A Qualitative Study on the Improvement of the Know-Your-Client Procedure Using a Centralized Database.

Name: Mark Derksen

Student number: 2978245

Date: 21/03/2024

Business Administration

University of Twente, Enschede, The Netherlands

Wordcount: 9912

Ethics Approval Number: 231134

Supervisor: Bert Bruggink

Second Supervisor: Henk Kroon

Preface

Dear reader,

Before you is the masters' thesis 'A Qualitative Study on the Improvement of the Know-Your-Client Procedure Using a Centralized Database'. This thesis is written for my graduation of the master's in business administration at the faculty of behavioural management and social sciences of the University of Twente. This thesis was written on behalf of Orange Only, a financial consultancy company in Utrecht.

During my thesis, I received assistance from Alex Buis from Orange Only, Prof. dr. ir. A Bruggink. And Dr. H. Kroon. I would like to thank the supervisors in their support during my research. Additionally, I would like to thank all interviewees who took the time for interviews and providing valuable information.

Mark Derksen

Loenen, March 21, 2024

Abstract

Introduction: Know-your-client, or KYC, is a mandatory customer check for all financial institutions in the Netherlands. This check is focused verifying the identity and information of the customer, to reduce risk of money laundering, fraud, and financing of terrorism. The current KYC procedure used by all financial institutions (FI's) is deemed sub-optimal in several news articles, research papers and employees of the FI's, seeing the need for improvement. This study investigates the reasoning behind the use of the current KYC structure and proposes a shift towards a centrally stored database structure. The research question for this study is as follows: *What are the potential advantages and disadvantages associated with adopting a centrally stored database for KYC data in the Netherlands?*

Method: This study uses grounded theory research methodology, aiming to derive theories from the collected data. Data collection is based on a literature review and semi-structured interviews with KYC specialists. Data is transcribed, coded, and constantly compared.

Results: Four research questions are set up to answer the main research question. These sub-questions highlight four different aspects of using a centrally stored database for KYC, and their up- and downsides. The questions are followed by their respective results. *1: What are the economic advantages and disadvantages?* Found advantages are a decrease in work and resource optimization, disadvantages are the uncertainty of costs and the required upfront investment. *2: What are the quality advantages and disadvantages?* The quality of KYC will rise, due to the ability to compare data. Also, fewer employees ar and/or education of employees is required for similar results. Comparing data could lead to discrepancies between companies, which can be hard to resolve. *3: What are the legal advantages and disadvantages?* Though the legal system can provide a framework for quality requirements, the legislation is mostly a challenge. The GDPR and other laws prohibit sharing data, and it is uncertain if current legislation allows a centralized database for KYC. *4: What are the security advantages and disadvantages?* The security advantages are that a central database is easier to protect than separate companies, though this also means that the database is prone to large-scale cyberattacks. Another disadvantage is the trust in the ownership of the database, and responsibility for quality.

Altogether, results show that while a centrally stored database presents notable advantages in terms of efficiency gains and streamlined processes, addressing challenges related to legislation, trust, costs, and security is imperative for successful implementation.

Implications: The research provides theoretical and practical implications for improving the KYC procedure within the Netherlands. The study challenges the current view on KYC procedures, shedding light on the advantages and disadvantages of centrally stored databases. Theoretical implications include contributing to the field of legal compliance and financial services by showing complexities in the KYC process. Practically, the study offers insights for stakeholders in the financial sector while also contributing to opening a discussion about future possibilities for KYC. This could be to either work and do research on implementing the proposed system, or to reject this system and improve the current structure.

Limitations and Future Research: The research has limitations, including difficulty in engaging the intended target audience for interviews and the evolving nature of the subject matter over time. The research provides insights into the considerations associated with transitioning to and implementing a centralised KYC database in the Netherlands. This leaves the door open for future research into the discussed hurdles. These findings offer a foundation for further exploration and refinement of KYC procedures in the Netherlands and beyond. Future research can dive deeper into the defined limitations of the proposed KYC system.

Table of Contents

Chapter 1 - Introduction

On the first of August 2008, the Act on Prevention of Money Laundering and Financing of Terrorism (AML) came into effect in the Netherlands. This law constitutes a set of measures to prevent the abuse of the financial system. The law consists of several measures, including but not limited to; A risk-oriented approach of a client, a reporting obligation for unusual transactions and client research. Client research is also known as KYC or know your client/customer (DNB, 2024).

KYC is a crucial process employed by financial institutions to verify the identity of their clients and understand their investment knowledge and financial background. This mandatory procedure is designed to comply with legal regulations and prevent financial crimes. KYC consists of three key components: Customer Identification Process (CIP), Customer Due Diligence (CDD), and Ongoing Monitoring or Enhanced Due Diligence (EDD) once a customer's account is established. These components collectively contribute to building a comprehensive understanding of the client's profile (Chen, J. 2023). This study is aimed at the topic of improving the know-your-client procedure. Currently, the KYC structure that is used by financial institutions, is sub-optimal. Sub-optimal is further defined within the literature review. The main focus of this study is to find out why these companies are using this structure instead of an, in theory, more efficient structure. As of now, all financial institutions do their research on new customers separately. This is even though the identity and financial profile of the person/company have already been checked, stored, and monitored by another financial institution. A different way to approach KYC is by creating a centrally stored database, where companies can search for the customer, they intend to do business with. Within this database, the information required for KYC could be stored, saving the company time and energy. Next to this, a database could assist in the standardization of the KYC data and improve quality overall.

