning and security of the cloud services and its implementation. Including assessments such as cloud privacy assurance or security assessments (Derrick Rountree, 2014), (Gurkok, 2013), (Laszewski & Nauduri, 2012), (Kearns, 2017).

2.2 Cloud migration in retail banking

2.2.1 Definition

The process of migrating infrastructure, applications, and databases from self-managed datacenters in an on-premises environment to a cloud computing environment from an external cloud service provider. A cloud migration may also include migrating from different environments such as migrating from a cloud environment to a new cloud environment or from a cloud environment back to on-premises (Jamshidi, Ahmad, & Pahl, 2014), (Laszewski & Nauduri, 2012).

To migrate to the cloud, a distinguishment between cloud migrations helps when recognizing which strategy is most effective for an organization.
A cloud migration is a plan for an organization describing how to conduct their cloud migration. To create a strategy, the objectives and requirements will be valuable input in creating a plan.
Factors that are relevant when migrating to a cloud environment would be legal, security, financial, technical, and organizational risks, and general measures.
SLA agreements can limit the legal risks exposed to the service consumer depending on the chosen cloud provider (Efremovska & Lago, 2017), (Efremovska, Lago, Kemmerich, Laszewski, & Nauduri, 2017).

2.1.7 Cloud migration types

There are multiple manners in which data, applications and infrastructure can be migrated to the cloud. According, the literature the models may be categorized under migration types which can be chosen depending on the migration objectives, available resources from the cloud service provider and current infrastructure at the service consumer. The cloud migration type can be a replacement of application tiers, partial migration, migration of the entire application stack and to cloudify which would be converting to a full-fledged cloud migration. To enable to a cloud migration, a cloud migration process must be completed, according to literature this process consists of several process steps such as migration planning, migration execution, migration evaluation and addressing cross-cutting concerns. The migration types and process steps are displayed below in detail in Table 3 and Table 4. (Jamshidi, Ahmad, & Pahl, 2014).

Migration type 1: Replacement of application tiers	**Migration type 2: Partially migrate**	**Migration type 3: Migrate whole application stack**	**Migration type 4: Cloudify/ complete migration**
The least invasive of methods where data and business tiers are migrated to the cloud stack.	This type migrates some of the software system's components to the cloud.	The easiest way of migration where the whole application is monolithically encapsulated in one or more virtual machines running on the cloud.	This is the most complete migration where an application is converted to a full-fledged cloud-enabled system by composing cloud service.

Table 3: Cloud migration type overview (Jamshidi, Ahmad, & Pahl, 2014)

Process I. Migration planning	**Process II. Migration execution**	**Process III. Migration evaluation**	**Process IV. Crosscutting concerns**
Feasibility study	Data extraction	Testing	Governance
Migration requirement analysis	Architecture recovery and adaptation	Validation	Security analysis
Provider choice	Code modification and wrapping	Deployment of migrated application are performed.	Training
Subsystems to be migrated	Legacy-to-cloud transformation (conceptual)	X	Effort estimation
Cloud services to use/needed	Legacy-to-cloud transformation (concrete)	X	Organizational change
Migration strategy development	X	X	Multi-tenancy and elasticity analysis
Output artifact is a migration plan	Output is the completion of the migration	Output is an evaluation of the success of the migration	Output is an integration of all relevant factors into the new IT infrastructure

Table 4: Cloud migration process steps overview (Jamshidi, Ahmad, & Pahl, 2014)

2.2.3 Cloud migration strategies

After understanding cloud migration's definition, several types of migration, the different forms of cloud infrastructure and roles involved in a cloud migration, it is also relevant to understand the cloud migration strategies that an organization can choose for.

Considering that the migration type, what exactly ought to be migrated, the current infrastructure and the different roles per party involved can be defined, a cloud migration strategy allows the different parties to know which exact approach will be used to practically conduct the actual cloud migration. Knowing the classification of the migration type does not give insights in the actual migration strategy that will be used in detail (NetApp, 2019).

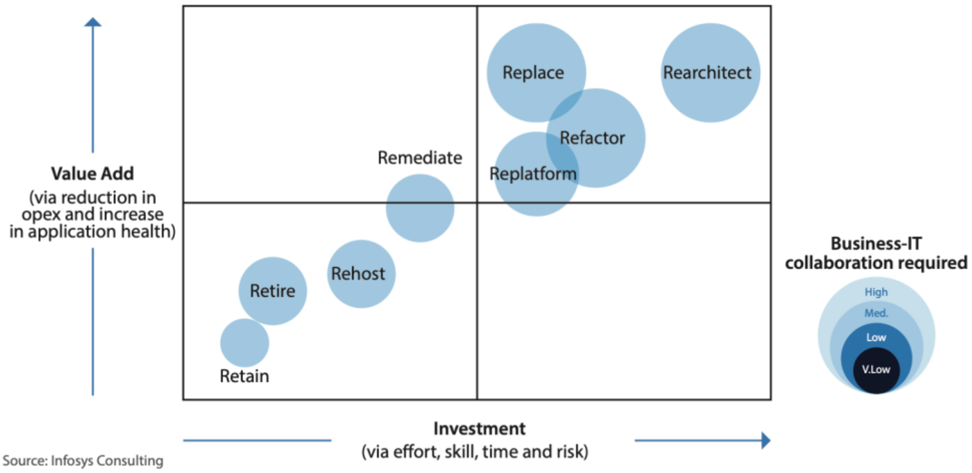
Therefore, the following six R's of cloud migration below will give an insight on common approaches when conducting migrations (Watson, 2010).
The six R's of cloud migration used by AWS consist of the following strategies (Orban, 2016):

- Rehosting ("lift and shift"): Encompasses lifting the stack from an on-premises hosting and transporting a copy of the environment to the cloud,
- Replatforming: maintaining the core architecture of your cloud applications but making a few adjustments to increase the platforms performance,
- Repurchasing: Moving current applications to a new cloud environments or landscape such as moving from CRM legacy systems to a cloud-based application like Salesforce.

- Refactoring/Re-architecting: rebuilding or re-architecting the applications from scratch.
- Retiring: Deciding to turn off an application that are not necessary to migrate.
- Retaining: Deciding not to migrate a set of data or applications for example for compliance reasons with legacy systems (Hughes, Randhella, & Tatwani, 2021)

Selecting the migration type depends on several factors, the following model developed by Infosys Consulting displays that it depends on investments, value added, and business-IT collaboration required. So, rearchitecting for example would require the most investments and business-IT collaboration but would also add the most value in the cloud migration strategy model (Clayton, 2018), (Hughes, Randhella, & Tatwani, 2021).

Figure 1. The optimal cloud migration strategy is based on three factors



Source: Infosys Consulting

Figure 2: InfoSys Consulting - Cloud migration strategy model (Hughes, Randhella, & Tatwani, 2021)

2.3 Retail banking

2.3.1 Definition and context

There are several legal definitions per country on the definition of a bank. In the Netherlands, The Financial Supervision Act of the Dutch Central Bank (De Nederlandsche Bank) defines a bank as a credit institution as referred to Article 4 of Capital Requirements Regulation (CRR). The following definition is upheld by the Dutch law, which defines a bank in the Netherlands as “a credit institution as an undertaking the business of which is (i) to take deposits or other repayable funds from the public and (ii) to grant credits for its own account” (De Nederlandsche Bank, 2017). Considering that the research is conducted in the Netherlands, the interviewed (retail) banks include banks such as ABN AMRO and NIBC Bank located in the Netherlands functioning under Dutch law. Therefore, the definition from the CRR mentioned above is most relevant for conducting this research.

Yet, the generic definition of a bank may be found in the Cambridge dictionary: “an organization where people and businesses can invest or borrow money, change it to foreign money, etc., or a building where these services are offered”.

When defining the scope of the research, a focus was made on retail banking. There are several forms of banking and organizations within the banking industry. Which include:

- Investment banking: a form of banking that aims to create capital for other companies, governments, and entities by conducting activities such as aiding in mergers and acquisitions, reorganizations, broker trades and underwriting new debt and securities for different types of corporations. Investment banks function as intermediaries in large, complex financial transactions. Examples include Morgan Stanley, J.P. Morgan Chase, Credit Suisse, Citigroup, Deutsche Bank, Goldman Sachs Group, and Bank of America (Hargrave, 2020).
- Commercial banking: the offering of basic financial products, loans, acceptance of deposits, offering checking account services to individual consumers and small-to-midsize businesses located in physical stores or (exclusively) online or both. Commercial banks derive their income from earning interest and charging a range of fees. Examples include Bank of America, HSBC Bank and Goldman Sachs Group (Commercial Banks Guide, 2015), (Kagan, 2021).
- Corporate banking: refers to the offering of banking services exclusively to businesses, from small-sized businesses to conglomerates such as treasury and cash management services, loans and credit products, equipment lending, commercial real estate, asset management and securities underwriting offered by a banks' commercial or investment banking divisions (Majaski, 2021), (Corporate Finance Institute, 2021).
- Private banking: offering personalized wealth management, investment, portfolio management, tax, insurance, trust, and other financial services for high-net-worth individuals of retail banks or other financial institutions. Often accompanied with a personal banker dedicated to every high-net-worth client. Examples include commercial banks with a private banking division or dedicated private banking organizations such as J.P. Morgan Chase, UBS, Raymond James, and Credit Suisse (Chen, 2020).
- Central banking: ensuring the economic and financial stability of a nation or group of nations by through a privileged control over the production and distribution of money and credit. Central banks conduct the monetary policy ensuring low and stable inflation whilst managing global financial crisis. Central banks such as the European Central Bank and national central banks.
- Online banking: offering users the possibility to conduct financial transactions online, available on desktop versions and mobile applications (International Monetary Fund, 2021), (Segal, 2020), (Frankenfield, 2020).
- Credit Unions: a tax-exempt, non-profit financial cooperative enterprise offering banking services formed by corporations, organizations and other entities operated by their participants (Grantt, 2021).

(Dixon, 2019)

2.3.2 What is retail banking?

Retail banking is a form of banking which provides financial services such as savings and checking's accounts, mortgages, debit or credit cards, and certificates of deposit to individual consumers and small businesses through branches, the internet, and other channels.

Large banking companies often have a retail banking business unit managing its own retail activities. The small businesses served by retail banking business units may vary from proprietorships to startups, the term “small business’ is a categorization based on the annual sales or revenue volume distinguishing medium-sized, large corporate/conglomerate businesses.

Retail banking services are offered through automated teller machines (ATMs), physical locations, online and telephone banking services.
Examples of retail banks include Goldman Sachs, Citibank, Wells Fargo, Bank of America.

2.4 Risk management strategies

2.4.1 Definitions

When addressing the third sub-research question, the relevant information that will serve the founding of an answer will bring forth the necessity of researching literature regarding the sub-research question’s components: definition of risk, definition of risk management strategies, risk matrix and a risk management strategies framework.

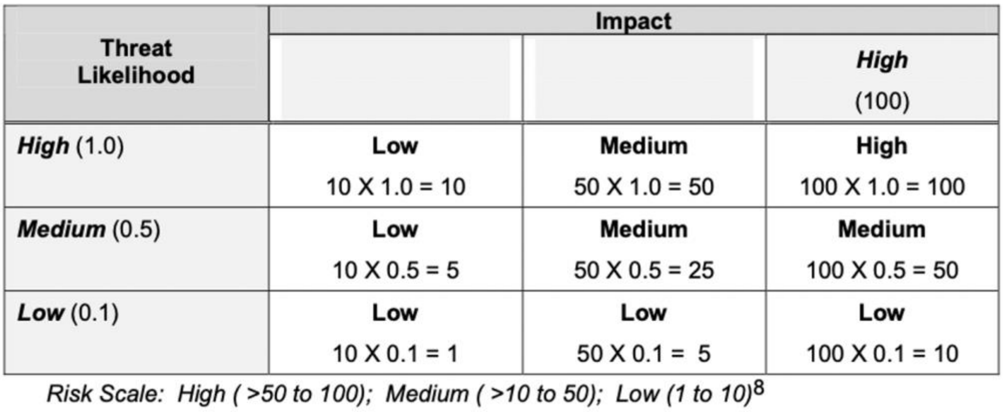
A risk can be defined as follows: “Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence” (Stoneburner, Goguen, & Feringa, 2002).

Managing risks is done through risk management which can be defined as: “Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems” (Stoneburner, Goguen, & Feringa, 2002).

The main components in the determination of a risk are the net negative impact of an exercise by considering the probability and impact when the risk occurs. Defining this risk calculation allows there to be a classification of every risk in combination with a risk analysis. The risk analysis allows the insight into the risk’s impact and probability to create a classification. The classification itself can be created by a risk matrix. A risk matrix offers a classification of risk levels and an overview of the probability level (Low, Medium, High) and the impact (Low, Medium, High) and allow for a calculation. This calculation creates a measured classification of a risk level being low, medium, or high, afterwards actions and resource allocation for risk mitigation can be determined. The risk matrix and risk level classification are discussed below (Hirao & Wun-Young, 2009).

2.4.2 Risk-Level Classification and Matrix

Through multiplying the two risk components ‘threat likelihood’/ probability and the threat impact, the risk classification can be established per risk. The matrix can use a 3 x 3 matrix with the Low, Medium, and High score given per risk. The matrix may be extended to a 4 x 4 or 5 x 5 matrix by adding the score possibilities of Very Low and/or Very High as possibilities per risk component in case the requirements of the risk assessments showcase the necessity for score possibilities to be added (Stoneburner, Goguen, & Feringa, 2002).

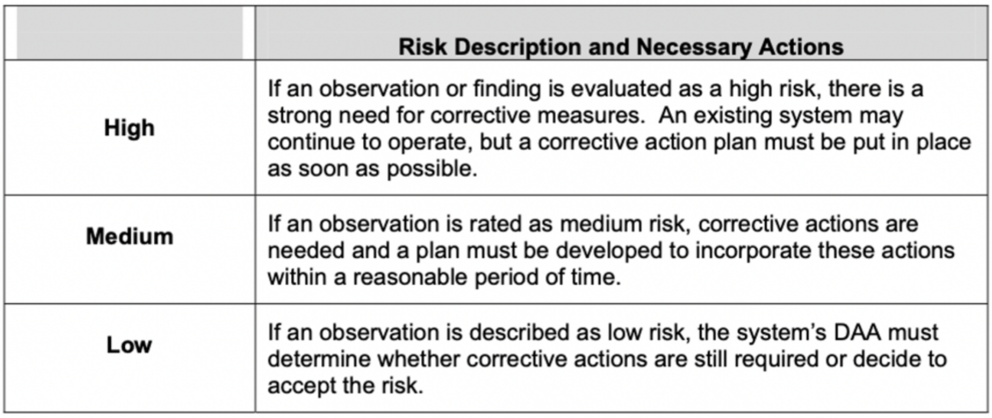


Threat Likelihood	Impact		
			High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Figure 3: Risk-Level Matrix (Stoneburner, Goguen, & Feringa, 2002)

The impact score per risk may be 10 (Low), 50 (Medium) and 100 (High). On the other hand, the probability score consists of a 0.1 (Low), 0.5 (Medium) and 1.0 (High). The multiplication calculation gives the rating of the risk level which is described in the figure below. The risk level addresses the level of risk as to which a procedure, process, department, team, employee, system may be exposed to. The risk level also directions as to how senior management ought to respond to a risk based on its risk level (Stoneburner, Goguen, & Feringa, 2002).



	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Figure 4: Risk Level Classification (Stoneburner, Goguen, & Feringa, 2002)

2.4.3 Risk management strategies and process

Risk management addresses risks that have not yet occurred, events that have future consequences and ought to be managed by applying a risk strategy. Which can be done through risk strategies such as acceptance/assuming the risk, mitigation, transferring and avoidance. The risks can be 'closed' often after mitigations are proven or being used (Stoneburner, Goguen, & Feringa, 2002).

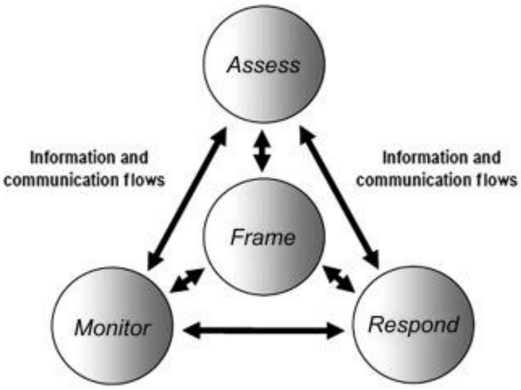

Assess
Information and communication flows
Information and communication flows
Frame
Monitor
Respond

Figure 5: NIST Risk Management Process

A risk management strategy specifies methodologies and procedures through which risk assessments, risk response and risk monitoring activities can be performed, reflecting the organizational governance decisions of an organization. The organizational governance decisions are specified in terms of risk assumptions, risk priorities, risk tolerance, risk constraints and risk acceptance (Stoneburner, Goguen, & Feringa, 2002), (National Institute of Standards and Technology (NIST), 2018).

The NIST risk management process is process-based approach where an organization constructs the risk management practices approved as policy for the organization. The NIST risk management process consists of four components: risk assessment, risk response, risk framing and risk monitoring. The main output from all the process steps is a risk management strategy that can function as policy within an organization (Stoneburner, Goguen, & Feringa, 2002), (National Institute of Standards and Technology (NIST), 2018).

The risk assessment is the first process step of the risk management process. Here there are several sub-steps to be completed to determine the threat and probability of risks. Sub-steps include system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations and results documentation. Interviews can be conducted which assess the probability and impact of risks, focusing on risks with a high-net impact (Stoneburner, Goguen, & Feringa, 2002), (National Institute of Standards and Technology (NIST), 2018).

The risk response identification or risk mitigation step is the second process step of the risk management process. The risks that were found ought to be reviewed by risk managers and courses of action need to be identified. Policies and guidance in the risk management strategy may influence the responses chosen to manage the risks. The risk management strategies that can be chosen include Acceptance, Mitigation, Sharing, Transference and Avoidance (Gantz & Philpott, 2013).
Every risk management strategy works as follows:

1. Acceptance: The risk is acceptable due to it falling within the limits of the organizations' risk tolerance and cost-benefit considerations tolerance.
2. Mitigation: Reducing the level of risk to a level within the risk tolerance limitations of the organization.

3. Sharing: Sharing the responsibility with a different organization to reduce the risk to an acceptable risk tolerance level for both organizations.
4. Transference: Liability of consequence or responsibility is outsourced to a different organization. For example, by purchasing insurance. The risk itself is not reduced by this strategy.
5. Avoidance: Action is taken to prevent the occurrence of the risk considering the risk is unacceptable and other risk strategies may not be effective (Stoneburner, Goguen, & Feringa, 2002), (National Institute of Standards and Technology (NIST), 2018).

The third process step is risk framing. Which refers to producing a risk management strategy addressing how an organization would like to respond, address, and monitor risk. The assumptions, risk tolerances, constraints, and tradeoffs to make operational decisions are specified within this risk management strategy or policy (Stoneburner, Goguen, & Feringa, 2002), (Federal Virtual Training Environment (FedVTE), 2014).

The fourth process step is monitoring. Which includes e.g., conducting continuous compliance verifications, risk response effectiveness measurements, initiate process improvement activities where needed (Stoneburner, Goguen, & Feringa, 2002), (Federal Virtual Training Environment (FedVTE), 2014), (Hirao & Wun-Young, 2009), (National Institute of Standards and Technology (NIST), 2018).

2.5 General Data Protection Regulation (GDPR)

2.5.1 Definition

The GDPR is regulatory body from the European Union. All Member States of the European Union (EU) ought to follow the data privacy and data retention restrictions given by the European Parliament through the General Data Protection Regulation (GDPR). The GDPR consists of regulations and laws addressing procedures, rights and requirements that need to be followed within the EU (Johnson, Kovacich, & Jones), (National Institute of Standards and Technology (NIST), 2018).

The GDPR document outlines the data privacy laws for all organizations working with data including micro, small, medium, and large-sized enterprises.
The data may be personal or sensitive personal data, relating to natural persons, which is protected by the GDPR through its laws and regulation on data privacy and data security (Metheny, 2017), (Johnson, 2019).

Globalization and technological advancement brought forth challenges requiring the GDPR to offer protection for natural persons and their sensitive, personal data. Every EU country or Member State has their own data privacy laws, the GDPR was designed to facilitate data flow within the EU more effectively, whilst protecting data flowing out of the EU (Beckett, 2017).

2.5.2 GDPR compliance risks

When GDPR guidelines are not followed, and the data security is not up to par, it can cause the following risks to occur:

1. Lack of data privacy,

2. Reputation damage,
3. Data leakages,
4. Fines from the European Union,
5. Hacks due to insufficient data security,
6. Loss of customer trust,
7. Personal damage to consumers due to their personal data being leaked or hacked (Beckett, 2017).

2.5.3 GDPR restrictions for banking and cloud provider organizations

The data privacy laws, principles and rights are addressed in the table below. All chapters of the GDPR document include:

1. General provisions,
2. Principles,
3. Rights of the data subject,
4. Controller and processor,
5. Transfers of personal data to third countries or international organizations,
6. Independent supervisory authorities,
7. Cooperation and consistency,
8. Remedies, liability, and penalties,
9. Provisions relating to specific processing situations,
10. Delegated acts and implementing acts,
11. Final provisions (Beckett, 2017), (European Parliament, 2014), (Information Commissioner's Office (UK), 2021).

Within the chapters, a set of articles are published that address a subject and the specific regulations that apply. The most relevant ones for banks that move their data to a cloud provider are principles to ensure rightful usage of data, the data subject rights to ensure all rights of natural persons are protected and lastly transfers of personal data to ensure that the data is transferred in a manner that is compliant with all GDPR guidelines. Chapter 1 and 4 address the context and roles of the different parties involved in the compliance process for the GDPR (European Parliament, 2014), (Voigt & Bussche, 2017).

The main roles identified by the EU GDPR are the:

- Data controller: entities or person collecting and processing the (personal) data,
- Data subject: natural person or entity of which the data is collected and ought to receive notice of collection,
- Data processor: a public authority agency, natural or legal person, or other body processing data for the controller,
- Data protection officer: an employee managing the compliance of data controllers and processors regarding the data protection regulation (European Parliament, 2014).

All data subjects have rights, the rights of the data subject are described in Chapter 3 and are listed in the table below in the middle column. The rights address that the data subject should be sufficiently informed, have access to their personal data, have the option to have their data erased, object the usage of their personal data and more (European Parliament, 2014).

Secondly, organizations ought to be processing personal data based on the GDPR principles displayed in the table below from Chapter 2 of the GDPR. Which include minimizing the usage of sensitive, personal data, being accountable, follow storage restrictions and more (European Parliament, 2014).

Thirdly, the transfer of personal data includes articles from Chapter 5 of the GDPR addressing derogations for specific situations, corporate rules, international cooperation and more (European Parliament, 2014).

Principles (Chapter 2, Art. 5-11)	Rights (Chapter 3, Art. 12-23)	Transfers of personal data to third party countries or international organizations (Chapter 5, Art. 44-50)
Personal data principles: 1. Lawfulness, fairness, and transparency, 2. Purpose limitation, 3. Data minimization, 4. Accuracy, 5. Storage limitation, 6. Integrity and confidentiality, 7. Accountability.	Rights of a data subject: 1. The right to be informed, 2. The right of access, 3. The right to rectification, 4. The right to erasure, 5. The right to restrict processing, 6. The right to data portability, 7. The right to object, 8. Rights in relation to automated decision making and profiling.	Consider when transferring data: 1. Transfers on the basis of an adequacy decision, 2. Transfers subject to appropriate safeguards, 3. Binding corporate rules, 4. Transfers or disclosures not authorized by Union law, 5. Derogations for specific situations, 6. International cooperation for the protection of personal data.

Table 5: Relevant GDPR policy regulations for organizations processing data (European Parliament, 2014), (Politou, Michotab, Alepisa, Pocsc, & Patsakis, 2018), (Khaled, Pattel, & Siddiqui, 2020), (Information Commissioner's Office (UK), 2021)

2.6 Literature study conclusion

An in-depth section in the results chapter 5.1 delivers the main conclusions per sub-research question based on the conducted literature study. Next to this the creation of the literature study is explained in the methodology, which is the following chapter. Next to this, the literature study provides the background to ensure literature-based answers for the research questions where possible and use to background literature on the subject matter to create interview questions.

The literature therefore serves as background material for creating interview questions that are consistent with the background information required to understand an interviewees answer. The literature background also serves to have sufficient information to explain the context of the situation that the employee must focus on, which is: “a cloud migration at a retail bank”.

The literature study also provides generic answers to the research questions asked. Yet, the literature-based answers given however are not sufficient to answer the research question since there is not available literature on the specific literature that is required. The first two sub-research questions can be directly answered with literature yet lack the context of retail banking being directly applied. The third sub-research question can be partly answered through literature where the risk management literature creates a structure for interviewees to give their answers through a risk strategy table showcased in the next chapter.

Chapter 3 Methodology

The following chapter describes the methods and research design that was used when conducting the research which include collecting data, analyzing data, processing the data into results, and drawing conclusions. The motivation behind the choices made regarding the selection of research methodologies is expanded on as well. This methodology chapter aims to showcase the believability of the results (chapter 4), describe the steps made to allow future researchers to replicate the steps made during this research study and grant a description of the materials, research process and theory. Lastly, it will also address limitations, assumption, validity, and a description of the analytical methods as well.

3.1 Qualitative research methodologies

This research study is qualitative in nature, it will explore the research topic by researching qualitative data. The two methodologies to collect the qualitative data include structural interviews with Cloud technology professionals from banking institutions and conducting a literature study. This data will be utilized to answer the sub-research questions and later the main research question.

3.1.1 Semi-structured Interviews

Interviews will be conducted with cloud, GDPR, banking and IT consultancy professionals from several banks including Capgemini, Ordina, NIBC and ABN AMRO.

The approach follows a set of steps based on three interview phases. The first phase is conducted after the literature review is partly conducted and enough qualitative data has been gathered to understand the basic concepts relevant for interview. Afterwards, interview questions are created for the exploratory phase, which consists of two interviews with industry experts. Afterwards this exploratory data is used to perfect the research question and interview questions for the next two interview phases, which on consist of 7-8 in-depth interviews per phase. The following phases are described below. The research questions were created based on the insights from and feedback received during the exploratory interviews. All interview data was recorded with permission only requested at the start of every interview, transcribed partly or fully, most important terms were extracted and used as insights when creating the final question list for interview phase 1.

The first interview phase had a question list consisting of four sections:

- thesis topic introduction and small talk,
- interviewee background questions,
- question list for research question 1 (cloud migration in retail banks),
- and the question list for research question 2 (GDPR risks).

The second interview phase has a question list consisting of four sections as well:

- Thesis topic introduction and small talk,
- Thesis results phase 1, GDPR risks identified and defining risk strategies,
- question list for research question 3 (cloud migration in retail banks),
- Feedback on current risk strategies found during literature review.

<u>Conducting Semi-structured Interviews</u>

When conducting semi-structured interviews, the main goal is to ask the most important questions and the emphasis is also on allowing new insights to be extracted from the interview. Due to Covid-19 restrictions and pandemic related measurements, face-to-face interviews are not possible and therefore all interviews are conducted by using Microsoft Teams, Google Meetings or WhatsApp phone calls. Displaying interest through body language and indirect signals is therefore more challenging and the interviewers is encouraged to feel free to address their time restrictions or refraining from discussing sensitive information. The language used in the interviews is either English or Dutch, most interviewees are native Dutch speakers, but some interviewees also do not speak Dutch, nor work or live in the Netherlands. Therefore, all Dutch answers are translated in the transcription process to English. Before the start of every interview, an introduction is made which can be found in Appendix A.

3.1.1.1 Interview question lists

The interview questions were created through the usage of the literature outlined in the literature study. This was done by finding literature on the different research questions by dividing them into the topics of cloud computing, cloud migration, retail banking, GDPR and risk management strategies. After the literature was found it was processed into the literature study when relevant to answering the research questions. The literature was used to identify which topics were important to understand how to find the answers for the research questions. The literature was used afterwards to create interview questions for phase 1, which would be for all questions from section 2, 3, 4 and 5.

Section 1: Thesis topic introduction and expressing gratitude for making time to conduct the interview.

Section 2: Interviewee background questions:

1. Can you tell me about your educational background?
2. Can you tell me about your former work experience and career path?
3. What does your current role entail?
4. Do you manage other consultants or team members?
5. What type of organization do your work for?
6. [For consultants] What clients does your consulting organization have in the banking industry (may be classified)?
7. Is your organization familiar with the usage of cloud technology and migrations?
8. What specific services does your organization provide or use regarding sensitive data management?

Phase 1
Section 3: Question list research question 1

To create a
- Address relevant context of GDPR
- Address cloud migration context
- Address retail banking context

RQ1: What defines a cloud migration in the context of retail banking?

1. Has your organization been involved in cloud migrations?
2. Does your organization consider sensitive personal data when conducting a cloud migration?
3. How are cloud migrations defined?
4. How are cloud migrations conducted within retail banks?
5. What cloud applications are used in the organization?
6. What cloud infrastructure is being used?
7. What cloud deployment model is being used?
8. What type of cloud migration is conducted (data, applications, infrastructure)?
9. What is the cloud strategy? (multi-cloud etc.)
10. Under what regulation are cloud migrations conducted?

Section 4: Question list research question 2

RQ2: What are GDPR compliancy risks within a retail bank related to cloud migration?

1. How does your organization manage GDPR-compliance when migrating data to the cloud?
2. Is there a procedure to manage GDPR compliance with cloud data?
3. Are there risks associated with not meeting the GDPR-compliance requirements with the cloud migration?
4. What are the biggest GDPR compliancy risks within a retail bank migrating data to the cloud?
5. What consequences will not meeting GDPR-compliance have on the data migrated to the cloud?
6. What consequences will not being GDPR-compliant have on the organization?
7. What departments will be affected the most when not being GDPR-compliant?
8. What procedures are in place to make a cloud migration GDPR-compliant?
9. What data can be considered sensitive?
10. What departments manage these GDPR-risks?
11. How is managing GDPR-risks differently in a retail bank compared to non-financial organizations?
    - Regulation-wise?
    - Process-wise?
12. How can GDPR-risks be prevented when migrating cloud data?
13. How can GDPR-risks be analyzed and mitigated?
14. How can GDPR-risks be avoided, regarding their impact?

Phase 2
In phase 2, the same procedure was conducted, yet here, only the interview questions relevant for research question 3 are asked.

Research question 3
What are the risk management strategies in response to the GDPR compliancy risks?

The interview questions were determined based on the results for phase 1. The research results that determined the answer for sub-research question 2 (RQ2): "RQ2: What are GDPR compliancy risks within a retail bank related to cloud migration?
", brought forth six GDPR risks for cloud migrations.

The risks were analyzed in a risk matrix table using interview and literature study data to determine whether the risks ought to be considered high impact risks. Afterwards, the risks were confirmed to all be high impact risks. This step was followed by researching the literature on generic risk management strategies that can be applied to enable the interviewee to have sufficient structure when answering which risk management strategies can apply per question.
To enable this interview therefore, the risk management strategy literature found in chapter 2 was applied to create a table with a central question asked per risk:

"When considering the following six GDPR risks, which risk management strategy applies and how can that strategy be applied in detail?"

The table consisted of the six GDPR risks from the first-round results of RQ2 on the vertical left side of the table. Whereas, on the horizontal upper right side of the table a row was offered with all the options for the interviewee to select answers from. The options included the five main generic risk management strategies from the literature study, which are Acceptance, Mitigation, Sharing, Transference and Avoidance. One of multiple risk strategies may be chosen by the interviewee per risk. The interviewee was encouraged to offer argumentation for their choose of selecting a risk strategy and in what practical manner the strategy could be applied or implemented. Risk strategy 3 and 4 were combined in the table for aesthetics and their similarity in approach.

The interviewees were presented with the following table below.

Section 5: Question list research question 3

Risk #	Risk strategy 1: Acceptance	Risk strategy 2: Mitigation	Risk strategy 3 & 4: Sharing & Transference	Risk strategy 5: Avoidance
Risk 1				
Risk 2				
Risk 3				
Risk 4				
Risk 5				
Risk 6				

Table 6: Interviewee question list table Round 2 sub-research question 3

Risk Level Classification and Matrix

The six GDPR risks were selected using the Risk Level Classification displayed through the Risk Level Matrix based on the literature in Chapter 2.4.2. All risks addressed by interviewees needed to have a high score in the final risk classification level, which was calculated by multiplying the probability score with the impact score of a risk. If risks were considered to have a low final score, they were not included. Interviewees were encouraged during interviewees to share the GDPR risks with a high impact and probability.

The risks were classified by using the interview data to classify the risks as having a High, Medium, or Low probability and impact.

- A low impact was considered having acceptable negative consequences on the bank.

- A medium impact would be considered problematic and requiring actions to be taken and investments to be made,
- yet not as urgent as a high impact risk which would have severe, potentially lasting impact on the bank requiring immediate attention, urgently.

The probability was determined by the likelihood of the event occurring based on the perceptions of the interviewees and their perspectives on how often such events are reported in the (financial) news.

- Low probability would indicate that the occurrence of this risk is very rare and should not be expected to occur in the near future.
- Medium probability refers to there being a realistic chance of this risk occurring.
- High probability refers to the risk occurring often enough for the risk to be considered highly alarming.

However, all scores within an organization depend on the influencing factors in the environment and current circumstances in the bank. When an organization managed to be effectively following all GDPR regulations and has implemented all required measures from the central banks to ensure data privacy, data safety and whichever risk management strategies are relevant for the organization, the probability of one of the six GDPR risks occurring will automatically decrease. Therefore, probability is dependent on the circumstance at hand and an average interpretation based on the interviewee data was used as input to determine the probability scores for risks occurring.

Structuring interview data Phase 2

The interview data gathered from interview phase 2 contained risk strategies. These risk strategies were collected using Table 6 during interviews and collecting data per interviewee per risk strategy option (Acceptance, Mitigation, Shared, Transference and Avoidance). Afterwards, the risk strategies were coded and summarized. The results were displayed in tables with three categories:

- organizational policy (1),
- process/ procedure (2)
- and technology resource usage (3).

These three categories were the main forms of answers that interviewees gave, most business and project management role fulfilling interviewees addressed organizational change, policy change and process changes. Cyber security consultants mostly addressed specific procedural changes and addressed in detail which technological resources ought to be used. Therefore, each (empty) risk strategy section of interview Table 6 of interview phase 2 (Acceptance, Mitigation, Shared, Transference, Avoidance) per risk (GDPR fines, Data leaks etc.) was filled by interview data. The interview data was afterwards structured in the three categories or organizational policy, process/procedure, and technology usage.

In the final conclusion in Chapter 5.1 and 5.2, the interview data-based risk strategies were given specific categories including information security, data privacy, customer trust, technological and contract management to showcase a more conclusive categorization of every specific risk strategy.

Research results

Phase 0 - Exploration round interviews

The research scope defined during the literature study will be utilized as a foundation of definitions that will be communicated to every interviewee in order to maintain a consistent research context when gathering research data from industry experts. This context and research data will also be used to construct research questions that are based on a foundation of literature and preparatory research. Every phase will have its own interview questions. Consists of 2 interviews.

Phase 1 - Risk Identification & Phase 2 - Research question 1 and 2

This question is reflected in phase 1 and 2 in the risk strategy creation process. The first round and second round of interviews will focus on research question 2. Which is Identification of GDPR risks & Qualitative analysis of GDPR risks. Consists of 7-8 interviews.

Phase 2 - Strategy development - Research question 3

This question is directly answered in phase 3 with the third round of interviews. A literature study will be used as supportive material. The focus is on identifying strategies. Consists of 7-8 interviews.

3.1.1.2 Interview Criteria & Process

To select interviewees, the goal of every interview phase is thoroughly considered. The type of questions that ought to be asked, require interviewees to have specific expertise as industry experts. Preferably in the financial services (banking), IT consulting, cloud engineering industry. Requirements for the selection criteria for interviewees per phase include the following:

Phase 0: Exploratory

- Interviewee must have a senior position in the role of technology management, data science, cloud computing, banking, IT transformations to advise confidently on the industries' conduct regarding cloud and GDPR compliance.
- Interviewee must have several years of experience in the IT field.
- Interviewee must be part of a company or have corporate clients.
- Interviewee must understand the cloud industry and financial services industry.

#	Company	Role	Status
1	Harvest (IT Recruitment) / Finance Industry	Data Science Lead	Interview done
2	Fortune 500 Cloud Service company, Worldwide industry leader and largest retail banks worldwide as clients	Banking & Cloud Executive + Senior Solution Engineer UK	Interview done

Table 7: Exploratory interviews

Phase 1 & 2: Risk identification & Analysis

- Must be an IT professional or banking professional knowledgeable about cloud computing, GDPR, data, enterprise architecture, IT transformation, compliance, regulation or risk management in the financial services or IT consulting industry.