The BKR, which stands for Bureau Krediet Registratie or Bureau Credit Registration, is an example of the discussed central database. They keep track of every person and organization that has (had) credit debt. It also keeps track of whether the debt was paid and if this was on time (Stichting BKR, 2022). The data can then be accessed by anyone who needs the information. The data can then be accessed by anyone who requires this information.

The gap this research aims to gain insight into, answering why financial institutions are not using a sub-optimal structure for KYC. Subjects that are discussed are for example, how having information separate could have benefits when looking at privacy, security, and company preferences to do their research. Also, as mentioned, storing data centrally could mean saving time, money, and energy. Finally, this research looks into how financial institutions feel about regulating data collection, addition, and monitoring. This topic is researched in this dissertation, and to fill the research gap the following research question is set up:

What are the potential advantages and disadvantages associated with adopting a centrally stored database for KYC data in the Netherlands?

To answer the research question, four sub-sections are set up that will be answered within this study. These sub-questions assist in answering the main research question.

1: What are the economic advantages and disadvantages?

2: What are the quality advantages and disadvantages?

3: What are the legal advantages and disadvantages?

4: What are the security advantages and disadvantages?

This research is practically relevant in the way that this research provides insight into a possible improvement of operations for the financial services industry. By analysing why financial institutions (FI) are using the current structure this research could come to several different conclusions. (1) The way FI's are currently performing KYC is the most optimal, or (2) a different system seems to also have its upsides and can transform the way that know-your-client is performed today. The information is also relevant to the company guiding the student in his research, where they can act based on the outcome of the research. Another possibility is that a different conclusion arises after analysing the acquired data.

The academic relevance of this study for the student is mostly that of qualitative analysis and asking critical questions about a subject that is not discussed widely. By questioning something that is not researched thoroughly, the student can either gain insight into why the questions is not asked or create value by asking these questions. The student is following a specialization in financial management and KYC is an important part of all financial institutions, which aligns the research goal with the study of the student. The outcome of this study can also lead to new research opportunities. For example, if the outcome of this study shows that a centralized system is better, new research opportunities arise in how to structure such a system. Since the research is larger than a single company, the relevance is of a larger scale and provides value to science as a whole. The research on a larger scale means that the student learns to look further than the company that supports the students. This way of problem-solving and research can support the student after this study, with the knowledge of looking at certain problems strategically and from different angles. Additionally, the student must create interview questions and set up different interviews with several banks to answer the research question.

Chapter 2 - Literature Review

To gain insight into KYC and related research, a literature review is mandatory. Within this review, literature related to the main research question is analysed, reviewed, and summarized. Starting with research on Know Your Client by Prof. Rajput (2013). This research gives an image of what KYC is and the knowledge that comes with it. Knowing your client is the due diligence and bank regulation that financial institutions must perform to identify their clients and ascertain information before doing financial business with them. Chapter 2.1 investigates literature for the current system, Chapter 2.2 into the proposed system's literature and 2.3 delves deeper into the GDPR, or General Data Protection Regulation.

2.1 Current know-your-client system.

KYC processes are employed by companies of all sizes, to ensure their proposed agents', consultants', or distributors' anti-bribery compliance. FI's are increasingly demanding that customers provide detailed anti-corruption due diligence information, to verify their probity and integrity. The adoption of effective KYC standards is an essential part of banks' risk management. Financial institutions with inadequate KYC standards may be subject to significant risk, especially legal and reputational. Good policies protect the integrity of banking by reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing, and other unlawful activities.

KYC was introduced in 2002 by the Bank of India. It directed all banks and financial institutions to follow a policy framework to know their customers before opening an account. KYC aims to prevent money laundering and financial fraud. The primary objective of KYC norms was to ensure that banks and other financial institutions have sufficient information about their customers to establish their identity and assess the risks involved in doing business with them. By implementing these procedures, the Bank of India aimed to enhance the integrity of the financial system, safeguard against illegal activities, and protect both customers and institutions from financial crimes. The steps in KYC are as follows (KYC check, 2022):

1. Identify the client: gather the basic information; name, address, date of birth, trade name, and chamber of commerce (KvK) number.

2. Verify the identity of the client: Because of safety and regulation, one cannot assume all information the client provides is correct. Thus, a check has to be done by checking the ID for a person or an abstract from the Business Register.

3. Establish the Ultimate Beneficial Owners (UBOs): UBOs usually own more than 25% of the stock or have voting rights within the company. The UBO must sign that the statement about the UBO is correct.

4. Create a risk assessment of the client: when all data is collected, the financial institution must assess the risk of a company or person. Assessment is based on client risk, product, transaction, distribution, and geographical factors. Categories often used are low, normal, high, and unacceptable.

5. The final step that is not required by law is the frequent monitoring of the client by doing a periodic review. This is to assess the risk of the company and by reviewing the client again, can change the risk to a lower or higher category dependent on the outcome.

A notable conclusion from The Business Standard is as follows; *"There is no escaping the paperwork while investing in financial products ... filling the know your client documents is a mandatory procedure today"* (Pai, 2013).

The KYC procedure is time-consuming. In the current KYC scenario, each financial institution must individually gain information about a client. (Moyano, 2019). Figure one shows the current inefficiencies with KYC. One customer must apply to three different banks and each bank must do their own research, has their own costs and their own required checks. The current procedure shows the amount of duplicate information within KYC, since banks do not and are not allowed to share this information right now. Resulting in each bank doing their own research, for data that probably already exists.