#	Industry	Role	Status
1	Largest Dutch retail banks	Cloud & Business consultant	Interview done
2	Large cloud service company, large retail, and digital bank client	Infrastructure Lead Consultant	Interview done
3	Largest Dutch retail banks and Large IT consulting firm	Cloud & Business consultant	Interview done
4	Large Dutch retail bank / investment bank	Data Scientist	Interview done
5	Large Dutch retail bank / investment bank	Tech. Infrastructure Implementation	Interview done
6	Large Dutch retail bank / investment bank	Business Process Consultant	Interview done
7	Large Dutch retail bank / investment bank and largest IT consulting firm	Digital Strategist	Interview done
8	Large Dutch retail bank / investment bank	IT Project Manager	Interview done
9	Large international IT consulting firm	Cloud consultant	Interview done

Table 8: Round 1 interviews

Phase 3: Risk strategies

- Must be an IT professional or banking professional knowledgeable about cloud computing, GDPR, data, enterprise architecture, IT transformation, compliance, regulation or risk management in the financial services or IT consulting industry.

#	Company	Role	Status
9	Large Dutch insurance and investment firm	Junior Cloud & IT Professional	Interview done
10	Large Dutch retail bank / investment bank	Data Engineer/ Data Scientist	Requested
11	Large Dutch retail bank / investment bank	Data Scientist	Interview done
12	Large Dutch retail bank / investment bank	Transformation Consultant	Requested
13	Large international IT consulting firm / Dutch government	Cybersecurity Consultant	Interview done
14	Large Dutch retail bank / investment bank	Business Consultant	Interview done
15	Large international IT consulting firm and large Dutch IT consulting firm	Cloud Consultant	Interview done
16	Largest Dutch retail banks and Big 4 IT consulting department	Enterprise Architect	Interview done
18	Large international IT consulting firm	Cloud consultant	Interview done
19	Large international IT consulting firm	Cloud consultant	Requested
20	Small Dutch data analytics & IT consulting firm	Data Analytics/BI Consultant	Interview done

Table 9: Round 2 interviews

The process of conducting interviews consists of:

- Selecting interviewees based on the criteria per phase,
- Approaching the interviewee regarding their willingness to conduct an interview through email, LinkedIn or by phone, if possible,
- Informing the interviewee on the purpose of the research, send form of compliance for usage of information (personal names and company will not be used),
- Schedule a meeting and ask questions according to interview plan,
- Inform the interviewee on the research context and setting whilst interviewing,
- Ask for contacts, leave space for feedback, opportunity to ask questions in the future,
- Communicate usage of interview data and thank the interviewee for their support.

3.1.1.3 Interview population, processing, and coding

Considering that there are different retail banks in Europe, I focused on finding professionals and organizations with international exposure regarding their operations and industries to have retail banks and consultancy firms with professionals that provide viewpoints applicable to literature relevant for academic purposes and perspectives relevant to the retail banking industry. The professionals needed be from credible backgrounds showcasing affinity with the financial industry, privacy law/GDPR and/or cloud computing. Considering that it is somewhat unrealistic for a professional to have advanced expertise in all three fields, the professionals are approached based on having expertise in one or two categories.

The interviewees' population include the following three examples of interviewees:

- Cloud migration category:
    - Interviewee example 1 (identity anonymized):
        - Role: Technical cloud migration consultant at a large Dutch retail bank (NIBC Bank, ING, ABN AMRO).
        - Profile: 8 years' experience working as a technology and project management professional in several industries.
        - Age: 34
        - Educational background: Bachelor's in economics, bachelor's in business administration and management and a master's degree in Public Administration at the Leiden University.
- GDPR category:
    - Interviewee example 2 (identity anonymized):
        - Role: Privacy & cloud migration consultant at one of the largest consulting firms in the world (Capgemini, Centric, EY, Deloitte, Accenture).
        - Profile: 3 years' experience working in the private and public sector.

        - Age: 27
        - Educational background: Bachelor's degree in Business IT & Management at the Hague University of Applied Sciences.
- Retail banking:
    - Interviewee 3 (identity anonymized):
        - Role: Senior Retail Banking Digital Project Manager at a large Dutch retail bank (NIBC Bank, ING, ABN AMRO).
        - Profile: 15+ years of experience working in retail banks predominantly as a (process) consultant.
        - Age: 42
        - Educational background: Bachelor's and master's degree in business administration at the University of Groningen.

Processing interview data

There are several steps taken to process the interview data collected. Firstly, there is a categorization made with the collected qualitative data based on industry and role. Which consists of the following categories:

- Industry: Retail bank
    - IT Professionals,
    - Cloud Professionals,
    - GDPR Professionals,
- Industry: IT Consultancy
    - IT Consultants,
    - Cloud Consultants,
    - GDPR Consultants,

Afterwards, all interviewed consultants and professionals are placed in the following categories. Afterwards, the interview data is transcribed, coded and the codes are also categorized within the following categories above. Then there is a clear distinction between what retail banking professionals and their perspectives, and potential differences with external consultants who may have a different viewpoint on the questions asked. All the coded answers and most relevant information is reviewed per question. And the answers are analyzed and further researched using literature. Afterwards, the answers are processed into finalized answers per question. Which must eventually grant sufficient information, in combination with the literature review data to grant a conclusion to every research question. Finally, this would allow all the results to be successfully processed into the final conclusions necessary to answer the main research question.

Coding process

Processing the codes was based on an open coding methodology called inductive coding, where all the interviews were transcribed and coded manually, codes were given for all answers per question. The interview data was reviewed carefully at first to give relevant codes. And the codes were reused as much as possible. Afterwards, the codes were counted in a quantitative overview where the most used codes per question were analyzed in-depth with literature, and all other codes were also analyzed. Every code was further analyzed with existing literature and context given during interviews and resulted in a conclusion. Afterwards, all conclusions were summarized into a conclusion per interview question. Which were eventually combined into a final summary for the research question itself. The qualitative data coding software ATLAS.TI was used for coding the interviews and a flat coding frame was used to structure the level of importance per code.

3.1.2 Literature study

In the literature study, the existing literature was studied, reviewed, and analyzed to be able to answer the research questions and draw conclusions by combining literature study data with interview data. The objective of the literature study was to gather data on cloud migration, data management, GDPR and risk management strategies. The second objective was to provide supportive material to create interview questions and conduct interviews with industry experts. To achieve this objective, literature was collected from digital consulting firm websites, public sector websites and literature databases.

Considering the complexity of the studies' subject matter, industry experts with experience in conducting cloud migration projects in the retail banking sector were researched. Articles from the firms McKinsey, Deloitte, Capgemini, CISCO, and Accenture were reviewed and referred to as literature due to their demonstrated high-quality industry expertise in cloud migration, data management, GDPR and risk management. Also, Amazon Web Services and Microsoft Azure's websites were also reviewed to be up to date with relevant services and innovations.

For the GDPR documents, the European Union, European Central Bank, and the Dutch central banks' websites were used as literature sources. Lastly, U.S. government websites were also used considering the provision of literature on frameworks and standards regarding cloud and risk management.

Yet, for the literature study the Leiden University Catalogue, Elsevier and ScienceDirect were predominantly used. The ScienceDirect website was also used to find summaries on most relevant literature for relevant topics such as cloud migration or cloud strategy.

The methodologies used were the snowball method and building block method. The literature's bibliographies were used to find the most referenced literature on the topics cloud migration and retail banking. The building block method was used when searching for literature.

The following keywords were used during searches:

- Cloud computing,
    - Cloud migration, cloud migration risks

    - Cloud computing GDPR,
- GDPR
    - GDPR risks, GDPR risk strategy, GDPR risk strategies
- Retail banking,
    - Retail bank GDPR, retail banking GDPR risks
    - Cloud retail banks, cloud retail banking, cloud banking, cloud banks

Chapter 4 Results

The fourth chapter provides the results of the research, containing interview data analysis and literature study results in the form of qualitative and quantitative data. The qualitative data contains the results from the literature study and main summary of the interview data interpretations gathered. The quantitative data added is the occurrence of codes per question asked from the interview data gathered. The codes provide evidence for the provided conclusions given by interviewees in the form of measurable overview of answers given per research question. The limitations of the research results have been addressed in Chapter 5.3.3.

4.1 Literature study results

The literature study results section concludes all the most important results gathered from the literature study.

Research question 1: What defines a cloud migration in the context of retail banking?

According to the literature, a cloud migration would be defined as:

A cloud migration is conducted based on the current infrastructure of an organization. The cloud migration is conducted through selecting a cloud migration type and cloud migration strategy after an infrastructure and requirements assessment. This depends on the required cloud resources the cloud provider must deliver.

What distinguishes a retail bank from other business is the management of capital, impact on the economy, regulatory compliance requirements to follow, management of private, sensitive, personal data which can have financial consequences when not handled securely regarding cyberthreats, privacy risks and other risks.

Therefore, a cloud migration can be conducted on a technical level in a similar manner as with other organizations. Yet, the compliance regulation from the central banks on a national and continental scale (European Central Bank) ought to be considered.

Research question 2: What are GDPR compliancy risks within a retail bank related to cloud migration?

The GDPR related risks are related to privacy risk for the data of citizens in the EU that would be migrated to a third-party cloud provider. Regulation that is most relevant includes rights of the data subject, principles, and rules regarding transferring data.

Rights of the data subject: right to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, to object, and rights in relation to automated decision making and profiling. These different laws, requirements and rights comes with the following risks occurring when GDPR compliance is not met:

- Lack of data privacy (1),
- Reputation damage (2),
- Data leakages (3),
- Fines (4),
- Hacks (5),
- Loss of customer trust (6)
- and Personal damage to consumers due to hacks and leaks (7).

Research question 3: What are the risk management strategies in response to the GDPR compliancy risks?

The risk management strategies are defined based on the NIST standard risk management process which is an approach to determine risks and create risk management strategies. The risks for GDPR are known, yet not the specific risks that apply to a retail bank. Field research is required to retrieve further data on this subject. Yet, the risk strategies that can be applied after most relevant high-net impact risks are assessed and identified are acceptance, mitigation, transference, sharing and avoidance.

These strategies ought to be accompanied with specific procedures and recreated into a risk management strategy policy. Which can be created upon completing the NIST risk management process of risk assessment, risk mitigation/identification, risk framing and risk monitoring.

4.2 Interview results

In the following section, an overview will be given of the main results taking from the process of conducting semi-structured interviews with nearly ten interviewees per round.

4.2.1 Round 1

RQ1: What defines a cloud migration in the context of retail banking?

A cloud migration according to interviewees is defined as the migration of parts of the IT infrastructure, application landscape and/or data from an on-premises environment to an external cloud services provider. All interviewees from the organizations NIBC, ABN AMRO, NetApp and Capgemini have all agreed to this definition.

The cloud migration is characterized by relevant factors when conducting a migration regarding the technological perspective such as the cloud maturity, existing IT infrastructure, service needs, requirements, service model, deployment model, migration method, challenges migrating certain systems (such a
s legacy systems), cloud migration strategy, high and low latency when migrating, identity access management and data security.

In summary, a cloud migration is characterized by the current infrastructure and the steps and considerations to take when migrating towards the desired infrastructure reaping the benefits of cloud computing mentioned in Table 2, Chapter 2.

The existing infrastructure in combination with the objectives dictate the requirements for the selection of the service model (SaaS, PaaS, IaaS), deployment model (public, private, hybrid and community) and other cloud service resources. Options to migrate can include: the decision to migrate the front-end applications first to ensure a low-latency experience considering employees' dependence on the decision, migrating only non-personal data to the public cloud, and migrating only personal data to a private cloud.

Within the context of retail banking there are several factors that are relevant when describing the definition of a cloud migration, which include banking services offered, processes, procedures, IT infrastructure, requirements, migration method, data privacy, data security, and regulatory compliance. According to interviewees the retail banks are dependent on their reputation, internal and external audits for regulatory compliance with authorities, data security for ensuring data privacy, IT systems to offer banking services to customers. Relevant for banks is also the usage and storage processes regarding personal data, the rights of the data subject and GDPR principles ought to be followed. Cloud migration within the banking context is also defined by its relationship with all the differing business processes: the CRM system is related to the marketing department and processes, which is often a SaaS service offered by a cloud service provider. The requirement for increased user capacity for the website can be offered as service through increasing the server, computing resources and/or storage capacity.

RQ2: What are GDPR compliancy risks within a retail bank related to cloud migration?

The following risks can occur when organizations are not GDPR compliant within retail banks according to the interviewees:

1. Data leaks internally or externally to employees, competition, online etc.,
2. Reputational damage,
3. Being hacked due to a weak security infrastructure when migrating data,
4. Fines from the EU (could be millions of euros, 4% of annual income),
5. Lack of data privacy with data being accessed by unauthorized individuals internally or externally,
6. Clients, partners, customers being socially, financially, psychologically damaged due to their data being leaked to the public, which includes sensitive data,
7. Loss of the banking license and the bank ceasing to exist due to failing DNB assessments.

According to interviewees there are also several aspects relevant when organizations are not compliant with the GDPR when migrating data:

- Failing or passing the DNB assessment,
- Not, partly, or completely following the GPDR regulations,
- Being unaware, insufficient of sufficient in managing your data inventory,
- Being irresponsible or responsible with customer data/sensitive data,
- Having an insufficient or strong security infrastructure.

Multiple risks are related to one another. The main risks that have the most impact is the failure of the DNB assessment, causing fines, reputational damage, data privacy vulnerability, data security vulnerability and a potential loss of the banking license.

The reasons for failing the DNB assessment include not following the GDPR regulations in regard to the data privacy being protected, data being securely stored, the data being stored within the EU, the banking customers having the opportunity to exercise their data subject rights such as the right to let their data be erased, accessed and them being informed on their personal data usage through for example a privacy notice they can authorize consent for willingly.

To ensure that the data usage within the bank and when migrating data to a third party is GDPR compliant, the bank can use resources and procedures such as having security infrastructure assessments, having a Data Protection Officer, having a compliance team, have a data inventory to manage for example the erasure of data, data location staying within the EU whilst working with international cloud service providers, using data anonymization techniques to ensure the data privacy internally and externally is ensured, data privacy assessments, data processing agreements, internal GDPR policy, internal data retention policy, staff training, SLA agreements preventing selling of data or data being accessed by or leaked with competition, identity access management preventing unauthorized individuals having access to personal data, testing and reviewing the cloud environment regarding their certifications and ensuring privacy by design processes. Other measures to prevent the impact of the GDPR compliance risks for retail banks include having external consultants to review security, compliance, risk management, data privacy processes and procedures. And lastly, using GDPR related products and services such as GDPR tooling to manage GDPR compliance processes company wide.

When these measures are not taken, the customer trust can be lost, data privacy is not guaranteed, data can be leaked, hacked, accessed by unauthorized individuals etc.

The final selection of risks is based on a combination of the literature study results and the semi-structured interview results. Considering the similarity of the results for the risks, certain risks were combined with other risks. The loss of data privacy and personal damage to customers was combined with data leaks. The loss of customer trust was combined with reputation damage.

Table 10 below describes which measures can be taken to prevent and mitigate the GDPR risk within retail banks migrating data to the cloud:

#	Risks	Risk strategies
1	GDPR fines	1. Maintaining a cash reserve for fines and applying all possible procedures within the time, resource, and budget constraints to ensure GDPR compliance to avoid fines.
2	Data leaks, internally to clients that are competition and externally to the rest of the world creating personal damage to customers	2. Having identity access management processes that prevent internal and external access to data that is considered personal and/or sensitive. Also, having data anonymization and encryption software used to ensure that the data stored at a cloud service provider is not readable when leaked to the public, therefore protecting the data privacy of data subjects/customers.
3	Reputation damage and losing customer trust	3. Reputation damage occurs when media relationships worsen, and the retail bank receives negative media attention due to incompetence in maintaining customer trust and data safety and data privacy. This causes a loss of customer trust and potential legal action. To prevent a loss of customer trust, data privacy and legal action, the following risk strategies include: - Customer trust: Prepared media relationship management and PR strategy when challenges occur publicly, - Ensuring data privacy and data subject rights: Implementing data inventory administration and GDPR tooling to enable a data infrastructure that can fulfil the GDPR principles, data subject rights and requirements. Examples include retention policy, identity access management and data anonymization.
4	Cyber security threats and dependency on	4. Hacking of data occurs when there is insufficient data security. Risk strategies include:

	cloud security against hacking	- Conducting data privacy assessments, - Security assessments, - Risk management assessments, - Cloud provider assessments, - SLA agreements on GPDR policies.
5	Losing the banking license	5. Losing the banking license occurs when the central banks' assessment on GDPR compliance is failed by a retail bank. Risk strategies include the following: - Appointing an internal (GDPR) compliance team, Data Protection Officer, GDPR banking policy, processes, procedures, and data management process. - Having GDPR requirements for the selection of a cloud service provider and its migration method, certification, and experience, - Implement reporting processes for regulatory compliance.
6	Cloud provider trusted with data they could sell for profit	6. Having SLA agreement requirements on GDPR policies and having contract management reviews.

Table 10: GDPR cloud migration risks categorized based on consequences and their management strategies

4.2.2 Round 2

RQ3: What are the risk management strategies in response to the GDPR compliancy risks?

The results from the first interview round and literature study resulted in the following table below (Table 11) where the six main GDPR risks related to cloud migration in retail banks are displayed. The risks encompass the fines, data leaks, reputation damage, loss of customer trust, hacking, losing the banking license and data being sold by a cloud provider for profit.

These risks were analyzed using the risk-level matrix according to the literature study data on risk classification/ categorization. After the analysis of the risks, they were given categorizations score based on the literature and interview data finding their impact and probability to be either Low, Medium, or High. Every risk was given a calculated final score based on multiplying the impact score (100 = High, 50 = Medium, 10 = Low) with the probability score (1.0 = High, 0.5 = Medium, 0.1 = Low). All risks have a high impact. Yet, the probability varies. Resulting in three risks with a High final score (highly alarming), three risks with a Medium final score (moderately alarming).