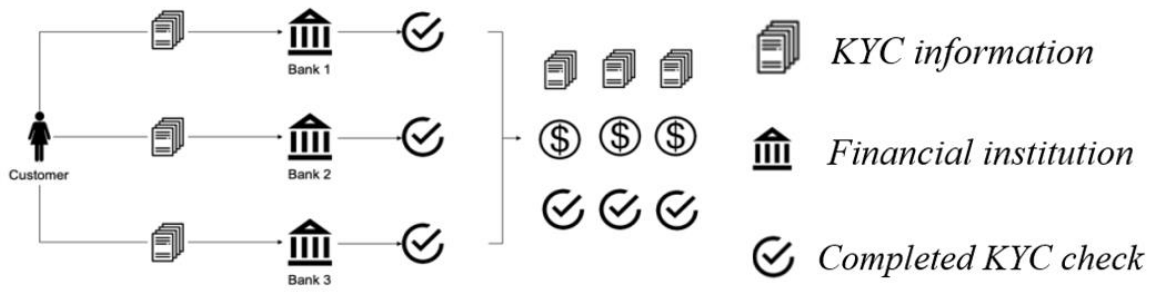

Figure 1: *Current KYC procedure. (Moyano, 2017).*

Next to the fact that the current procedure can be classified as 'inefficient', most customer data is stored within firms, and the computer programs acting are also governed by the (one) company and thus are not tamper-proof. This makes them susceptible to vulnerabilities and attacks (Denson et al., 2019). This gives another reason why the change of the current system is in favour of the customer as well as the financial institutions.

Another sign that the current KYC system is becoming more and more time-consuming and costly, is a statement on the website of one of the largest banks in the Netherlands, Rabobank. From the 1st of January 2023, costs for KYC are partially passed on to customers. The costs lie between 3 to 24 euros per legal form. The reasoning for this, according to Rabobank, is as follows: "The efforts we make have the highest priority. We continuously monitor customers and conduct various investigations. This is becoming increasingly intensive, resulting in increased costs. We currently pass on a small portion of these costs. This way, we can continue to fulfil our gatekeeping function and ensure your safe banking experience" (Rabobank, n.d.). The same goes for ING, another large bank in the Netherlands. Their costs are slightly lower and are implemented from the 1st of September 2022. The reasoning for passing on the costs is similar to Rabobank's' reasoning (ING, n.d.). This is also the case for the smallest of the three largest banks in the Netherlands, ABN Amro. The costs calculated for KYC are similar to those of ING but implemented since the 1st of July 2022 (ABN AMRO, n.d.). An interesting observation is that the medium-sized and smaller banks in the Netherlands (Triodos, AEGON, Achmea Bank, BNG) do not calculate costs for performing KYC to the customers, even though they do work with businesses and offer business accounts. This is a fact that can be considered when setting up the interview questions for the different banks and in establishing the differences between differently sized banks in the Netherlands.

In current events, published by financial news channel Accountantweek, the need for a change in the KYC structure is further defined. The article states that the current laws and regulations for the prevention of money laundering and terrorism are an issue for the *entire* financial sector. ING and ABN AMRO already paid hundreds of millions in fines due to violations of these rules. The financial institutions have already suggested a mutual warning-system, to reduce the time invested and the risk of mistakes. However, with the current laws and structure, this is not possible. This leads to not only

more risk but also frustration for the client. For example, when a client wants to purchase a house, he/she must provide identical information to the bank, the notary as well as the broker (Accountantweek, 2023).

The above-discussed structure and its issues are defined as the sub-optimal KYC system in this research. Sub-optimal is further defined as follows: The implemented framework for KYC does not meet the fully desired standards or requirements for effectively verifying the identities of their customers. It implies that the current KYC practices have limitations, inefficiencies, or shortcomings that hinder the institution financially and operationally by increasing costs and unnecessarily spending time and energy on the upkeep of this system. Concerning the sub-optimal system, a more optimal system would mean that the inefficiencies, limitations, and shortcomings are improved upon by creating less financial or operational hindrance while fulfilling the KYC requirements.

The current KYC procedure has reached a state in which different news sites and branch-specific sites mention the issues arising from the current system. The following information is available on KYC through these sources. The Financial Newspaper (Financieel Dagblad) states that following the money laundering fines for ING and ABN Amro, banks are taking compliance seriously and rapidly expanding their compliance departments.

However, the market for specialists in KYC and CDD is drying up. As a result, other financial institutions including pension funds, fintech companies, insurers, and accounting firms are entering the competition to secure scarce KYC and compliance professionals. These professionals are in high demand and are difficult to find. The scarcity of KYC personnel has led to increased competition among banks and other financial service providers, with fines imposed on ING having a significant impact. Despite efforts to recruit more professionals, banks are still facing backlogs in their compliance departments, and regulators are demanding more each year. The scarcity of these professionals means they can command relatively high starting salaries, which quickly increase with experience. Many individuals in this field start their businesses or switch to competitors for better pay.

Compliance with anti-money laundering and fraud legislation is a relatively new discipline without a specialized higher education program. Large banks often handle training internally, and the main requirements for these positions are analytical skills, logical thinking, and good writing abilities.

Proficiency in Dutch is a must since many clients are Dutch, and analysts need to review Dutch documentation and write reports that can be understood by all stakeholders. The demand for Dutch-speaking professionals is estimated to account for 80% of the job vacancies (Financieel Dagblad, 2021).

An analysis by ‘Proud Experts’ reveals that approximately 15% of the total workforce at the top three banks in the Netherlands is now engaged in Customer Due Diligence (CDD) customer research. Financial institutions are taking their responsibility to screen customers and identify suspicious money flows much more seriously than before, prompted by ING's €775 million settlement.