4.2.2.1 Risk-Level Matrix

#	Risk	Impact	Probability	Score (High/Medium/Low)
1	GDPR fines	High (100)	High (1.0)	High 100 X 1.0 = 100
2	Data leaks, internally to clients that are competition and externally to the rest of the world creating personal damage to customers	High (100)	High (1.0)	High 100 X 1.0 = 100
3	Reputation damage and losing customer trust	High (100)	Medium (0.5)	Medium 100 X 0.5 = 50
4	Cyber security threats and dependency on cloud security against hacking	High (100)	High (1.0)	High 100 X 1.0 = 100
5	Losing the banking license	High (100)	Medium (0.5)	Medium 100 X 0.5 = 50
6	Cloud provider trusted with data they could sell for profit	High (100)	Medium (0.5)	Medium 100 X 0.5= 50

Table 11: Risk-Level Matrix

The risks from the risk-level matrix all score High or Medium in regard to their categorization and therefore have a significant impact/probability which indicates that risk strategies are required for these risks to be either accepted, mitigated, shared, transferred, or avoided. Therefore, in the following section below, the risk management strategies, also referred to as risk mitigation strategies, were combined into a table below and used to conduct interviews with interviewees. This resulted in several risk strategies per risk. The reasoning behind the scores per risk was addressed in Chapter 3.1.1.1 and the limitations of the score allocation is addressed in Chapter 5.2.

4.2.2.2 Risk management strategies per risk

Every risk was presented to interviewees by showcasing Table 12 and displaying the five risk management strategies and asking one main interview question.
The main interview question was: *"When considering the following six GDPR risks, which risk management strategy applies and how can that strategy be applied in detail?"*

The following literature definitions, cited from Chapter 2.4.3, were used to define every risk strategy (Gantz & Philpott, 2013):
"1. Acceptance: The risk is acceptable due to it falling within the limits of the organizations' risk tolerance and cost-benefit considerations tolerance.
2. Mitigation: Reducing the level of risk to a level within the risk tolerance limitations of the organization.
3. Sharing: Sharing the responsibility with a different organization to reduce the risk to an acceptable risk tolerance level for both organizations.
4. Transference: Liability of consequence or responsibility is outsourced to a different organization. For example, by purchasing insurance. The risk itself is not reduced by this strategy.
5. Avoidance: Action is taken to prevent the occurrence of the risk considering the risk is unacceptable and other risk strategies may not be effective (Stoneburner, Goguen, & Feringa, 2002), (National Institute of Standards and Technology (NIST), 2018)."

#	Risks	Risk strategy 1	Risk strategy 2	Risk strategy 3 & 4	Risk strategy 5
		Acceptance	Mitigation	Sharing & Transference	Avoidance
1	GDPR fines				
2	Data leaks, internally to clients that are competition and externally to the rest of the world creating personal damage to customers				
3	Reputation damage and losing customer trust				
4	Cyber security threats and dependency on cloud security against hacking				
5	Losing the banking license				
6	Cloud provider trusted with data they could sell for profit				

Table 12: Risk strategies table per risk

4.2.2.3 Interview round 2 summary

The results that were collected are displayed in the tables below. The following section summarizes all the tables of coded data from interview round 2 found in Appendix C. In the tables below the text displays the risk strategies given by interviewees. Afterwards, the tables showcase how the strategies can be implemented within an organization by addressing which policy or organizational changes could be made, how those changes translate to processes and procedures, and which technology usage is required to implement such changes within a retail bank’s organization.

The content of the interview data addresses why the strategies per risk strategy were showcased in tables with the categories of organizational policy (1), process/ procedure (2) and technology resource usage (3). These three categories were the main forms of answers that interviewees gave, most business and project management role fulfilling interviewees addressed organizational change, policy change and process changes. Cyber security consultants mostly addressed specific procedural changes and addressed in detail which technological resources ought to be used. Therefore, each (empty) risk strategy section of Interview Table 12 of Interview Phase 2 (Acceptance, Mitigation, Shared, Transference, Avoidance) per risk (GDPR fines, Data leaks etc.) was filled by interview data. The interview data was afterwards structured in the three categories or organizational policy, process/procedure, and technology usage.

All strategies are summarized in Chapter 5.2 Discussion & Conclusion. In the final conclusion in Chapter 5.1 and 5.2, the interview data-based risk strategies were given specific categories including information security, data privacy, customer trust, technological and contract management to showcase a more conclusive categorization of every specific risk strategy.

Risk 1: GDPR fines

- Acceptance: When accepting the risk, the finance and accounting systems can be used to review if there are sufficient cash reserves to manage a fine. When investing in policy changes is too costly, time-consuming, or complicated a calculated risk can be taken, and cash reserves can be allocated to pay the fine.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	• Having cash reserves • Possibly too costly, timely or complicated to implement policy changes	• Calculated risk is taken/accepted	• Finance/ Accounting system to review cash reserves and capacity to pay for fines.

- Mitigation: When mitigating, GDPR software and security protocols can be used to assign GDPR policy mitigation teams with the tools to conduct GDPR procedures, data privacy impact assessments and handle data protection requests. This would require the organization to build a team of IT, GDPR, Cloud, Compliance, Security and Risk professionals that work with the internally existing teams to ensure process and procedural changes required. The standard GDPR procedures include creating process changes internally where the data privacy of customer’s data is ensured, protected and that the data subject rights of customers are respected by the organization through facilitating processes that ensure these rights. This includes retention policies, the right to object the usage of customer data or ensuring that data is not accessible by unauthorized personnel. The usage of GDPR software helps manage the differing GDPR related rules, guidelines and also offers a sensitive data management overview.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Mitigation	• Assign GDPR policy/process mitigation teams	• Standard GDPR procedures, • Data protection request (How you change systems, working practices etc.) • Privacy impact assessment	• Use GDPR software • Security protocols

- Transference/Sharing: When transferring or sharing responsibility, an insurance can be chosen for professional errors. The insurance held in place ensures that the organization has limited social and financial damage due to professional failures regarding GDPR compliance since GDPR compliance related activities are outsources or the liability is outsourced. Yet, the usage of GDPR software allows for the data actors, which include the data controllers and processors to be reviewed by the organization, considering the decrease in financial liability does not ensure the limitation in reputational damage, decrease of data privacy for customers or loss customer trust. The monitoring of GDPR related processes and data privacy using GDPR software allows for improved mitigation for the risk of fines, yet the insurance allows the damage to be limited in case fines are given.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Sharing/ Transference	• Insurance for professional errors	• Knowing the data controllers and processors within and outside the organization and ensuring they are GDPR compliant.	• Use GDPR software to conduct reviews on controllers and processors.

- Avoidance: Avoiding the risk requires the bank to change their internal processes or choosing to completely erase their personal/sensitive customer data if possible. Changing processes is more realistic and can include implementing privacy by design, giving the customer the right to erasure, right to access/ insights into data processing. This can be done using data inventory administration.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Avoidance	• Changing processes	• Option: Delete all customer data, start again from scratch. • Option: Changing processes by offering the right to erasure, retention policies, right to object, right to restrict processing and all other data subject	• GDPR software / Data inventory administration

		rights to customers.	

Risk 2: Data leaks

- Acceptance: This risk can be accepted when there is an internal leak in cases where the data leak does not contain sensitive data. Generally, however, when there is a data leak that the public has access to it is critical when personal or sensitive data is involved and not acceptable. Yet, when the data leaked to the outside is non-sensitive, not personal, and non-critical it is acceptable. Data inventory administration and data privacy assessments can be used to determine where sensitive data is stored and use data anonymization techniques to minimize the impact.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	• Leaks to the outside world/public is not acceptable and the impact is too great. • Internal leaks are still acceptable in some cases. • Leaks can never be 100% prevented, risk always exists. Choose to use data anonymization to remove the impact. Probability is always present.	• Non-sensitive/non-personal data leak has less of an impact. Depends on what kind of data it is. Some is sensitive / irrelevant data. • Determining the severity and preventing personal data to be leaked should be the focus.	• Using data inventory administration • Data privacy impact assessment with GDPR software

- Mitigation: To mitigate, Identity Access Management, employee training internally and certificate verification for cloud providers can be applied to ensure high quality infrastructures where unauthorized personnel does not have access to sensitive, personal data.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Mitigation	• Minimize human errors through training • Certificates required: ISO 270001, SOC 2/3 etc. • Data storage within EU Member States.	• Security matrix and roles are defined, limit permissions to prevent data leaks • Training staff, ensuring security policies and procedures. • Restrict data and systems access to data, physically & technologically.	• Using Identity Access Management and security roles with authentication procedures with system usage. • Testing your systems, testing your controls

- Transference/Sharing: Choosing to outsource the data management activities to third party that helps maintain data security and privacy is an option as well.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Sharing/ Transference	• Outsourcing policy by dividing responsibilities/roles.	• Outsource security procedures to a third party specialized in cyber security.	• Third-party support

- Avoidance: Using data anonymization, 3 step verifications for users to gain access to data securely and using minimal (sensitive/personal) data in the cloud prevents data leaks from occurring.
  Data anonymization is a technique that allows all the sensitive and personal data to be encoded, allowing names, addresses, bank account information etc. to be mentioned in the form of unreadable numbers and letters. Therefore, even when the data is leaked, it will not be useful to external parties accessing it. The verification steps allow for users to only be able to access data when the identity is verified through ensuring that not only the password, yet also the company card, identified device and text message code have to be given. Lastly, the risk can be completely avoided by deciding to not (certain) place sensitive or personal data in the cloud.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Avoidance	• Using minimal personal/sensitive data • Using verification and anonymization to ensure that hacking or data leaks will not have any negative impact on the data privacy of customers/ data subjects.	• OTA and not your OTAP in the cloud. • Using Data anonymization techniques. • Verification necessary for every employee requesting to access data in the cloud.	• 3 step verifications with a card, identifier, and text message. • Using anonymous coding software to ensure that personal and sensitive data becomes unreadable when placed in the cloud.

Risk 3: Reputation damage and loss of customer trust

- Acceptance: Accepting responsibility through a practiced media strategy and can allow for damage control with clients and reputation.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	• Transparent, proactive communication first with clients and media, • Too much damage is never acceptable	• Show accountability • Practice the PR strategy • Having reporting procedures ready	• Data inventory administration can be used to showcase which data was leaked and how this translates to (potential) damage the company and its stakeholders ought to face.

- Mitigation: Mitigating through managing access to sensitive data through Identity Access Management with screenings and background checks for all parties interacting with data should allow for a safe and secure data management process. Which should mitigate reputational damage from occurring since the private data from customers is safe.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Mitigation	• Manage access to sensitive data	• Limit with screenings and background checks	• Identity Access Management

- Transference/Sharing: The reputational damage cannot be shared or transferred according to interviewees.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Sharing/ Transference	• Not applicable according to interviewees.	• Not applicable according to interviewees.	• Not applicable according to interviewees.

- Avoidance: Having data security assessments, preventing corruption, reviewing security vulnerabilities, having employee awareness training, reviewing data privacy vulnerabilities, and reporting all changes/investments made to the central bank/authorities showcases all will contribute to preventing circumstances that could create reputational damage. But even when they occur, the reports can showcase that all the procedures were followed and that the bank should not be receiving harsh judgement compared to organizations that did not invest as heavily in GDPR risk management.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Avoidance	• Prevent corruption and accepting gifts • Review security vulnerabilities • The central banks judgement and the degree of reputational damage is less negative if the bank showcased all procedures being done well with the DNB or in a lawsuit.	• Security procedures and measures in advance • Review customer service or data privacy failures • Employee awareness and training	• Data security assessment • Register all procedures and investments made in GDPR software • Report to the central bank/authorities through GDPR software

Risk 4: Cyber security

- Acceptance: Having on-premises back-ups and using data anonymization will allow a limited level of acceptance to be considered if combined with an insurance policy. The procedure to apply would be to also limit the sensitive data's exposure to security vulnerabilities in the cloud, by for example only placing non-critical, non-personal data in the cloud.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	• Limited level of acceptance due to insurance policy protection	• Option: Prevent having sensitive data exposed to security vulnerabilities as much as possible, including cloud environments.	• On-premises backups • Data anonymization

- Mitigation: Using cyber security software and security audits (based on the National Cyber Security Center) in combination with penetration tests allows for mitigation of hacks.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Mitigation	• Always maintain up to date with the National Cyber Security Center recommendations.	• Internal penetration tests • Check whether you are doing everything according to rules, audit	• Cyber security testing software • Security audit

- Transference/Sharing: Using monitoring software to assess the cyber security protection assurance in the organization whilst outsourcing allows for insight in the current situation regarding data safety.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Sharing/ Transference	• Look at expert companies. Share the responsibility with these types of companies. For example, cyber security companies	• Review cyber security companies/services	• Use dashboards and monitoring software to assess the cyber security protection assurance.

- Avoidance: Maintaining personal or sensitive data on its own hard disk and data center by not sharing it in the cloud and only using the cloud for non-critical data such as diaries, minutes, policy documents etc.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Avoidance	• Do not share personal data. Not even in the cloud	• Only use cloud with non-critical documents (Diaries, minutes, policy, organization charts)	• Sensitive data must be on its own hard disk and data center

Risk 5: Losing the banking license

- Acceptance: Not applicable according to all interviewees.
- Mitigation: Not applicable according to all interviewees.
- Transference/Sharing: Not applicable according to all interviewees.
- Avoidance: Applying regulatory reporting processes and software with data safety assessments in combination with policy on service management, employee awareness training and data storage locations being within the EU creates an assurance for a data management process that is GDPR compliant and will not breach GDPR regulation or customer trust. The security team monitoring the IT infrastructure whilst granting employees cyber security awareness through training allows the data to be managed in a secure manner that respects the rights and privacy of data subjects. All GDPR risks ought to be managed to successfully prevent the banking license to be lost.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.
Mitigation	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.
Sharing/ Transference	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.
Avoidance	• Prevent, insure, invest heavily, do everything possible • Host all data within the EU • Vendor management,	• Security team that monitors the IT infrastructure daily • Data storage location management • Review the SLA • Review from a legal point of	• Regulatory reporting processes and software • Data safety assessment for the cloud environment • Yearly penetration test, recovery test, data breach

	Service guarantees policy/ service management policy - Employee awareness procedures	view - Contract management review - Employee cyber security workshops, training (incl. Not clicking on certain links for example to prevent leaks/hacks)	test

Risk 6: Cloud service provider selling data for profit

- Acceptance: Having insight into the organizations data allows the personal/sensitive data to be separated from the non-critical data. Third party cloud service providers selling corporate data is unacceptable when not mentioned in the conditions. Therefore, reviewing conditions and applying contract management as prevention and legal measures consequently for the service provider are advised by interviewees.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Acceptance	- With some data it is acceptable if it is communicated by the cloud provider. - Using personal data is not acceptable.	- Review conditions and apply contract management review - Depends on which service/website it is, for example Google uses it with Salesforce for google search optimization. That's acceptable.	- Data inventory administration

- Mitigation: Havin an encryption policy allowing the cloud service provider to not have access to encrypted data yet let the retail bank be able to decrypt and view the data ensures effective mitigation since the data cannot be sold without it being decrypted first. Therefore, the data is useless for a cloud provider willing to sell this data to external parties.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage
Mitigation	- Encryption policy o Inaccessible for the cloud provider o Accessible for the retail bank	- Perform an assessment on the cloud provider.	- Use encryption to store data in the cloud but make it inaccessible to unauthorized individuals and protected. - Decrypt it on your on-premises systems and you can store it encrypted in the cloud.

- Transference/Sharing: Not applicable according to all interviewees.
- Avoidance: Having data inventory administration to ensure insight on where the data is stored, whether it is stored within the EU, therefore the vendor having to follow EU law, including GDPR policy is required. The background checks and contract management reviews are vital to ensure that the service provider is reliable and trustworthy.

Risk strategy	Organizational/Policy	Process/Procedure	Technology usage

Sharing/ Transference	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.	• Not applicable according to all interviewees.
Avoidance	• Host everything within the EU • Assess the cloud service package selection	• Data storage location management • Background checks on vendors, • Choosing a reliable partner, Certification checks • Contract management, SLA.	• Data inventory administration

Chapter 5 Discussion & Conclusion

5.1 Conclusion main research question

"What are the retail banking cloud migration risk management strategies in compliance with GDPR regulations?"

This research aimed to identify GDPR risk management strategies for retail banks conducting cloud migrations. Using qualitative analysis of semi-structured interviews and a literature study researching GDPR compliance risks when conducting cloud migration, retail banks applying GDPR and ensuring data privacy when migrating data as a retail bank to a cloud service provider. The results indicate that there are several risk management strategies that can be applied. The main results are demonstrated in the table below.
In summary the risks can be mitigated and avoided by applying the strategies mentioned in this overview table below.

#	Risks	Risk strategies
1	GDPR fines	1. Financial: Maintaining a cash reserve for fines and applying all possible procedures within the time, resource, and budget constraints to ensure GDPR compliance to avoid fines.
2	Data leaks, internally to clients that are competition and externally to the rest of the world creating personal damage to customers	2. Technological: Having identity access management processes that prevent internal and external access to data that is considered personal and/or sensitive. Also, having data anonymization and encryption software used to ensure that the data stored at a cloud service provider is not readable when leaked to the public, therefore protecting the data privacy of data subjects/customers.
3	Reputation damage and losing customer trust	3. Reputation damage occurs when media relationships worsen, and the retail bank receives negative media attention due to incompetence in maintaining customer trust and data safety and data privacy. This causes a loss of customer trust and potential legal action. To prevent a loss of customer trust, data privacy and legal action, the following risk strategies include: - Customer trust: Prepared media relationship management and PR strategy when challenges occur publicly, - Ensuring data privacy and data subject rights: Implementing data inventory administration and GDPR tooling to enable a data infrastructure that can fulfil the GDPR principles, data subject rights and requirements. Examples include: o Policy: Retention policy, o Technological: Identity access management and Data anonymization.
4	Cyber security threats and dependency on cloud security against hacking	4. Hacking of data occurs when there is insufficient data security. Risk strategies include: - Data privacy: Conducting data privacy assessments,

		- Information security: Security assessments, Risk management assessments, - Contract management: Cloud provider assessments, SLA agreements on GPDR policies.
5	Losing the banking license	5. Losing the banking license occurs when the central banks' assessment on GDPR compliance is failed by a retail bank. Risk strategies include the following: - Organizational: Appointing an internal (GDPR) compliance team, Data Protection Officer, GDPR banking policy, processes, procedures, and data management process. - Technological: Having GDPR requirements for the selection of a cloud service provider and its migration method, certification, and experience, - Compliance: Implement reporting processes for regulatory compliance.
6	Cloud provider trusted with data they could sell for profit	6. Cloud providers can have a negative impact on customer trust and data privacy due to them sharing or selling the personal or sensitive data from customers / data subjects. Risk strategies include: - Contract management: Having SLA agreement requirements on GDPR policies and having contract management reviews.

Table 13: GDPR cloud migration risks matched with risk management strategies

5.2 Risk management strategies per risk

Risk 1: GDPR fines:

Acceptance:

- Financial: When accepting the risk, the finance and accounting systems can be used to review if there are sufficient cash reserves to manage a fine. When investing in policy changes is too costly, time-consuming, or complicated a calculated risk can be taken, and cash reserves can be allocated to pay the fine.

Mitigation:

- Information security, software, policy: When mitigating, GDPR software and security protocols can be used to assign GDPR policy mitigation teams with the tools to conduct GDPR procedures, data privacy impact assessments and handle data protection requests.

Transference/Sharing:

- Policy: When transferring or sharing responsibility, an insurance can be chosen for professional errors.

Avoidance:

- Processes and data privacy: Avoiding the risk requires the bank to change their internal processes or choosing to completely erase their personal/sensitive customer data if possible. Changing processes is more realistic and can include implementing privacy by design, giving the customer the right to erasure, right to access/ insights into data processing. This can be done using data inventory administration.

Risk 2: Data leaks:
Acceptance:

- Data privacy: This risk can be accepted when there is an internal leak in cases where the data leak does not contain sensitive data. Generally, however, when there is a data leak that the public has access to it is critical when personal or sensitive data is involved and not acceptable. Yet, when the data leaked to the outside is non-sensitive, not personal, and non-critical it is acceptable. Data inventory administration and data privacy assessments can be used to determine where sensitive data is stored and use data anonymization techniques to minimize the impact.

Mitigation:

- Technological and Information security: To mitigate, Identity Access Management, employee training internally and certificate verification for cloud providers can be applied to ensure high quality infrastructures where unauthorized personnel does not have access to sensitive, personal data.

Transference/Sharing:

- Organizational/ Policy: Choosing to outsource the data management activities to third party that helps maintain data security and privacy is an option as well.

Avoidance:

- Technological and Information Security: Using data anonymization, 3 step verifications for users to gain access to data securely and using minimal (sensitive/personal) data in the cloud prevents data leaks from occurring.

Risk 3: Reputation damage and loss of customer trust
Acceptance:

- Procedure Media relations: Accepting responsibility through a practiced media strategy and can allow for damage control with clients and reputation.

Mitigation:

- Customer trust, data privacy and Information Security: Mitigating through managing access to sensitive data through Identity Access Management with screenings and background checks for all parties interacting with data should allow for a safe and secure data management process. Which should mitigate reputational damage from occurring since the private data from customers is safe.

Transference/Sharing:

- The reputational damage cannot be shared or transferred according to interviewees.

Avoidance:

- Data privacy and Information security: Having data security assessments, preventing corruption, reviewing security vulnerabilities, having employee awareness training for hacking, reviewing data privacy vulnerabilities, and reporting all changes/investments made to the central bank/authorities showcases all will contribute to preventing circumstances that could create reputational damage.
- Compliance: But even when circumstances occur that can cause reputational damage, the compliance reports can showcase that all the procedures were followed and that the bank should not be receiving ‘harsh judgement’ compared to organizations that did not invest as heavily in GDPR risk management.

Risk 4: Cyber security threats/ hacking
Acceptance:

- Technological and data privacy: Having on-premises back-ups and using data anonymization will allow a limited level of acceptance to be considered if combined with an insurance policy. The procedure to apply would be to also limit the sensitive data's exposure to security vulnerabilities in the cloud, by for example only placing non-critical, non-personal data in the cloud.

Mitigation:

- Information security: Using cyber security software and security audits (based on the National Cyber Security Center) in combination with penetration tests allows for mitigation of hacks.

Transference/Sharing:

- Information security: Using monitoring software to assess the cyber security protection assurance in the organization whilst outsourcing allows for insight in the current situation regarding data safety.

Avoidance:

- Technological and data privacy: Maintaining personal or sensitive data on its own hard disk and data center by not sharing it in the cloud and only using the cloud for non-critical data such as diaries, minutes, policy documents etc.

Risk 5: Losing the banking license
Acceptance:

- Not applicable according to all interviewees.

Mitigation:

- Not applicable according to all interviewees.

Transference/Sharing:

- Not applicable according to all interviewees.

Avoidance:

- Compliance, data privacy and software: Applying regulatory reporting processes and software with data safety assessments in combination with policy on service management, employee awareness training and data storage locations being within the EU creates an assurance for a data management process that is GDPR compliant and will not breach GDPR regulation or customer trust.
- Information security: The security team monitoring the IT infrastructure whilst granting employees cyber security awareness through training allows the data to be managed in a secure manner that respects the rights and privacy of data subjects. All GDPR risks ought to be managed to successfully prevent the banking license to be lost.

Risk 6: Cloud service provider selling data for profit
Acceptance:

- Contract management and data privacy: Having insight into the organizations data allows the personal/sensitive data to be separated from the non-critical data. Third party cloud service providers selling corporate data is unacceptable when not mentioned in the conditions. Therefore, reviewing conditions and applying contract management as prevention and legal measures consequently for the service provider are advised by interviewees.

Mitigation:

- Information security and data privacy: Having an encryption policy allowing the cloud service provider to not have access to encrypted data yet let the retail bank be able to decrypt and view the data ensures effective mitigation since the data cannot be sold without it being decrypted first. Therefore, the data is useless for a cloud provider willing to sell this data to external parties.

Transference/Sharing:

- Not applicable according to all interviewees.

Avoidance:

- Contract management and technological: Having data inventory administration to ensure insight on where the data is stored, whether it is stored within the EU, therefore the vendor having to follow EU law, including GDPR policy is required. The background checks and contract management reviews are vital to ensure that the service provider is reliable and trustworthy.

5.3 Discussion

In approaching the research, the decision was made to conduct qualitative research. Conducting quantitative research would require statistical data or survey data. The choice to apply qualitative data collection was a more applicable approach since in-depth information was required that was not of quantitative or statistical nature. The data would have to give in-depth information and context on complex subjects intertwined with each other. The subjects GDPR compliance, cloud migration, retail banks and risk management strategies all require in-depth understanding of their context to combine the data on these subjects to formulate answers to the main research question.

5.3.1 Key findings

The most important findings can be summarized by quoting the following sections from the results chapter below:

Sub-research question 1:
The interview data indicates that interviewees define cloud migrations as "the migration of parts of the IT infrastructure, application landscape and/or data from an on-premises environment to an external cloud services provider." This interview data is consistent with the literature study results showcasing a similar definition. Yet, within the context of retail banking the literature study data does not define notable distinctions between other organizations.

Yet, the interview data addresses that the context of a retail bank requires the cloud migration to be "characterized by relevant factors when conducting a migration regarding the technological perspective such as the cloud maturity, existing IT infrastructure, service needs, requirements, service model, deployment model, migration method, challenges migrating certain systems (such as legacy systems), cloud migration strategy, high and low latency when migrating, identity access management and data security."

Sub-research question 2:
Both the interview data and the literature study support the identification of the same risks: "The following risks can occur when organizations are not GDPR compliant within retail banks when migrating data to the cloud according to the interviewees":

- Data leaks,
- Reputational damage,
- Hacking,
- Fines from the EU,
- Lack of data privacy,
- Personal damage to customers due to data leaks/hacks,
- Loss of the banking license and the bank ceasing to exist due to failing DNB assessments.

Sub-research question 3:
"To ensure that the data usage within the bank and when migrating data to a third party is GDPR compliant, the bank can use resources and procedures such as":

- Organizational: Creating a GDPR banking policy, processes, procedures,
- Technological: using GDPR software tools,
- Personnel: appointing a Data Protection Officer,
- Data privacy procedures: using data privacy assessments,
- Advisory: external consultancy,
- Information security: security assessments, security awareness staff training,
- Policy: data processing agreements,
- Contract management: SLA contract management and data anonymization.

5.3.2 Generalizability

The data collected from the literature study was generalizable for GDPR compliance in organizations considering that the regulation applies in all the Member States of the European Union. Yet, how the GDPR specifically applies in retail banks was not (heavily) researched and was a gap in literature.
Therefore, considering as a researcher and former Technology Process Analyst at a Dutch retail bank, I had sufficient connections in my professional network to request interviews. My network offered a set of banking and consulting organizations with IT and retail banking professionals having 2 to 15+ years of experience. The professionals and organizations asked were international, large corporations. Certain IT professionals that were interviewed had worked at all the 5 largest Dutch retail banks. Including ING, ABN AMRO, Rabobank, NIBC Bank etc. Therefore, the generalizability and trustworthiness of the answers given by the interviewees were based on relevant working experience and an in-depth understanding of the context. The backgrounds of the interviewees (Cloud consultant, Data scientist, Privacy & Cyber Security Consultant, Infrastructure Team Lead, Cloud Implementation Project Manager etc.) and the diversity in retail banking and consulting organizations (NetApp, Capgemini, Centric, Deloitte, KPMG, Ordina, Cegeka etc.) where they (had) worked gave sufficient evidence of trustworthiness and generalizability for the answers given.

5.3.3 Limitations

The literature was based on international standards, whilst the interviewees were limited to the Netherlands and UK, with employees who have worked or studied in other countries such as Ghana, South-Africa, China, and Ukraine. Therefore, the context of the interview data is applicable to the Netherlands, UK, and most Member

States of the European Union where all the banking regulations are supervised by the European Central Bank and Dutch central bank (De Nederlandsche Bank).

There is an awareness of the legal implications on a national and continental scale that all interviewees portrayed in the context of their answers, but not in-depth applicable differences identified in how the application of the GDPR risk management strategies would be effective outside of the Netherlands and UK.
Generally, the GDPR policies are applicable in all Member States of the European Union, so therefore, most differences are accompanied for by the EU through the standards the GDPR applies, yet countries may have differing manners in which they apply the regulations. So therefore, interviewing the interviewees predominantly from the Netherlands and UK, despite their diverse backgrounds, may still leave an opportunity to enrich the interview data with interviews with retail banks located in other Member States in the EU such as Poland, Belgium, France, Spain, Italy, or Greece. Yet, the trustworthiness of the interview data is still ensured due to the interviewee criteria being met by all interviewed professionals.

Regarding the interviewee answers of Phase 2, described in Chapter 4.2.2.3, there are limitations considering the differing backgrounds of interviewees creating different interpretation of the definitions of the risk management strategies in round 2. Several interviewees gave answers that could not directly be categorized under one of the five risk strategies categories (acceptance, mitigation, sharing, transference, and avoidance). Therefore, their strategies were eventually placed under one of the five risk strategies after discussion during the process of conducting the interviews in collaboration with the interviewees. This, however, has caused certain risk strategies to be placed under the category of risk strategies that may be considered to be placed under a risk strategy category that may require correction due to misinterpretation by interviewees of the definition of the risk strategies. This was mentioned by several interviewees during the semi-structured interviews of Phase 2. Predominantly, strategies placed under the strategy category “Risk strategy 5: Avoidance” was often mistake for “Risk strategy 2: Mitigation”. Yet, the placement of the strategies has not been altered due to the fact that the interviewees were convinced of these strategies being correct within the context of their own organization and professional experience.

The risk categorization of every risks’ classification score (High, Medium, and Low) based on the probability multiplied by the impact of a risk, was based on the literature regarding the risk-level-matrix. Yet, the measurement of probability and impact of the six main GDPR compliance risks found in the research results is limited to interpretations of the risk by interviewees, derived from the interview results. Interviewees were requested to focus only on risks with a high to medium impact and high probability. Therefore, all risks were given a final classification score of Medium or High. Yet, the final score, as well as the probability and impact of a risk is dependent on factors that happen to be outside the limitations of the research. Risk 5, losing the banking license can be considered a risk with a high impact under any circumstance, yet the probability depends on the GDPR related measures an organization has managed to implement that ensure GDPR compliance. When these measures are implemented according to the standards of the GDPR regulation, the probability can be considered Low, yet when the standard are not met and the GDPR compliance has been insufficient for extended periods of time, surpassing potential warnings from central banks or authorities, the probability of Risk 5 occurring would be considered High. Therefore, the limitations regarding the classification score allow for different interpretations based on the circumstances an organization is facing. Within this research's risk classification specific scenarios or circumstances have not been used. Scores per organization and Member State within the European Union may differ in practice.

5.3.4 Interpretations

The results are highly consistent with the found literature. The answers however, given by interviewees, tend to differ based on the experience, expertise, and category that the interviewee fits into based on their role and the company they work for. Many interviewees used their expertise and work experience as a reference. Hereby, examples were given where their work environment, projects they have been involved in, challenges found within their company and news reports were mentioned. Therefore, I found there to be a correlation with the strategies given and the background of the interviewee. The interviewees with a background in cyber security addressed more details in their answers and used the cyber security viewpoint in many of their answers. This was mostly the case for the consultants. A correlation with the consultants and their answers is the fact that they give in-depth knowledge based on expertise but there is less connection with work experience related to financial services. Therefore, their answers were valuable, but more so from an external viewpoint. The context brought forth by professionals in retail banking allowed there to be more insight as to which risk management strategies can realistically be applied.

The answers given by the retail banking professionals with an IT background in cloud, data or project management was limited to the viewpoints of an internal banking employee. In this case, the working experience combined with the expertise allowed the results to seem more trustworthy. Yet, less self-critical. And the expertise was less technical. Considering the consultants are external and the retail banking IT professionals are internal employees, there could be a correlation between the external consultants offering advanced expertise yet lack experience, and the internal employees offer experience yet lack advanced expertise. Most answers given by the internal retail bankers had less technical depth then the external IT consultant.
A correlation can also potentially be made with the fact that many of the retail bankers interviewed had part of their IT process activities already outsourced and supported by external consultants.

The expectation I had beforehand was that the retail bankers would have more in-depth technical answers and perspectives on how to offer solutions. Yet, the external consultants had more of this than the retail banking employees. Also, a second expectation was that the strategies would be clear, concise, specific and address a similar level of detail. Yet, interviewees gave differing levels of detail in their answers. Also, their answers often consisted of high-level answers or in-depth procedures that could apply, not structured, thought-out strategies to systematically manage risks.

Despite, the lack of structure, the applicability and the unexpected answers given were consistently surprising, all interviewees agreed on certain strategies for multiple questions, yet for other questions their answers differed enormously based on their background. This also allowed me to understand that the answers are all applicable, yet applicable in the environment the interviewee considers, which would be a different environment for an external cyber security consultant versus an internal data scientist. The data scientist works within a set of team members focused on data projects. Therefore, his/her perspective is influenced by the data team/department. The security consultant speaks to other security consultants, has a more overseeing viewpoint reviewing different departments company-wide and will be able to give different advice.

Yet, the different perspectives altogether allow for a diverse, trustworthy set of answers considering the legal, security, data, cloud, technical, process, policy, compliance, internal, external, managerial, financial, social, cultural point of views altogether. Yet, it allows for less pattern recognition on strategies. Except, for answers that can be supported with literature.

The results indicate as well that there is a relationship between the different risks. The failure of the central banking assessment for a bank allows banks to not be considered GDPR compliant, which causes them to be vulnerable to fines, reputation damage, hacks, data leaks and having their cloud service provider sell data for profit. Which is followed by the consequences of a loss in customer trust, customer count, revenue, and have reputational damage. Which will allow the banking authorities to take away the banking license of a bank letting the organization cease to exist legally. This pattern of consequences is consistent with the literature on GDPR risks found in Chapter 2.5.

5.3.5 Implications

The results of the study are consistent with the existing descriptive literature on cloud migration, cloud computing, GDPR, risk management strategies and retail banking. The new insights contributed are the list of specific risk management strategies per GDPR risk specifically applicable in West-European large to mid-sized retail banks. The data delivers a clearer understanding of how the GDPR policy ought to be applied in practical procedural retail banking policies resulting in improved data privacy, data security and GDPR compliance. The results do not contradict existing literature.

5.3.6 Contributions

Afterwards, the literature study data was found to be applicable but there was a gap in research present in current existing literature. The gap in research was filled by the interviews that were conducted and allowed new research data to be offered to academia reviewing in-depth risks regarding the GDPR when migrating data to a cloud services provider in the retail banking industry. Retail banks may use this research as suggestions for applying strategies for their cloud migration. projects and managing GDPR compliancy risks regarding such procedures.

5.3.7 Recommendations and future research

Further research will allow the different strategies to be expanded on in detail. The results indicate that the application of a GDPR banking policy including processes and procedures such as data anonymization and data inventory administration would allow the overall data privacy of customers and their customer data to be improved.

- Further research can explore the in-depth details regarding how strategies mentioned in the results chapter may be delivered/ executed specifically within the retail banking industry migrating data to a third-party cloud services provider.
- Further research can explore potential differences in the effectiveness of risk management strategies in different EU Member States based on the technological maturity, corruption, cloud maturity and as to what extent restrictions are considered when managing data within the entire country. Certain hypothesis may be framed where the impact of how the GDPR is applied per country could cause sufficient differences in circumstances as to which countries require potentially different risk management strategies. This research enrichment could result in the confirmation that mentioned risk management strategies apply in potentially most retail banks within the European Union.

Chapter 6 Reflection

The following sections intends to offer an academic, personal, and systematic perspective on the research conducted. With the objective the critically assess whether the research results or research conducted were influenced by factors whilst conducting the research which may have influenced the outcome of the results.

6.1 Academic perspective

Despite having a background in information technology and having working experience at a retail bank in a process analyst role, understanding three topics requiring different specialized backgrounds requires taking a risk.

The first risk when conducting the research was that I would lack the understanding and context on the topics to recognize what information/literature I needed to research to be sufficiently educated on the topics to write down, find, understand all three different topics in ways that allow there to be a constructive set of interview questions created and literature study conducted. There was not a large gap in knowledge for myself as a researcher considering I had working experience and a matching academic background. This enabled me to understand the context of the differing topics cloud, GDPR and banking. The risk was also managed by conducting exploratory interviews before starting the actual interview rounds.

A second risk was that the interviewees had differing backgrounds, experience, and expertise. This was managed by recognizing that the diversity of perspectives was required for giving in-depth answers on certain topics. A retail banking employee working as an IT project manager, has a more high-level perspective but will give certain viewpoints that a specialist such as a retail banker who is a data scientist will not be able to give. Despite the specialist's knowledge on the different topics is more valuable, a diverse range of perspectives was necessary to understand the relationship between the different topics.