The costs associated with these extensive checks are being passed on to customers, resulting in higher fees for maintaining business accounts. Banks have seen a 42% increase in costs over the past five years, leading to dissatisfaction among consumers, particularly customers of major banks. The increased fees are necessary to cover the expenses of employing KYC personnel, with up to 20% of bank employees in the Netherlands performing gatekeeping functions. However, despite these efforts, the effectiveness of the process remains minimal, with a significant increase in reported cases but limited actual detection and prosecution. Proud Experts suggests implementing a "fast lane" for low-risk cases to streamline the process and focus on relevant cases, using automation to handle approximately 80% of cases more efficiently. This would allow for more thorough manual checks on high-risk cases while reducing costs and improving effectiveness (InFinance, 2023).

The risk aversion among banks has resulted in a significant increase in the number of customer transactions classified as "unusual." Banks now tend to stretch the definition of unusual to avoid any risk of involvement in suspicious transactions. This risk-averse approach is not efficient, and the system is overwhelmed due to the under-resourced Financial Intelligence Unit (FIU), which is responsible for processing reports of unusual transactions. Customers are now bearing the brunt of the Know Your Customer (KYC) efforts, having to provide excessive amounts of information, and facing the risk of account termination if the provided information is deemed insufficient. To improve the quality of the monitoring of ‘unusual’ transactions, the five largest banks in the Netherlands have set up the TMNL (Transaction Monitoring Netherlands). This institution follows up on the insights into whitewashing and terrorism financing. This cooperation is a step in the right direction following up on the decrease in quality/ efficiency of banks. However, the TMNL is not responsible for gathering information on clients,

only for analysing transactions and patterns. The banks are responsible for the TMNL also suggest that this control in whitewashing is something that should be considered a societal responsibility, for which the government is responsible (Compliance Institute, 2023).

As a result of these rising requirements, shortages in personnel, decrease in quality, and increase in unusual transactions, Rabobank has invested €250 million to increase the monitoring of money laundering and the top management layer of Rabobank will also gain an additional director focusing on the KYC process. Additionally, between the years 2016 and 2021, the amount of KYC employees has risen from 1700 to 4900. According to the regulator, Rabobank is (still) not doing enough to prevent money laundering and has therefore started a 'punitive enforcement process' against the bank. The bank has been told by DNB that it must have its KYC affairs in order by 15 December 2023 at the latest (banken.nl, 2022). These shortages also affect other banks and their customers. In August of 2022, ING announced that they were not opening new accounts due to the amount of work in checking the existing accounts for money laundering. Additionally, the costs of opening an account have risen from €3 per month to €7.50. (banken.nl, 2022).

2.2 Proposed know-your-client system.

The financial sector is currently facing two significant compliance challenges, Customer Due Diligence (CDD) and Know Your Customer (KYC), in line with existing regulations. Major banks, including ING and Rabobank, have been penalized for inadequate anti-money laundering processes, as discussed previously. Globally, banks are striving to improve their approach to customer profiles and transaction monitoring to identify suspicious activities effectively. The traditional method of adding more staff to address these issues is costly and lacks the required quality control (Banken.nl, 2019).

Research by Isherwood (2022) discusses perpetual KYC (pKYC). This research touches on the benefits and challenges of pKYC. One of the benefits that is discussed is that again, less time is consumed when the customer announces to the financial institution that information has changed and what information has changed. Also, an internal system would monitor suspicious transactions, payment screenings, or credit risk analyses, which can alert the financial institution. The challenges that firm face right now are overly complicated KYC processes, limited resources, and difficulty in determining

the frequency of updates. Different studies have been conducted, trying to automate this inefficient process. Most of these studies that were conducted, focused more on exploratory studies than implementing the concept. The article 'How Blockchain Can Automate KYC' by Malhotra et al. (2021), also acknowledges the issues with the current KYC procedure. This is done with a systematic review which involves a plan, and strategy with priori and has the goal to reduce bias.

The application of technology in KYC and CDD has been talked about for some time. At the event 'Augmenting Customer Due Diligence', compliance is presented as an opportunity to streamline KYC and CDD processes and introduce innovations. The presentation by David Hodgson from Dow Jones stressed the importance of intelligently automating KYC and CDD processes. He highlighted the need for organizations to be aware of recent developments in sanction regulations. Integrating external data, using analytical tools, and leveraging technologies like Artificial Intelligence (AI) are essential for maintaining compliance in the increasingly complex data landscape for financial institutions. AI allows the analysis of large data volumes and focuses on detecting abnormal behavior, such as money laundering and fraudulent activities. Rabobank's Nico Strauss highlighted the importance of integrating compliance and risk management with the business, emphasizing that compliance should be an integral part of the business rather than operating in isolation (Banken.nl, 2019).

The implementation of blockchain to improve KYC is a distributed ledger technology by Sinha and Kaul (2018). This technology is a decentralized system that can be used at multiple places to validate the identity of the individual who accesses the database. The distributed ledger has a feature of immutability, which is the key concept to ensure that the data is tamper-proof. Data is stored in a distributed database that replicates data so that there is no single point of failure. The decentralized architecture of the system `ensures there is no dependency on a centralized client-server architecture. The system is cost-efficient since KYC analysis does not have to be done multiple times for a single company.