A third risk was that the relationship between the topics cloud, GDPR and banking are not possible to be made in a methodologically driven manner which may be required. Yet, in practice, the topics did not need to relate to each other in procedural manner, the data given was analyzed and the interview questions created sufficient context for all the different topics to be addressed by interviewees in relationship to each other. Yet, it did create a circumstance where the literature can give a detailed confirmation on the risk management strategies advised, yet, not within the context of retail banking since that literature is not available.

In conclusion, the research conducted contained results and strategies known in literature, yet not applied within the specific context of retail banking with a focus on cloud migration projects. Initial expectations were purposefully held off since the data that needed to be gathered was so complex. Therefore, there was not a focus on a specific hypothesis beforehand.

6.2 Approach perspective

Things I would have done differently would be the following points below:

Firstly, to have a search strategy for finding IT professionals. I had a set of criteria for interviewees. But it would have been better if I had a strategy to find the professionals with the most suitable backgrounds more easily. Yet, I also was somewhat limited to my own network since individuals I approached on LinkedIn outside of my network did not respond to my requests.

Secondly, to have a structure and categorization of the type of risk management strategies to include a structured method for the level of depth a strategy requires to have. Which could be strategic, tactical, operational. Yet also, programs level, department level, project level, process level, procedural level. Through this structure the answers could have been more easily categorized into a model.

Thirdly, I would have a coding plan with preexisting codes to ensure a more efficient process when conceiving a set of answers.

Lastly, I would have had less interview questions and more follow-up questions with interviewees with the structures addressed in the previous paragraphs. This could have resulted in more valuable, detailed answers.

References

W. Kuan Hon, C. M. (2018). Banking in the cloud: Part 1 – banks' use of cloud services. *Computer law & security review 34* , 4–24.

Derrick Rountree, I. C. (2014). *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice.* Waltham MA: Elsevier.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing — The business perspective. *Decision Support Systems 51* , 176–189.

Forbes. (2019, July 22). *Banks' Inevitable Race To The Cloud*. Retrieved from www.forbes.com/: https://www.forbes.com/sites/ronshevlin/2019/07/22/banks-inevitable-race-to-the-cloud/?sh=5118c17b1135

Calvet, S. (2017). *WHAT'S DRIVING THE RETAIL BANKING INDUSTRY TO CLOUD?* Retrieved from www.accenture.com: https://www.accenture.com/t20171228T034133Z__w__/us-en/_acnmedia/PDF-69/Accenture-Cloud-Vision-POV-Retail-Banking-111817.pdf

Mell, P., & Grance, T. (2011, September). *The NIST Definition of Cloud Computing* . Retrieved from https://csrc.nist.gov/: https://csrc.nist.gov/publications/detail/sp/800-145/final

Capgemini Consulting. (2017, July). *Backing up the Digital Front: Digitizing the Banking Back Office*. Retrieved from www.capgemini.com/: https://www.capgemini.com/wp-content/uploads/2017/07/backing_up_the_digital_front25_11_0.pdf

McKinsey. (2016, April). *FinTechnicolor: The New Picture in Finance.* Retrieved from www.mckinsey.com: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/bracing%20for%20seven%20critical%20changes%20as%20fintech%20matures/fintechnicolor-the-new-picture-in-finance.ashx

Directive (EU) of the European Parliament and of the Council. (2015, September 9). *Art. 4 GDPR Definitions.* Retrieved from https://gdpr-info.eu/: https://gdpr-info.eu/art-4-gdpr/

European Commission, Directorate-General for Communication. (2020). *Under what conditions can my company/organisation process sensitive data?* Retrieved from ec.europa.eu: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

Directive of the European Parliament and of the Council. (2014, March 12). *Art. 5 GDPR Principles relating to processing of personal data.* Retrieved from https://gdpr-info.eu: https://gdpr-info.eu/art-5-gdpr/

Rountree, D., & Castrillo, I. (2014). *The Basics of Cloud Computing Understanding the Fundamentals of Cloud Computing in Theory and Practice* . 225 Wyman Street, Waltham, MA 02451, USA: Elsevier.

(Olaru), M.-G. A. (2014). *Advantages and challenges of adopting cloud computing from an enterprise perspective.*

Avram (Olaru), M.-G. (2014). Advantages and challenges of adopting cloud computing from and enterprise perspective. *Procadia Technology 12*, 529-534.

Cloudflare. (2021, February 15). *What is the cloud? Public vs. Private cloud*. Retrieved from Https://www.Cloudflare.com: https://www.cloudflare.com/en-gb/learning/cloud/what-is-a-public-cloud/

Laszewski, T., & Nauduri, P. (2012). Chapter 1 - Migrating to the Cloud: Client/Server Migrations to the Oracle Cloud. *Migrating to the Cloud Oracle Client/Server Modernization* , Pages 1-19. Retrieved from https://www.sciencedirect.com/science/article/pii/B9781597496476000016

Gurkok, C. (2013). Chapter 6 - Securing Cloud Computing Systems. *Computer and Information Security Handbook (Second Edition)*, Pages 97-123.

Kearns, D. K. (2017, December). *Planning & Management Methods for Migration to a Cloud Environment.* McLean, VA: The MITRE Corporation. Retrieved from https://www.mitre.org/sites/default/files/publications/pr-17-4029-planning-management-methods-migration-to-cloud-environment.pdf

Jamshidi, P., Ahmad, A., & Pahl, C. (2014). Cloud Migration Research: A Systematic Review. *IEEE TRANSACTIONS ON CLOUD COMPUTING*, 142-157. Retrieved from https://ulir.ul.ie/bitstream/handle/10344/3656/Jamshid_cloud.pdf;jsessionid=EE0DE0CF1FE4FAAB74E21A812CF31DA7?sequence=2

Hughes, H. K., Randhella, S., & Tatwani, V. (2021). Retrieved from www.infosys.com: https://www.infosys.com/about/knowledge-institute/insights/documents/cloud-migration.pdf

Watson, R. (2010, December 03). *Migrating Applications to the Cloud: Rehost, Refactor, Revise, Rebuild, or Replace?* Retrieved from https://www.gartner.com: https://www.gartner.com/en/documents/1485116/migrating-applications-to-the-cloud-rehost-refactor-revi

NetApp. (2019, July 25). *AWS Migration Strategy: The 6 Rs in Depth.* Retrieved from https://cloud.netapp.com/: https://cloud.netapp.com/blog/aws-migration-strategy-the-6-rs-in-depth

Clayton, T. (2018, November 20). *Decision Point for Choosing a Cloud Migration Strategy for Applications.* Retrieved from https://www.gartner.com/: https://www.gartner.com/en/documents/3893681/decision-point-for-choosing-a-cloud-migration-strategy-f

De Nederlandsche Bank. (2017, April 1). *Definition of a bank.* Retrieved from https://www.dnb.nl/: https://www.dnb.nl/en/sector-information/supervision-sectors/banks/licence-as-a-bank-overview/definition-of-a-bank/

Hargrave, M. (2020, October 23). *Investment Bank.* Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/i/investmentbank.asp

Dixon, A. (2019, July 19). *Types of Banks.* Retrieved from https://smartasset.com/: https://smartasset.com/checking-account/types-of-banks

Commercial Banks Guide. (2015). *USA Commercial Banks*. Retrieved from www.commercialbanksguide.com: http://www.commercialbanksguide.com/usa+commercial+banks/

Kagan, J. (2021, February 21). *Commercial Bank*. Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/c/commercialbank.asp

Majaski, C. (2021, April 30). *Retail Banking vs Commercial Banking*. Retrieved from https://www.investopedia.com/:

https://www.investopedia.com/articles/general/071213/retail-banking-vs-commercial-banking.asp

Corporate Finance Institute. (2021). *Corporate Banking*. Retrieved from https://corporatefinanceinstitute.com: https://corporatefinanceinstitute.com/resources/knowledge/finance/corporate-banking/

Chen, J. (2020, August 31). *Private Banking*. Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/p/privatebanking.asp

International Monetary Fund. (2021, March 16). *Monetary Policy and Central Banking*. Retrieved from https://www.imf.org/: https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/20/Monetary-Policy-and-Central-Banking

Segal, T. (2020, September 29). *Central Bank*. Retrieved from https://www.investopedia.com/: https://www.investopedia.com/terms/c/centralbank.asp

Frankenfield, J. (2020, May 4). *Online Banking*. Retrieved from https://www.investopedia.com: https://www.investopedia.com/terms/o/onlinebanking.asp

Grantt, M. (2021, February 24). *Credit Union*. Retrieved from https://www.investopedia.com/: https://www.investopedia.com/terms/c/creditunion.asp

Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). *Risk Management Guide for Information Technology Systems.* Retrieved from https://www.archives.gov: https://www.archives.gov/files/era/recompete/sp800-30.pdf

Hirao, J., & Wun-Young, L. (2009). *SAP Security Configuration and Deployment: The IT Administrator's Guide to Best Practices.* Elsevier. Retrieved from https://www.sciencedirect.com/book/9781597492843/sap-security-configuration-and-deployment

Federal Virtual Training Environment (FedVTE). (2014). *NIST SP 800-39 and 800-37.* Retrieved from https://fedvte.usalearning.gov/: https://fedvte.usalearning.gov/courses/CRRM/course/videos/pdf/CRMM_D01_S02_T03_STEP.pdf

Johnson, L., Kovacich, D. G., & Jones, D. A. (n.d.). *Risk Management Process.* Retrieved from https://www.sciencedirect.com/: https://www.sciencedirect.com/topics/computer-science/risk-management-process

Metheny, M. (2017). *Federal Cloud Computing: The Definitive Guide for Cloud Service Providers* . Elsevier. Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/book/9780128097106/federal-cloud-computing

Johnson, L. (2019). *Security Controls Evaluation, Testing, and Assessment Handbook* . Elsevier.

Beckett, P. (2017, May 18). *GDPR compliance: your tech department's next big opportunity.* Retrieved from https://reader.elsevier.com: https://reader.elsevier.com/reader/sd/pii/S1361372317300416?token=91D7942688F2562E7F1F9A2A7AAE7FDBEFCD83278696CAC366A32C94E1E11D5532E5EFDA3BFE0A4614402BEBA65DC376&originRegion=eu-west-1&originCreation=20210506185147

National Institute of Standards and Technology (NIST). (2018, December). *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy.* Retrieved from https://nvlpubs.nist.gov/: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

European Parliament. (2014). General Data Protection Regulation GDPR / REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Union*. Retrieved from https://gdpr-info.eu: https://gdpr-info.eu

Politou, E., Michotab, A., Alepisa, E., Pocsc, M., & Patsakis, C. (2018, September 13). *Backups and the right to be forgotten in the GDPR: An uneasy relationship.* Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S0267364918301389?via%3Dihub https://www.sciencedirect.com/science/article/pii/B9780128054673000090?via%3Dihub

Khaled, N., Pattel, B., & Siddiqui, A. (2020). *Digital Twin Development and Deployment on the Cloud* . Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/book/9780128216316/digital-twin-development-and-deployment-on-the-cloud

Information Commissioner's Office (UK). (2021). *Guide to the General Data Protection Regulation GDPR.* Retrieved from https://ico.org.uk: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Voigt, P., & Bussche, A. v. (2017, Augustus 28). *The EU General Data Protection Regulation (GDPR) : A Practical Guide (Book).* Retrieved from https://ebookcentral-proquest-com.ezproxy.leidenuniv.nl/: https://ebookcentral-proquest-com.ezproxy.leidenuniv.nl/lib/leidenuniv/reader.action?docID=4942001&ppg=207

Orban, S. (2016, November 01). *6 Strategies for Migrating Applications to the Cloud* . Retrieved from https://aws.amazon.com/: https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

Efremovska, A., & Lago, P. (2017, June 23). *Chapter 9 - From Legacy to Cloud: Risks and Benefits in Software Cloud Migration.* Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/science/article/pii/B9780128054673000090?via%3Dihub

Laszewski, T., & Nauduri, P. (2012). *Migrating to the Cloud: Oracle Client/Server Modernization.* Elsevier. Retrieved from https://www.sciencedirect.com/book/9781597496476/migrating-to-the-cloud

Efremovska, A., Lago, P., Kemmerich, T., Laszewski, T., & Nauduri, P. (2017). *Cloud Migration.* Retrieved from https://www.sciencedirect.com: https://www.sciencedirect.com/topics/computer-science/cloud-migration

Gantz, S. D., & Philpott, D. R. (2013). *FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security* . ScienceDirect. Retrieved from https://www.sciencedirect.com/book/9781597496414/fisma-and-the-risk-management-framework

Appendices

Appendix A: Thesis topic introduction

Thesis topic introduction and small talk

“Thank you for being here and granting me some of your time, I am absolutely grateful and very happy to speak to you.
Maybe we should shortly introduce ourselves to each other briefly to start.”
[Allow the interviewee to introduce themselves if they would like to do so first.] (Rountree & Castrillo, 2014)
“I am a MSc ICT & Business student at Leiden University, and I am writing my masters’ thesis about understanding the GDPR risks in cloud migration. With a specific focus on retail banking. Of course, that process is complex since managing risks regarding not being GDPR compliant can be a huge challenge. The aim of this research is making sure that those GDPR risks with all the sensitive data are managed is really what I am trying to identify whilst also understanding what strategies can be used to manage those compliancy risks. In case, you feel uncomfortable answering questions for any reason, feel free to not answer these questions or stop the interview. In case, you do not have sufficient time to continue the interview due to unexpected events, feel free as well to stop the interview. Your name and company name will not be displayed when processing the information for the thesis research study.
Before we start, is it possible for me to record the interview? Feel free to refuse this request since it is perfectly fine for me to write the information down during the interview as well. The interview and transcript will remain confidential, and the interview recording will be deleted after the transcription is completed.”

Approaching Dutch speaking former colleagues or professionals in my network on LinkedIn or WhatsApp has been done by sending the following message:

“Hi [insert name], how are you?
It's Jousuf from [address previous work relationship together or last meeting together]. I was wondering if I could message you about a request. After [address last point of contact together] I started doing a master's at Leiden University and I am currently writing my thesis on “GDPR compliance in cloud migrations in banks”. For this I am looking for IT professionals working at banks who are open to hold a meeting for an interview of 30-45 minutes for this thesis research. You may have a hole this month or the next and are open to it. I fully adapt to your schedule. If possible, this would be great. Thank you very much in advance! Greetings, Jousuf.”

After this a follow-up message was sent to set an appointment after interviewee agrees to conduct and interview:
“Hi [insert name],
Thanks again for the help with the thesis!
Now I have progressed further, and the interview phase has started. I was wondering when would be best in the next few weeks to do an interview together for 30-45 min? Maybe next week or the week after [insert relevant date]? Greetings, Jousuf”.

Appendix B: Results interview round 1

Research question 1: Coded results overview

Sub-research questions

1. Has your organization been involved in cloud migrations?

Interview data SRQ1: All organizations where interviewees work are involved or have been in involved in migrating data to the cloud or advising in this process. Some have not been directly involved but their organization has.
Aspects that are important when migrating data in banks is having risk assessments, secure data migration environments and a consideration for banking and DNB policies. Also, a data privacy administration is important when migrating data to the cloud since you need to know where your data is stored and how to find it and delete it.

RQ	Code	Count	Contributors
RQ1 – SRQ1	Yes	8	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ1	No	0	-
RQ1 – SRQ1	Yes, one of our tools for this is the = data privacy register	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ1	Yes, one of our tools for this is the = risk assessments	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ1	Yes, one of our tools for this is = the report to DNB	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ1	Yes, one of our tools for this is the = secure data migration environments	2	Retail banker, cloud consultant, privacy consultant

2. Does your organization consider sensitive personal data when conducting a cloud migration?

Interview data SRQ2: Personal data is always considered when migrating data since the internal and external audit teams will have to ensure that the data privacy regulations of the company and GDPR guidelines are followed. Therefore, data containing sensitive information retraceable to a natural person will be assessed with a data privacy assessment to ensure that cloud related risks are prevented. Also, other GDPR regulations such as having the location of the data maintaining in the EU will be considered and followed, auditing teams will try to ensure all legal and compliance requirements are met.

Question	Code	Count	Contributors
RQ1 – SRQ2	Yes	8	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant, data scientist, implementation manager
RQ1 – SRQ2	No	0	7.
RQ1 – SRQ2	Yes, we consider through using and managing = data privacy assessments	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant, data scientist, implementation manager
RQ1 – SRQ2	Yes, we consider through using and managing = Cloud related risks	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ2	Yes, we consider through using and managing = data location	2	IT business consultant, cloud consultant

3. How are cloud migrations defined?

Interview data SRQ3: A cloud migration according to interviewees is the migration of parts of the IT infrastructure, application landscape and or data used on -premises to an external third-party cloud services provider.

Banks have a dependency on their IT infrastructure, and this determines their business, functional, non-functional, technical requirements, and migration method. The DNB assessments and internal and external audits made will be considered when making decisions regarding migrating to a cloud environment and how that environment should look like. The cloud environment could be a customized environment, public, private, hybrid and community cloud.

There can be multiple cloud providers and the choice can be made to only outsource infrastructure (IaaS), application landscape (PaaS) or the services (SaaS). The methodology to migrate therefore differs, banks tend to have legacy systems that are difficult to migrate with high latency, and low-latency applications easy to migrate. Often, front-end is low latency such as the website and CRM. Mentioned options to migrate are:

- Server first,
- First front-end and then back-end,
- Based on low latency first,
- Partly migrating,
- Moving the data warehouse/data bases,
- Moving personal data to a private cloud,
- Using a container like Docker, Kubernetes (having all your operating systems, databases in here),

- Testing the cloud environments connection to migrate in a testing environment with irrelevant data,
- Only migrating non-personal data to a public cloud,
- Having partly on-premises, partly cloud-infrastructure (hybrid)

Question	Code	Count	Contributors
RQ1 – SRQ3	Migration of parts of the infrastructure, applications and/or data	8	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Using different service models	6	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Moving data, application, infrastructure to a third-party cloud services provider	8	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Using different deployment models	6	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	They tend to be reviewed through audits	3	Retail banker, IT business consultant, cloud consultant
RQ1 – SRQ3	They tend to be reviewed through: DNB assessment	4	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Tend to be migrated by the method: server first	1	Retail banker, cloud expert,
RQ1 – SRQ3	Tend to be migrated by the method: Low latency first	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Tend to be migrated by the method: First front-end	1	Retail banker, cloud expert,
RQ1 – SRQ3	Tend to be migrated by the method: move my data warehouse	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ1 – SRQ3	Tend to be migrated by the method: including your operating system and databases, all in your container	2	Retail banker, cloud expert, IT business consultant,
RQ1 – SRQ3	Tend to be migrated by the method: dependency on application landscape	1	Retail banker, cloud expert

RQ1 – SRQ3	Tend to be migrated by the method: Container, Docker	2	Retail banker, cloud expert, IT business consultant,
RQ1 – SRQ3	Defined by the types: public, private, on-premises, hybrid	2	Retail banker, cloud expert, IT business consultant,

4. How are cloud migrations conducted within retail banks?

Interview data SRQ4: Predominantly, the same way, for the most part. There are different policies to consider when migrating data from banks will require approval from the compliance department, security, service level agreements need to be met since applications that the bank depends on still need to be operational, data must not be lost, the connection must be secure.