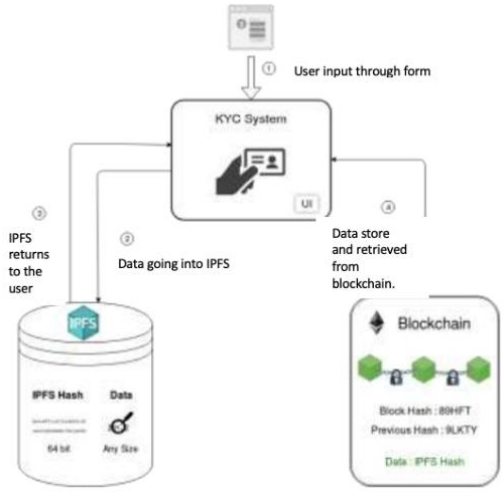

Figure 2: *Architecture Diagram (Sinha, 2018)*

Because the distributed ledger is based on blockchain, data is encrypted. This means that even if it is not based in a decentralized database (so no data replication), there is no harm when the data is compromised. The takeaway from this literature is that this proposed system is the potentially 'more beneficial' system for KYC. Within this research, the pros and cons of this system are compared to those of the current system. N. Sundareswaran et al. discuss that there are multiple solutions based on Distributed Ledger Technology for the issue of KYC verification in concerned organizations. The first approach is to have a decentralized system where each node is having a complete copy of the KYC-verified documents. The second approach suggests that each node has a copy of KYC documents verified and validated by that specific node and requests data from other nodes whenever needed as proposed with experiment and cloud-based validation. The third approach proposed is that of a centralized system with a central point of control to reduce costs even more. All the implementations are suggested to be performed using the Ethereum platform.

This research by Sundareswaran concludes that while there is a very good scope for implementing a KYC verification system using blockchain and DLT (distributed ledger technology), it is still under the development stage and requires extensive implementation (Sundareswaran, N. et al., 2020). So, even though there is not a definitive 'best way' to implement a different system, results show that there are several possible solutions that can improve the current structure.

The proposed structure that is tested within this study, to improve the current structure is based on companies using a centralized database containing all required information for the KYC check. This reduces the duplicate work and data currently existing within KYC.

2.3 Privacy law (GDPR)

KYC is based on personal, private, and sensitive information. The proposed system, and KYC in general, uses a lot of private information. Sharing this information between companies could be a bottleneck in implementing this system. For this reason, the General Data Protection Regulation (GDPR), AVG in Dutch, is summarized in nine points which could apply to this system. European law prohibits sharing this information with everyone and there are many regulations that databases,

companies, and users have to comply with to share any personal information. To prepare for the interviews the main topics of the GDPR are summarized below (wetten.nl, 2018).

To gain insight into the GDPR, a quick summary of the topics that fall under the GDPR is shown below:

1. Scope and Application: The GDPR applies to all data processing that takes place in the EU. The GDPR also applies to organizations outside the EU that offer goods or services to individuals in the EU or monitor their behaviour.

2. Principles of Data Processing: The GDPR establishes principles for the lawful processing of data. These principles include legality, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

3. Legal Basis for Processing: Organizations must have an appropriate legal basis to process personal data. It can be the need to process data for the performance or completion of a contract or legal obligation, the protection of vital interest, consent, performance or exercise of an official authority or public task, or the data controller's legitimate interests.

4. Individual Rights: GDPR gives individuals various rights about their data. These include the right to access and rectify data, to erase it, to restrict processing, to transfer data, to object to processing, to portability of data, to not be subjected to automated decision-making, etc.

5. Consent: GDPR sets higher standards for valid consent. The GDPR requires consent to be given freely, specifically, in a clear and informed manner. The ability to withdraw consent must be easy for individuals.

6. Data Breach notification: Organizations must notify the appropriate supervisory authority and the affected individuals immediately if a personal data breach is likely to threaten rights and freedoms.

7. Data Protection Officer: Certain organizations are required by GDPR to appoint Data Protection Officers to supervise data protection activities.

8. Data Transfers: The GDPR restricts the transfer of personal information to countries outside of the EU which do not provide an adequate level of data protection. It includes mechanisms like Standard Contractual Clauses or Binding Corporate Rules that facilitate legal data transfers.

9. Enforcement and Penalties: Supervisory authorities are empowered to enforce GDPR and impose penalties for non-compliance. The maximum fines are substantial depending on the nature of the violation and its severity.

From this literature review, the following parts are used for the continuation of the research.

1. Current KYC system challenges and inefficiencies: Current KYC is time consuming, expensive, and inefficient according to studies conducted on this subject. The current KYC structure is deemed sub-optimal due to these limitations.
2. Rising costs for KYC compliance: The costs of KYC are passed on to customers. Large Dutch banks like ING, Rabobank and ABN Amro are calculating costs through to the customers.
3. Scarcity of KYC professionals: A shortage of KYC specialists leads to competition among financial institutions. The training of employees is also a costly and time-consuming task.
4. Proposed KYC solution: A centralized database is the proposed solution for more efficient and secure data management.
5. Privacy law: the GDPR poses challenges to the sharing of KYC information between companies, while also keeping information secure from cyber-attacks. These limitations pose a reason for concern among financial institutions and a reason to stay with the current procedure.

The literature review provides guidance in the research and helps shape the framework of this research in chapter 3.3: Conditions of the research. Other information is used to set up the interview questions. The research gap is as follows: the current KYC-structure is deemed sub-optimal, though it is not clear why the Dutch financial institutions have not changed this structure to the proposed KYC system. This is also the gap this research aims to provide the answer to.

Chapter 3 – Methodology

This chapter gives insight into the methods used to acquire valid and accurate information to use in the next chapter. The main research question is answered using the grounded theory method, explained in chapter 3.1. The method of analyzing data is clarified in chapter 3.2, this also includes the literature review. In chapter 3.3 the conditions of this research are described.

3.1 Grounded Theory Research

This research is done based on grounded theory research. This means that this research tries to answer the main question by generating theories grounded in the data collection during the research process. By constantly comparing collected data to each other and already established literature, the result can provide valuable insight into the research question and serve as a basis for future research.

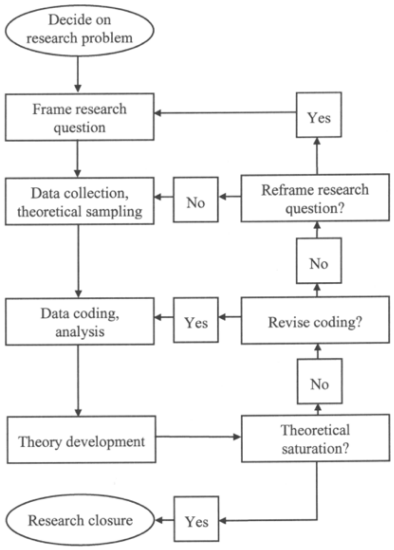

Figure 3: *Grounded theory flowchart (Bitsch, 2005).*

A part of grounded theory research is theoretical saturation. This refers to the point at which enough data is collected that no new concepts or categories are emerging, and the existing data can answer the main research question. Within this research, saturation will most likely be reached when different interviews do not supply vastly different information.

The research uses both literature and interviews to answer the main research question. All studies/papers are gathered from Lexis Nexis, Google Scholar, and Web of Science. To create insight into the relevance of this research, recent news is used and gathered from credible sources. Most of the information required to answer the research question is gathered through semi-structured interviews. The interviews will focus on KYC specialists or experienced employees within the KYC system who can supply adequate information about the above subjects. Though it is of value for this research to interview companies (banks) with many customers- and thus a lot of work in terms of KYC, the larger companies may not want to open up about inefficiencies or opinions about the current system. For this reason, the KYC specialists could potentially provide more insightful information. The interviews will

focus on the topics discussed in the introduction and literature review. These include but are not limited to the current structure's efficiency, safety/privacy concerns, legislation, quality of KYC, companies' trust in centralized data, and the perceived need for change.

To make sure that the data collected is trustworthy, the following set of four standards is used: (1) Truth value, which determines whether the researcher is confident the findings are truthful responses. Truth value is obtained using the strategy of credibility. (2) Applicability refers to the degree to which the findings can be applied to the research question. The strategy of transferability measures applicability. (3) Consistency considers whether the findings will be consistent if the inquiry is replicated with the same participants in a similar context. The strategy of dependability is used to confirm this. (4) Neutrality entails freedom from bias during research. To ensure neutrality the strategy of confirmability is used (Klopper, 2008). These strategies each have different criteria to be complete. These criteria are shown in the table right. The individuals selected to interview are planned to a certain degree, with the possibility of changes dependent on the interview outcome. This is due to the constant comparison, a large part of grounded theory research.

Strategies	**Criteria**
Credibility	Prolonged engagement
	Triangulation
	Peer examination
	Negative case analysis
	Member checking
Transferability	Selection of sources
	Saturation of data
	Thick description
Dependability	*Indirect:*
	Measures of credibility
	Direct:
	Stepwise replication
	Inquiry audit
	Triangulation
Confirmability	Confirmability audit
	Triangulation

3.2 Data analysis

The interviews are transcribed, then different codes are created to analyse the different opinions and reactions of the interviewees. To analyse the data, the codes are matched with the interviews. Since the chosen structure is grounded theory research, the results are constantly compared. Constantly analysing collected data can help identify patterns, categories, and relationships. When the data is sufficient the most prominent codes are worked into a conclusion on why the financial institutions are using a sub-optimal structure. The coding of the transcribed interviews is done in three steps. First, open coding. This means giving labels to statements from the interview that describe the main theme. After all parts are coded, the next step is axial coding. To make the codes comprehensive and understandable,

singular codes are added to a larger theme that describes several singular codes. Finally, the most important categories are combined in selective coding to create an analysis and conclusion. Additionally, the before-mentioned constant comparison plays a role while coding. When new interviews are conducted, codes that were assigned earlier are subject to change in retrospect to create a clearer image (McGhee, 2007).

3.3 Conditions of the research

Establishing effective research requires conditions that limit its scope; several topics require limitations when looking at the optimal KYC system. First, the research examines two KYC systems - the current and proposed centralized database systems. This approach seeks to provide key insights into each system while avoiding excessive research that might obstruct the conclusion. As this study takes a qualitative approach, interviews serve as the main source of data to fill the research gap. The proposed interview setup involves engaging with two large, medium-sized, and small banks based in the Netherlands. This is to account for potential variations in perspectives on KYC between banks depending on size, market capitalization, and balance total. It should be noted that certain banks may decline participation due to a lack of interest in supporting the research, privacy restrictions, or other restraints.

The study includes two months for data collection. The expected range of interviewees ranges from six to ten interviewees depending on the results obtained and availability. Given the number of financial institutions with an obligation to the AML, interviewees should be from different sectors to gain enough of a representative insight in Dutch FI's. Potential interviewees are contacted via phone or email and must work in the KYC branch of their respective companies or possess adequate knowledge about the current KYC structure. This research may be prone to bias by selecting interviewees on availability. Furthermore, due to the qualitative nature of this research, findings may not apply universally across financial institutions or banks. Information accessibility may be hindered by banks opting to keep certain information private, including customer details, KYC process costs, or opinions on related topics. All interviewees are kept anonymously for this study since identity is not of importance.