So, the process of conducting the migration depends however on the organization's starting point, so what their infrastructure looks like currently and what exactly they want to migrate. And whether they have legacy systems they use, their cloud maturity, their expertise regarding cloud, their requirements regarding infrastructure and services and their budget. Therefore, the outcome of how the cloud migration is conducted depends on this.
Every major cloud provider has a process to transfer data, applications, or an entire infrastructure step-by-step.

One of them is setting up a connection where a server can be transferred, an application, front-end and back-end systems, a data warehouse, and infrastructure. Generally, they have specific migration tools they use depending on the infrastructure you as a client work with.
Depends as well on what is trying to be created, they might only need a new space to store their public data for a cheap price. Or they require a private cloud environment with separate storage space not shared with other clients where the excess capacity is exclusive for them for security and data sensitivity/privacy governance reasons.

Generally, the cloud provider is entrusted with gaining access to the data by transferring the data and applications of the client to the servers and data centers of the cloud provider. This process is reviewed by the compliance office and security office teams of a bank by reviewing the providers previous experience and frameworks, SLAs, and certifications through an assessment on security, risks, cloud infrastructure, contract agreements, performance, testing and alignment with the current infrastructure, legal requirements, and organizational banking policies.

Question	Code	Count	Contributors
RQ1 – SRQ4	Conducting a requirements analysis		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Migration type		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Migration methodology		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Current		Retail banker, cloud expert, IT business consultant,

	infrastructure analysis		cloud consultant, privacy consultant
RQ1 – SRQ4	Moving front-end applications before back end and legacy		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Discuss the cloud provider being entrusted with all data access	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Reviewing the cloud provider's certifications	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ4	Avoiding chain risk from outsourced service selection	2	Retail banker, cloud expert, IT business consultant
RQ1 – SRQ4	Reviewing organizational policy/ banking policy	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

5. What cloud applications are used in the organization?

Interview data SRQ5: There are quite a lot of categories of applications based on the different departments of an organization. Firstly, there is the organization type, in this case a retail bank or IT consulting firm working with retail banks. Secondly, the departments determine the needs based on the services provided and processes maintained. Thirdly, the actual applications such as Accounting, finance, CRM, documentation, administration systems. Examples are Salesforce, Excel, Microsoft CRM Dynamics, Oracle, SAP etc.

Question	Code	Count	Contributors
RQ1 – SRQ5	CRM	2	Cloud expert, retail banker, cloud consultant
RQ1 – SRQ5	Accounting	1	Cloud expert, retail banker
RQ1 – SRQ5	Finance systems	1	Cloud expert, retail banker
RQ1 – SRQ5	ERP systems	1	Cloud expert, retail banker
RQ1 – SRQ5	Salesforce	1	Cloud expert, retail banker

6. What cloud infrastructure is being used?

Interview data SRQ6: This may be a network infrastructure that is built on-premises, partly uses cloud or is fully using the cloud. It depends on the organization.

Question	Code	Count	Contributors
RQ1 – SRQ6	on-premises or cloud	1	Cloud expert, retail banker
RQ1 – SRQ6	a combination	1	Cloud expert, retail banker
RQ1 – SRQ6	network infrastructure	2	Cloud expert, retail banker, cloud consultant

7. What cloud deployment model is being used?

Interview data SRQ7: This fully depends on the infrastructure used by the organization, and this is classified information. Many of them use on-premises for personal data, or private cloud. And for non-sensitive data the public cloud is utilized.

Question	Code	Count	Contributors
RQ1 – SRQ7	Varies per organization	2	IT business consultant, retail banker, cloud expert

8. What type of cloud migration is conducted (data, applications, infrastructure)?

Interview data SRQ8: This fully depends on the infrastructure used by the organization, and this is classified information.

Question	Code	Count	Contributors
RQ1 – SRQ8	Varies per organization	2	IT business consultant, retail banker, cloud expert

9. What is the cloud strategy? (multi-cloud etc.)

Interview data SRQ9: A cloud strategy is a plan that consists of the requirements for the cloud migration, the objectives that the migration ought to achieve and the most important aspects of the plan that ought to be specified for the successful transition to cloud technology such as the cloud deployment model, cloud providers, what ought to be migrated, how it ought to be migrated, under which circumstances the migration ought to be conducted, the current infrastructure, the desired infrastructure etc. Interviewees found it challenging to define cloud strategies because organizations do not refer to their cloud migration plans as cloud strategies often, also, every organization has very different needs and starting points.
A retail bank that wants to start integrating AI services will have different cloud service needs than the requirements of an organization that would like to scale their infrastructure to accompany the growth of customers using their online banking services on the website and phone application. Therefore, both organizations, with different needs, require very different plans and every cloud provider uses somewhat different methods and tools.

However, interviewees did mention the following cloud strategies:

- Multi-cloud with choosing different cloud providers in case one cannot deliver/has system failures or to have more choice in services,
- Maintaining mostly on-premises,
- Depends much on the current infrastructure,
- A mixture of on-premises and cloud,
- A private cloud environment,
- A customized cloud solution based on choosing standard deployment and service model and customizing with choosing services while specifying exactly what ought to be migrated.

Question	Code	Count	Contributors
RQ1 – SRQ9	Multi-cloud with choosing different cloud providers	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ9	Maintaining	3	Retail banker, cloud expert, IT business consultant,

	mostly on-premises		cloud consultant, privacy consultant
RQ1 – SRQ9	Depends much on the current infrastructure	8	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ9	A mixture of on-premises and cloud,	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ9	A private cloud environment	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ1 – SRQ9	A customized cloud solution	2	IT business consultant, retail banker, cloud expert
RQ1 – SRQ9	Depends on the rules from the: DNB / central banks	2	IT business consultant, retail banker, cloud expert

10. Under what regulation are cloud migrations conducted?

Interview data SRQ10:

- The DNB regulation/central banks/ECB
- The internal banking policy regulations
- The GDPR regulations

To ensure this, there are:

- Certifications, testing rounds and assessments for privacy, risk, security on the cloud provider(s)
- External parties auditing the cloud providers
- Internal and external audits on the bank

This is done through:

- Risk, privacy, security, cloud infrastructure assessments
- Data inventory administration
- Testing plan
- Banking policy

Question	Code	Count	Contributors
RQ1 – SRQ10	Risk, privacy, security, cloud infrastructure assessments	4	IT business consultant, retail banker, cloud expert
RQ1 – SRQ10	The internal banking policy regulations	4	IT business consultant, retail banker, cloud expert
RQ1 – SRQ10	Testing plan	2	IT business consultant, retail banker, cloud expert, cloud consultant
RQ1 – SRQ10	The DNB regulation/central banks/ECB	5	IT business consultant, retail banker, cloud expert
RQ1 – SRQ10	Internal and external audits on the bank	3	IT business consultant, retail banker, cloud expert

Research question 2: Coded results overview

1. How does your organization manage GDPR compliance when migrating data to the cloud?

The organizations tend to make a data inventory and a data privacy register using GDPR tooling to register where data is stored and register which data is sensitive/private. For this there are banking policies internally and external policies from the DNB. Which are regulated with a report given towards the DNB in the DNB portal and realized through data management processes. Examples of cloud services are Microsoft Financial Services Cloud and examples of providers are Azure Cloud from Microsoft or Microsoft CRM Dynamics.

To enable the execution of the migration process in a GDPR compliant manner. The process workflows help to facilitate the processes regarding data management and transitioning data to a new cloud environment, whilst doing a round of data anonymization. The process workflow overviews allow the risk assessments to be done and the migration process to be done whilst considering risks such as data falling in the wrong hands, data leaks, inability to follow the retention policy, inability to delete data.

This can be done through identity access management, data anonymization, data inventory administration, GDPR tooling and data privacy assessments, verifying cloud certifications, secure data migration environments, privacy by design and reporting to the DNB.

Question	Code	Count	Contributors
RQ2 – SQ1	data privacy register	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	risk assessments	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	report to DNB	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	secure data migration environments	2	Retail banker, cloud expert, IT business consultant
RQ2 – SQ1	Microsoft Financial Services Cloud.	1	Retail banker, IT business consultant
RQ2 – SQ1	Azure Cloud.	1	Retail banker, IT business consultant
RQ2 – SQ1	data management processes	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	migration process	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	process workflows	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	data anonymization	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	CRM (Microsoft Dynamics	2	Retail banker, cloud expert, IT business consultant
RQ2 – SQ1	data privacy register	4	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	privacy by design	3	Retail banker, cloud expert, IT business consultant
RQ2 – SQ1	risk management, risk manager,	3	Retail banker, cloud expert, IT business consultant

RQ2 – SQ1	organizational perspective	1	Retail banker, IT business consultant
RQ2 – SQ1	retention policy, data removal per request	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	identity access management, IAM	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	data leaks, data leaks procedures	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ1	cloud provider certifications	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

2. Is there a procedure to manage GDPR compliance with cloud data?

There are again several procedures:

- Doing an in-depth requirements analysis before making decisions,
- Doing data privacy assessments,
    - Which includes making sure that the GDPR regulations are followed,
- Sensitive data is protected,
- Identity access management,
- DPA data processing agreement,
- DNB assessment
- Data location is in EU
- Reviewing the SLA agreement and implementing non-competitiveness and conflict of interest in there, so that the cloud provider is trustworthy enough to share sensitive data with,
- Testing the environment,
- Analyzing the current, infrastructure and customizing the deployment, service models and data warehouses,
- And review the former experience and certifications of the cloud provider to ensure GPDR and security requirements being followed.

There are some other procedures that are relevant to manage GDPR risks as well:

- Making requirements,
- Creating a data inventory,
- Having data privacy processes in place,
- Having data privacy banking policy in place,
- Making a service level agreement,
- Identifying sensitive data,
- Adding and logging data into a GDPR compliance application,
- Setting up a DPA, cloud risk, data privacy, data management, security assessment for the cloud infrastructure of the provider and the connection with the third part,
- Testing the environment,
- And having a compliance office, CISO and DPO (data privacy officer).

The procedures depend on the following factors:

- GDPR policy,
- GDPR tooling available,

- DNB/Central banking policy,
- Cloud provider chosen,
- SLA agreement for migration,
- Current infrastructure and cloud maturity and compatibility,
- Certifications of provider and client,
- Process for procurement of cloud services,
- Requirements and needs.

Question	Code	Count	Contributors
RQ2 – SQ2	data privacy assessment, data privacy register procedures	4	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ2	Cloud related risks, cloud risk assessments	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ2	data location review	2	
RQ2 – SQ2	DNB assessment, DNB/central banks, report to DNB	12	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ2	GDPR tooling reviews	1	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ2	SLA agreement review	2	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ2	DPA review	1	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ2	Compliance (8), compliance team (6)	14	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ2	Testing the environment, pen test procedure	9	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ2	Current infrastructure and cloud maturity and compatibility review	2	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ2	Certifications of provider and client, cloud provider certification review	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ2	Requirement's analysis, non-functional requirements, BIO requirements, legal requirements analysis	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

3. Are there risks associated with not meeting the GDPR compliance requirements with the cloud migration?

There can be several risks occurring:

- Failing the DNB assessment,
- Not following the GPDR regulations,
- Being unaware of your data inventory,
- Being irresponsible with customer data/sensitive data,

- And having a weak security infrastructure.

Can cause:

- Data leaks,
- Reputation damage,
- Hacking/ having a hacked infrastructure,
- Fines from the EU, could be millions of euros, 4% of annual income,
- Data falling in the wrong hands internally and externally,
- Being fined 4% of annual income,
- Reputation damage, for clients, partners, associates,
- Legal issues, lawsuits from stakeholders,
- Clients, partners, customers being socially, financially, psychologically, damaged due to their data being leaked to the public, which includes sensitive data,
- the data being stored with competitors and falling into,
- the cloud service provider failing to deliver which shuts down the business,
- legacy systems not being able to be migrated,
- And latency because of legacy systems being incompatible with transferring data to a cloud environment.

Making big mistakes such as data leaks or failing DNB assessments continually can lead to losing the banking license and the bank ceasing to exist.

Question	Code	Count	Contributors
RQ2 – SQ3	Risk: failing audits	3	Retail banker, data scientist, IT business consultant, privacy consultant
RQ2 – SQ3	Risk: failing DNB assessment	4	retail banker, data scientist, privacy consultant, IT business consultant
RQ2 – SQ3	Risk: data leaks	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ3	Risk: Fines GDPR	10	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ3	Risk: reputation damage	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ3	Risk: cloud security	5	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ3	Solution: security awareness	1	Privacy consultant
RQ2 – SQ3	Risk: security risks/hacking	5	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ3	Risk: Cloud provider security dependency	5	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ3	Risk: data security problems	5	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ3	Risk: penetration security	5	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ3	Risk: legacy problems (ACE100, legacy systems, mainframe)	3	Cloud expert, cloud consultant

4. What are the **biggest** GDPR compliancy risks within a retail bank migrating data to the cloud?

- Financially, the burden of fines from the EU is manageable, medium impact,
- Reputation damage is incredibly damaging, high impact,
- Data leakage, loss of trust, personal damage to clients,
    - Clients, high impact,
    - Bank, high impact,
    - Competitive advantage lost, high impact,
    - Trust from investors/partners lost, high impact,
- Losing the banking license is catastrophic, highest impact, with lower probability,
- Cyber security threats and hacking have a high impact,
- Cloud providers leaking data internally to competition, high impact, lower probability,
- Personal data being sensitive and falling in the wrong hands, being exploited,
- Cloud provider entrusted with all data access; cloud provider could sell the data for profit to buyers.

Risk	Impact (1-5)	Probability (1-50	Score (High/Medium/Low)
1. GDPR fines	4	4	High
2. Data leaks, internally to clients that are competition and externally to the rest of the world	5	4	High
3. Reputation damage	5	3	High
4. Cyber security threats and dependency on cloud security against hacking	5	4	High
5. Losing the banking license	5	2	Medium
6. Cloud provider trusted with data they could sell for profit	4	2	Medium

Question	Code	Count	Contributors
RQ2 – SQ4	Biggest risks: cloud provider entrusted with all data access	4	Cloud consultant, privacy consultant, cloud expert
RQ2 – SQ4	Biggest risks: bad cloud provider certifications	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ4	Biggest risks: chain risk from outsourced service selection	2	Cloud consultant, privacy consultant
RQ2 – SQ4	Biggest risks: GDPR fines	10	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

RQ2 – SQ4	Biggest risks: Data leaks	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ4	Biggest risks: Personal data leaks	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ4	Biggest risks: Reputation damage	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ4	Biggest risks: Losing banking license	1	Data scientist, retail banker

5. What consequences will not meeting GDPR compliance have on the data migrated to the cloud?

Question	Code	Count	Contributors
RQ2 – SQ5	Consequence: Fines GDPR		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ5	Consequence: Reputation damage		Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

6. What consequences will not being GDPR compliant have on the organization?

- Financial consequences would be losing 4% of the annual income to fines and being fines approximately a million euros,
- There can be severe reputation damage,
- Severe impact on the privacy and safety of customers due to their sensitive, personal information leaking.
- The data may be used for hacking, selling data illegally to external parties, or exploiting people.
- The data may be used to gain a competitive advantage over the bank by having insight on their projects, internal operations, and strategy.

Question	Code	Count	Contributors
RQ2 – SQ6	Consequence: Fined 4% annual income	10	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ6	Consequence: Reputation damage	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

7. What departments will be affected the most when not being GDPR compliant?

All departments affected of the entire organization are affected, the entire organization is responsible. Yet, internally, the project team of the cloud migration will be held accountable according to interviewees in most organizations.
The compliance, security, DPO, risk management, IT/Cloud/Privacy/Security consultants, CISO etc. all have advisory roles is many organizations. Therefore, they do not have the directive influence hierarchically in many banks to ensure that project employees will follow their demands/advisory regarding GDPR and security. Therefore, the project employees working on the cloud migration are mostly responsible.

Certain countries differ as well in how they incorporate the GDPR policy, the Netherlands is somewhat lenient and not being 100% compliant with all regulatory policy demands is not immediately causing the DNB or EU to consider giving a fine or a negative consequence. If you have portrayed that most of the policy regulation has been followed up on and your company is making considerable progress the DNB assessment may be positive enough for you to not get any negative consequences at all your progress will still be monitored.

When breaking GDPR rules and guidelines, such as with leaks, hacking etc. then the consequences mentioned in question 4 will be more common, such as reputation damage, fines or even losing your banking license.

Question	Code	Count	Contributors
RQ2 – SQ7	All departments are affected	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ7	The project team of the cloud migration	1	cloud consultant, privacy consultant

8. What procedures are in place to make a cloud migration GDPR compliant?

The procedures include the data privacy assessment, cloud risk assessments but in general most migration procedures are not inherently different for the financial sector on a technical level. Mainly, the regulation is different, and the fact that there is more personal data involved.

Hereby, it is important to ensure that the following regulatory requirements and factors are considered:

- Certifications
    - Security
    - Privacy
    - Cloud
- Regional regulations
    - Local national banking policies
    - DNB/Central banks/ European Central Bank
    - EU
- Policies
    - Banking policies
    - GDPR
- Processes
    - Requirement analysis
    - SLA agreement
    - Risk assessments
    - Compliance assessments
    - Contract management
    - Security assessments
        - Penetration testing
        - Certifications
        - Testing environment with non-critical data
- Workflows
- Infrastructure compatibility

Question	Code	Count	Contributors
RQ2 – SQ8	Cloud risk assessments	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ8	Data privacy assessment	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ8	Data privacy agreement	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ8	standard GDPR policy	3	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ8	No difference between financial and non-financial migrations	2	Retail banker, cloud expert, IT business consultant,

9. What data can be considered sensitive?

All data retraceable to a natural person. Therefore, these sensitive parts of the data must be protected. Examples include salary, name, address, phone number, identification number etc.

Question	Code	Count	Contributors
RQ2 – SQ9	Personal data	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ9	Data anonymization	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

10. What departments manage these GDPR risks?

The entire organization is responsible for ensuring the prevention or mitigation of GDPR risks in RQ2-SRQ3 and RQ-SRQ4 and ensuring GDPR policy is followed. Yet, there are departments that are involved and affected more due to their roles:

- Risk management,
- Compliance team,
- Cyber security department,
- DPO (Data Privacy Officer),
- CISO (Chief Information Security Officer),
- Consultants (external and internal),
- Third party cloud provider,
- DNB auditors,
- Government/Tax department.

Question	Code	Count	Contributors
RQ2 – SQ10	Department: DNB auditors / DNB assessment	4	Retail banker, cloud expert, IT business consultant, cloud consultant
RQ2 – SQ10	Department: Compliance/ compliance team	14	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ10	Department: Data security department	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ10	Department: DPO / Data Privacy Officer	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

RQ2 – SQ10	Department: CISO	3	Retail banker, IT business consultant, privacy consultant
RQ2 – SQ10	Department: Risk management	2	Retail banker, IT business consultant
RQ2 – SQ10	Department: External / Internal Consultants	1	Retail banker, IT business consultant
RQ2 – SQ10	Department: Third party cloud provider	1	Retail banker, IT business consultant
RQ2 – SQ10	Department: Data management processing	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ10	Retention policy data leaks	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ10	Retention policy: keep data for taxes 7 years	1	Retail banker, IT business consultant
RQ2 – SQ10	Production: testing the data/ environment	2	Privacy consultant, cloud expert

11. How is managing GDPR risks differently in a retail bank compared to non-financial organizations?

General differences:

- No technical difference between financial and non-financial migrations,
- Banking policies and DNB policies,
- More financial sensitive information,
- Competition challenges with other banks make leaking and access that a cloud provider has and entrusting them a bigger risk,
- Compliance needs to be managed more heavily based on more policies such as the DNB,
- Dependency on the current infrastructure mainly.

Regulatory differences:

- Managing banking policies
- managing EU policies, laws, regulations
- Managing GDPR policy

Process differences:

- A retail bank is managing funds, clients, and resources,
- Financial, sensitive data,
- Dependent on reputation,
- Complex IT infrastructure,
- Uses a lot of legacy systems/unless it is a digital bank,
- Managing heavy competitors,
- Managing pressure to innovate,
- Managing pressure to adhere to changing, increasing demands from customers on infrastructure and banking services,
- Managing a banking culture, not always very agile, IT driven, somewhat traditional.

Question	Code	Count	Contributors
RQ2 – SQ11	No difference between financial and non-financial migrations	6	Retail banker, data scientist
RQ2 – SQ11	Compliance	14	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ11	Current infrastructure situation/dependency on current infrastructure	1	

12. How can GDPR risks be prevented when migrating cloud data?

According to interviewees, the prevention of the GDPR risks can be achieved by:

- Choosing the right cloud provider,
- Cloud assessments & security assessments: ISO27000 and other frameworks and certifications such as SOC2,
- Data inventory administration,
- Using GDPR tooling,
- Having a data privacy officer,
- Data privacy agreements,
- And the retention policy being followed,
- Consulting (external),
- Security certifications,
- Security awareness on for example human errors, security leakages
- GDPR tooling
- Service level agreement – competition protection, safety data sold,
- Data masking and anonymization on both parties
    - If there is a leak, the data is coded and unrecognizable, impact is prevented
    - Companies are struggling with the procedure of masking big data that they store
    - AI automated data masking

Question	Code	Count	Contributors
RQ2 – SQ12	choosing cloud providers	2	cloud expert, IT business consultant
RQ2 – SQ12	Prevention from managing risks	2	cloud expert, IT business consultant
RQ2 – SQ12	measures for risk	2	cloud expert, IT business consultant
RQ2 – SQ12	ISO27000	3	cloud expert, IT business consultant
RQ2 – SQ12	certification SOC2	1	Privacy consultant
RQ2 – SQ12	cloud security	4	cloud expert, IT business consultant, cloud consultant
RQ2 – SQ12	cloud assessments	3	cloud expert, IT business consultant, cloud consultant
RQ2 – SQ12	Data Privacy Officer	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

RQ2 – SQ12	data leaks	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ12	retention policy	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ12	data anonymization	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ12	data inventory administration	8	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

13. How can GDPR risks be analyzed and mitigated?

Firstly, the risks ought to be categorized and see which departments take responsibility for which risks. Security risks are managed by the CISO, data privacy risks by the DPO (data privacy officer) with a DPA (data privacy agreement). Next to that, the legal team ensures legal risks are analyzed and mitigated in collaboration with compliance.
The (personal) data needs to be:

- Administrated
- Scanned for personal data in a data inventory
- Managed by data management processes
- According to policies such as a data privacy agreement, privacy by design to
- Migrated to a test environment before migrating

The cloud migration process and cloud provider need to be:

- Assessed with a:
    - Security assessment,
    - Cloud assessment,
    - Privacy assessment,
    - Review of certifications,
    - Review of previous cases/projects,
    - Multiple stability tests, Penetration tests, etc.
- Held accountable:
    - Data privacy agreement,
    - Service level agreement,
    - Contract management,
        - Preventing competitors gaining access to sensitive information,
        - Prevent data leaks,
        - Ensure secure migration and cloud environment.

Innovative ideas:
Using AI / Machine learning – Solving the bigger causes of the problems and risks and innovative solutions to manage risks

- To quickly do a cloud assessment,
- To do security assessment automated,
- To do an automated risk assessment,
- To do an automated data warehouse assessment for searching personal data,
- To do an SLA agreement assessment.

Question	Code	Count	Contributors
RQ2 – SQ13	Assessments (Security, Cloud, Privacy, Certificates, experience, stability, penetration)	2	cloud expert, IT business consultant
RQ2 – SQ13	Conduct latest penetration tests	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	Appoint Data Privacy Officer	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	Organizational policy/ banking policy	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	Data privacy agreement, data privacy assessment, privacy by design	16	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	personal information/ personal sensitive data policy	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	data leaks prevention plan	13	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ13	cloud assessments, cloud provider certifications, cloud provider security, Cloud related risks	17	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant

14) How can GDPR risks be avoided, regarding their impact?

The management of GDPR compliance when migrating data is related to several factors. GDPR compliance may be defined as being compliant with the majority if not all aspects of GDPR policy in the EU to ensure the safety and privacy of sensitive personal data of banking consumers.

Avoiding the impact of the risk relates to ensuring that the impact or probability of the risk occurring will reduce by the usage of specific procedures. Interviewees advised having a review on the cloud provider agreements, creating more risk awareness in the company on security risks, not using sensitive data in the cloud unless there is a private cloud environment, testing the security, tackling weaknesses in the policies and process workflows, and having compliance assessments accompanied with a GDPR tool. Also, having external consultants give advice to a retail bank allows for an objective outsiders' perspective. Lastly, having prepared procedures for data leaks and ensuring data anonymization. Whilst also having requirements before making decisions on cloud implementation and preventing reverse engineering. This can be done through for example involving key stakeholders such as the data compliance officer to ensure a clear understanding of requirements.

There are several valuable steps to consider. Risk management is one. Security management. Compliance management. Banking policy. Assessing the processes for approving a cloud migration. Doing cloud maturity assessments. Data inventory assessments.

Question	Code	Count	Contributors
RQ2 – SQ14	Method: Data inventory administration	8	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: Cloud provider agreements	2	Cloud expert, IT business consultant, cloud consultant
RQ2 – SQ14	Method: Risk awareness	2	Cloud expert, IT business consultant, cloud consultant
RQ2 – SQ14	Method: Less data the better	3	Cloud expert, IT business consultant, cloud consultant
RQ2 – SQ14	Method: Response time review	1	Cloud expert, IT business consultant
RQ2 – SQ14	Method: Penetration test	1	Cloud consultant, privacy consultant
RQ2 – SQ14	Method: Policy weaknesses	2	Cloud expert, IT business consultant
RQ2 – SQ14	Process weaknesses review	1	IT business consultant
RQ2 – SQ14	Method: Security risks assessments	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: Standard GDPR policy incorporation	3	Cloud expert, IT business consultant, privacy consultant
RQ2 – SQ14	Method: Organizational policy/ banking policy update	7	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: GDPR Tool for administration of personal data, etc.	2	Cloud expert, IT business consultant
RQ2 – SQ14	Method: Compliance assessments	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: Process workflows administration	5	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: Consulting advisory (externally)	2	Cloud expert, IT business consultant
RQ2 – SQ14	Method: Data compliance manager	4	Cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: “BIO Baseline Overheid “(minimal cloud migration requirements Dutch government)	1	Privacy consultant
RQ2 – SQ14	Method: Data leaks procedures	1	Data scientist, retail banker
RQ2 – SQ14	Method: Prevention from managing risks	2	Cloud expert, IT business consultant
RQ2 – SQ14	Method: Requirement’s analysis	10	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy consultant
RQ2 – SQ14	Method: Data anonymization	6	Retail banker, cloud expert, IT business consultant, cloud consultant, privacy

			consultant
RQ2 – SQ14	Method: Avoid sensitive data in cloud	2	Cloud expert, IT business consultant
RQ2 – SQ14	Method: Reverse engineering prevention	2	Privacy consultant, cloud expert
RQ2 – SQ14	Method: Private cloud for data safety	4	Cloud expert, cloud consultants, privacy consultant

Appendix C: Results interview round 2

Research question 3: Coded results overview

RQ3: What are the risk management strategies in response to the GDPR compliancy risks?

Risk	Strategy	Code	Count	Contributors
GDPR fines	Acceptance	Cash reserves	1	Cloud & Banking Executive Solutions Engineer
	Acceptance	Possibly too costly, timely or complicated to implement policy changes	1	Cloud & Banking Executive Solutions Engineer
	Acceptance	Immediately implement the solution and learn from it	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Acceptance	Deploy people, everything done to prevent	1	IT Project Consultant/Manager in retail banking
	Mitigation	Standard GDPR procedures, use GDPR software and Security protocols	1	Data & BI Engineer/Consultant, retail banker
	Mitigation	Data protection request (How you change systems, working practices etc.)	1	Cloud & Banking Executive Solutions Engineer
	Mitigation	Banks always want to follow the rules, yet Calculated risk is taken/accepted	1	IT Project Consultant/Manager in retail banking
	Mitigation	Privacy impact assessment	1	IT Project Consultant/Manager in retail banking
	Shared/ Transference	Insurance for professional errors	1	Data & BI Engineer/Consultant in retail banking
	Shared/ Transference	Knowing the data controllers and processors within and outside the organization and ensuring they are GDPR compliant.	1	Cloud & Banking Executive Solutions Engineer
	Avoidance	Delete all their customer data, start again from scratch	1	Cloud expert, retail banker
	Avoidance	Changing processes	1	Cloud expert, retail banker
	Avoidance	Right to delete, insight into data processing, users own their own data as much as possible	1	Cloud Professional in Insurance/financial services
	Avoidance	News influences their reputation. Customers are therefore afraid.	1	Data Analytics Consultant in IT consulting

Risk	Strategy	Code	Count	Contributors
Data leaks	Acceptance	Leaks to the outside world/public is not acceptable and the impact is too great. Internal leaks are still acceptable	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Acceptance	Non-sensitive/non-personal data leak has less	2	Privacy, Cyber

		of an impact. Depends on what kind of data it is. Some is sensitive / irrelevant data		Security & Cloud Consultant in IT consulting, Cloud Professional in Insurance/financial services
	Acceptance	Name and surname and age is not a disaster, but credit card details on the street then it is completely over.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Mitigation	Minimize human errors	1	Data & BI Engineer/Consultant in retail banking
	Mitigation	Security matrix and roles are defined, limit permissions to prevent data leaks	1	Data & BI Engineer/Consultant in retail banking
	Mitigation	Training staff, ensuring security policies and procedures. Regarding system usage, authentication security policies and procedures	1	Cloud & Banking Executive Solutions Engineer
	Mitigation	Restrict data and systems access to data, physically & technologically.	1	Cloud & Banking Executive Solutions Engineer
	Mitigation	Certificates – ISO 270001, SOC 2/3, servers	1	IT Project Consultant/Manager in retail banking
	Mitigation	Data storage within EU	1	IT Project Consultant/Manager in retail banking
	Mitigation	Party trust with all certificates, SLA, testing your systems, testing your controls	1	IT Project Consultant/Manager in retail banking, IT Department Manager in retail banking
	Mitigation	Double verification, identifiers and passes. 3 step verifications = Your card, identifier, and your text message.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting,
	Mitigation	Train your employees, so employees are aware of the risks. Have enough compulsory courses.	1	Cloud Professional in Insurance/financial services
	Shared/ Transference	-		
	Avoidance	Outsource security procedures to a third party specialized in cyber security.	1	Data & BI Engineer/Consultant in retail banking
	Avoidance	Identity access management for vendors, third parties etc., reviewing who has access to data, systems, datacenters, at what time.	1	Cloud & Banking Executive Solutions Engineer
	Avoidance	Using the minimum amount of data	1	IT Project Consultant/Manager in retail banking
	Avoidance	Party trust with all certificates. What if, help to prevent, SLA.	1	IT Department Manager in retail banking
	Avoidance	Your OTA and not your OTAP in the cloud.	1	IT Department Manager in retail

		Great time to anonymize.		banking
	Avoidance	Cannot be prevented, it can always happen	1	Privacy, Cyber Security & Cloud Consultant in IT consulting

Risk	**Strategy**	**Code**	**Count**	**Contributors**
Reputation & customer trust	Acceptance	Showcase open and honest communication first and show accountability, Practice the PR strategy, Security	1	IT Department Manager in retail banking
	Acceptance	Can't be accepted, many organizations change their name.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Mitigation	Limit with screenings and background checks	1	Data & BI Engineer/Consultant in retail banking
	Mitigation	Disruption to services and anything customer facing	1	Cloud & Banking Executive Solutions Engineer
	Mitigation	Inform customers before it happens. In the news. Have a media relations strategy.	1	Cloud Professional in Insurance/financial services
	Shared/ Transference	-		
	Avoidance	Security procedures and measures in advance	1	Data & BI Engineer/Consultant in retail banking
	Avoidance	Corruption and accepting gifts and security vulnerabilities	1	Data & BI Engineer/Consultant in retail banking
	Avoidance	Customer service or data privacy failures	1	Cloud & Banking Executive Solutions Engineer
	Avoidance	Assessing suppliers	1	IT Project Consultant/Manager in retail banking
	Avoidance	Checks on the reputation and certifications of the supplier/vendor	1	IT Project Consultant/Manager in retail banking
	Avoidance	Identity Access Management	1	IT Project Consultant/Manager in retail banking
	Avoidance	Severe damage to customers to the point that the whole country is involved. Then you're already losing customer trust.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Avoidance	Mainly employee awareness and training	1	Data Analytics Consultant in IT consulting
	Avoidance	Never 100% watertight, but if you have done everything you can. So, then it's not the company's fault. The central banks judgement will be less harsh. The degree of reputational	1	Data Analytics Consultant in IT consulting

		damage is more limited since you showcased all procedures being done well with the DNB or in a lawsuit.		

Risk	Strategy	Code	Count	Contributors
Cyber security	Acceptance	Limited level of acceptance due to insurance policy protection	1	Cloud & Banking Executive Solutions Engineer
	Acceptance	On-premises backups	1	IT Department Manager in retail banking
	Mitigation	Always up to date with the National Cyber security center. All adjustments to be made asap, you can't see a threat coming, it happens, and you learn from it.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Mitigation	Internal penetration test to be done, Check whether you are doing everything according to rules, audit	1	Cloud Professional in Insurance/financial services
	Shared/ Transference	Look at expert companies. Share the responsibility with these types of companies. For example, cyber security companies outsourcing	1	Data Analytics Consultant in IT consulting
	Avoidance	Do not share personal data. Not even in the cloud.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Avoidance	Sensitive data must be on its own hard disk and data center	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Avoidance	Only use cloud with non-critical documents (Diaries, minutes, policy, organization charts)	1	Privacy, Cyber Security & Cloud Consultant in IT consulting

Risk	Strategy	Code	Count	Contributors
Losing the banking license	Acceptance	-		
	Mitigation	-		
	Shared/ Transference	-		
	Avoidance	Prevent, insure, invest heavily, do everything possible.	1	Data & BI Engineer/Consultant in retail banking
	Avoidance	Not acceptable, in any circumstances, all other risks being prevented ensure this.	1	Cloud & Banking Executive Solutions Engineer
	Avoidance	Good regulatory reports necessary	1	IT Department Manager in retail

				banking
	Avoidance	Conduct a data safety assessment for the cloud environment	1	IT Department Manager in retail banking
	Avoidance	Trust in the organization through audits, assessments, tests, that is trust that you can demonstrate	1	IT Department Manager in retail banking
	Avoidance	Yearly penetration test, recovery test, data breach test	1	IT Department Manager in retail banking
	Avoidance	Data storage location management	1	IT Department Manager in retail banking
	Avoidance	Vendor management, guarantees, service management, bonus management	1	IT Department Manager in retail banking
	Avoidance	Standard practices, being certified, regular check-ups	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Avoidance	Security team that monitors everything daily, otherwise it leaves vulnerabilities, and everything can then be hacked or is opened to be exploited in other ways.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Avoidance	Give employee awareness and prevention workshops, training, not clicking on certain links etc. to prevent leaks/hacks		

Risk	**Strategy**	**Code**	**Count**	**Contributors**
Cloud provider selling data	Acceptance	With some data it is acceptable if it is communicated by the cloud provider. Impact is limited if it is stated in the conditions.	1	Privacy, Cyber Security & Cloud Consultant in IT consulting
	Acceptance	Depends on which service/website it is, for example Google uses it with Salesforce for google search optimization. That's acceptable. But personal data is not possible.	1	Cloud Professional in Insurance/financial services
	Mitigation	Perform an assessment on your cloud provider.	1	Cloud Professional in Insurance/financial services
	Mitigation	Use encryption at this level so that all data stored in the cloud is not accessible to unauthorized individuals and protected. Decrypt it on your on-premises systems and you can store it encrypted in the cloud.	1	Cloud Professional in Insurance/financial services
	Shared/ Transference	-		
	Avoidance	Host everything within the EU	1	Data & BI Engineer/Consultant in retail banking
	Avoidance	Background checks, where are they registered, choose a reliable partner, Trust check. Review the cloud provider, legal point of view etc.	3	Data & BI Engineer/Consultant in retail banking
	Avoidance	Record contractually, Contract management,	5	IT Project

		SLA.		Consultant/Manager in retail banking
	Avoidance	Assess the cloud service package selection	1	Cloud Professional in Insurance/financial services