Chapter 4 – Results

The research analysis involved conducting interviews and transcribing the audio recordings. Using these transcripts, the interviews were first looked through individually where quotes were given a code. Following the individual coding of the interviews, all codes were sorted into one of ten general codes presented in Appendix B. In this appendix, the related quotes are also located. To answer the main research question, *what are the potential advantages and disadvantages associated with the adoption of a centrally stored database for KYC data in the Netherlands?* The four sub-questions are answered first in chapter 4.1 until 4.4, in chapter 4.5 a general conclusion and table of the results are formed.

4.1 The economic advantages and disadvantages

The first sub-question focuses on a centrally stored database's economic advantages and disadvantages. The codes related to the economic advantages and disadvantages are *Efficiency and Time factors* and *Economic Aspects.* The efficiency and time factors are based on several issues the current KYC procedure has. This code refers to the continuous increase in workload, the inefficient way of gaining the required information, and the time inefficiency because of these issues. Economic aspects are related to investment costs, management of the database and return on this investment. The questions set up to gain insight into economic aspects were asked to all participants. The participants unanimously agreed that a centralized database would be beneficial looking at costs. One of the most time-consuming tasks in KYC is determining the UBO, especially in complex business structures. The increase in workload is caused by the difficult structures existing to either hide the ownership of a company or create tax benefits. This is largely diverted by establishing an UBO once and then communicating this with other companies. A cause mentioned in six of the eight interviews is that of duplicate data, currently existing. The interviewees are aware of the fact that the current KYC procedure results in a lot of duplicate data, which is backed by several quotes, for example, *"And every accounting firm does indeed do that, so separately, your focus is mainly the banks, but accountant offices have the same problem and they have to go through the whole procedure of the WWFT for every new customer, just like the*

banks".[1] A centralized way of storing data reduces duplicate work and means that companies can focus more on other tasks important to their business. This is the most discussed improvement when looking at the proposed KYC system compared to the current system. By reducing duplicate data, a direct result is that of less time spent on KYC. Fewer employees are required to do checks and time can be spent elsewhere, while also reducing the need for education of new KYC employees. The investment beforehand is a hurdle discussed in two interviews, but not mentioned by all interviewees. The management costs of a database, and who should pay for this are unclear for the interviewees who felt adequate giving more information about this. The uncertainty of the size of this database and security requirements makes an estimation not accurate. *"I can't make a statement about this; it depends on how this database operates and who is responsible for it".*[2] The responsibility of this database is discussed in sub-question four.

The advantages of a centralized database, when looking at economic aspects are the decrease in duplicate work, resource optimization and long-term benefits in acquiring new customers. Disadvantages are the uncertainty in costs of managing a database, per company and the upfront investment required to establish a database in the first place.

4.2 The data quality advantages and disadvantages

The second question is related to the quality advantages and disadvantages a central database could have on the know your client data. The codes used to define the potential up- and downsides are *Employee Skill and Education* and *Data Quality and Accuracy.* Data quality and accuracy are centred on meeting the specific requirements and goals of each company within the KYC process. This involves obtaining more precise information and conducting thorough investigations of red flags. These considerations are closely tied to the utilization of a centrally stored database, given that each company may have different standards. Employee skills and education are focused on the dependence on employee skills and the need for continuous education. Educating employees to ensure proficiency and

[1] Page 47, Interview 1, Accountancy

[2] Page 66, Interview 5, Accountancy

addressing subjectivity in risk assessment are vital components. Mentioned by six of the eight respondents is the investment in properly educating employees, since KYC data is subjective, the judgement of individual employees must be adequate and correct. A quote from an interview with a bank compliance officer describes this issue: *"I think that is the biggest problem. Many employees have just graduated from school. And many young people have very little experience in the field. And if you then talk about practice and theory, those are two very different things".*[3] This also relates to duplicate work, since all the companies that must follow the AML, have employees who must be educated to understand and analyse a client. A large part of KYC currently is gathering information and understanding the data that is gathered. Educating employees to gather the correct data takes time, while the collection of data is a time-consuming task as-is. A large portion of time spent on the education of employees can be disregarded when a centrally stored database is adopted. Furthermore, the only work that has to be done, if the database contains the data necessary, is the analysis of the data. This would save a lot of education for employees and employees in general. This, in turn, relates to the second code: data quality and accuracy. If a centralized database is set up, the data in the database has to be correct and fulfils the needs of the database's users. A quote that shows the benefit of working together is *"I think centralized data could improve the quality of the data. Just one database for the Netherlands. If you do everything centrally, everyone is aware of everything. You have one way of working and one version of the truth".*[4] This thought process is shared through four of the eight interviews. So, working together could improve the data quality, since multiple registrations are compared and any discrepancies can be investigated further, increasing the overall quality.

Overall advantages for quality of the data are the ability to compare data which increases quality and less employees and/or education of employees required. A disadvantage is the potential discrepancies in the quality of the data between companies.

[3] Page 51, Interview 2, Banking

[4] Page 68, Interview 6, Consultancy

4.3 The legal advantages and disadvantages

The third sub-question focuses on the legal disadvantages and advantages of the proposed system. The legal doubts and limitations are registered using the codes *Compliance Challenges.* Compliance challenges revolve around the legal aspects of adopting a different approach to KYC, particularly in the context of a central database. This is compliance with GDPR and the prohibition of information sharing between companies. The most common response, which was present in all interviews, was about the legal ability to create such a database. With the GDPR, sharing and/or storing private information is strict. The following quote shows this doubt: "*I believe that, under current laws and regulations, a centralized database would not be successful. Critical data used to assess the client cannot/must not be included in this database due to current privacy legislation".*[5] A way to work around the GDPR, not confirmed through knowledge from the interviewees but based on assumptions, is to make businesses voluntarily enter information into the database. Under the GDPR, sharing personal data is generally allowed if the data subject provides explicit and informed consent for the specific purpose of data processing. Note that the consent must meet certain criteria to be considered valid:

- Freely Given: The individual must have a genuine choice and not be forced or pressured into giving consent.
- Specific Purpose: The consent should be specific and tied to a particular purpose for processing. You cannot obtain broad consent for any and all purposes.
- Informed: Individuals must be informed about the purpose of the data processing, the data controller's identity, and any other relevant information.
- Clear Affirmative Action: Consent must be given through a clear affirmative action, such as checking a box or actively providing consent in some way.
- Easily Withdrawn: Individuals should have the right to withdraw their consent at any time, and it should be as easy to withdraw as it was to given.

[5] Page 64, Interview 4, Accountancy

If these conditions are met, sharing personal data with the explicit consent of the data subject is generally permissible. However, organizations must handle personal data responsibly, ensure the security of the data, and comply with other GDPR principles and obligations (Art. 6 & 7 GDPR – Conditions for consent – General Data Protection Regulation, 2018). This also represents the disadvantage of a central database when looking at legislation. The strictness of the GDPR, and perhaps other laws, are significant and require more research to determine whether a database is even legally allowed in the Netherlands. The interviews show that when looking at the proposed system, legal does not have advantages. However, laws and restrictions provide a framework for the quality of data, requirements for security and integrity when working with this data.

4.4 The security advantages and disadvantages

The final question used to answer the main research question is about the security advantages and disadvantages. The codes related to the security and privacy are *Security and Cybersecurity* and *Ownership and Access*. Security and cybersecurity concerns aspects such as safeguarding against cyber threats, controlling added data, and managing trust issues. Ownership and access involve recognizing the customer as the owner of their data, determining appropriate access levels, and establishing trust among different companies. A frequent response were the safety concerns. In five of the eight interviews, this came forward. Because private information is very valuable, a centralized database would be prone to attacks to gain access to this information. Security and cybersecurity are a big concern. As mentioned previously, the government has received double the number of cyber-attacks in the last few years. The attacks were aimed at gaining private information from the government. This means that security is a crucial part of the equation in the implementation of this database. *"I think that's also the condition for a solid construction, you have to be able to guarantee that it's 100% secure because otherwise, people won't do it. So that's a really important condition. That you have to make sure that the integrity of that data is safeguarded".*[6] This means it is imperative that the database is built on the best security systems, perhaps using blockchain to secure data.

[6] Page 69, Interview 6, Consulting

A lesser-mentioned doubt, though mentioned in three interviews, is the trust in data quality by others. This is coded as ownership and access. Since currently all companies do their research and collect their own data, they are certain that everything is correct to their standards. This, however, does not mean that different companies agree with this standard. When data is shared, some data may not be up to par, depending on who gathered the data. This is also related to the responsibility companies have over the data. For example, if a company receives a large fine for using incorrect information, who is responsible if they received the data from the central database? To take away the issue of trust in the data and other companies, a controlling company must oversee the quality of data. Multiple Interviewees stated either one of two possibilities: either a commercial company takes charge, or the government becomes involved. On one hand, a commercial company could be more feasible and actionable than the government. However, the question remains that if businesses feel safe giving their private information to a company that is focused on making money. The government could also fulfil the role of controlling the data. A disadvantage of involving the government is that it is prone to a lot of cyber-attacks. The cyber-attacks on municipalities have doubled over the last few years, with attackers demanding a ransom (Van Ooij, 2022). This might bring more risk due to the limits in budget and time that the government must fulfil this role. The following quote shows the general thought of several interviewees: *"The government does not generally have a profit perspective, and it has a supervisory role to ensure that this is done in the right way. And with a commercial company with shareholders, not being the government or government-related, there will always be an idea of, what do those guys know about me who are up there".* And *"it doesn't even have to be the government, but there has to be a huge amount of supervision from the government. That this integrity is guaranteed".*[7]
A hurdle related to the access and ownership of the database is that of costs since companies with fewer clients can provide less data and can perhaps have to take more data than they provide. Banks have a lot of data, which when looking at other banks might be comparable. SMB companies, however, have a lot less data to add to the database. How companies pay for this database and who adds what data is

[7] Page 86, Interview 8, Finance

something that is not yet defined. However, two respondents came up with the same solution to this problem, which was as follows. *"I would like to look at it from the customer's point of view. In other words, from those companies that always have to provide data to all service providers. I just do it centrally, so I pay to put It there once. And then anyone can get It from there".*[8] This suggestion would lead to the customer paying for the database, for which in return the businesses in the register would no longer have to gather all information to provide to all different AML-obligated companies they want to work with.

4.5 Conclusion

In conclusion, the research findings show up- an downsides related to the adoption of a centrally stored database for Know Your Client data within Dutch companies: the current KYC procedures have issues that can be resolved using a centralized structure, particularly regarding efficiency issues, the demand for skilled personnel, and concerns about data quality and interpretation. While a centrally stored database is recognized as a promising solution to streamline processes, reduce duplicate work, and enhance overall efficiency, the implementation is not without hurdles. Legislation, especially compliance with the GDPR poses a significant challenge. Doubts were expressed regarding the legal feasibility of creating such a database, and potential solutions, such as voluntary data entry with explicit consent. Trust in data quality emerged as a notable concern, with considerations about the need for a controlling entity, either commercial or governmental, to oversee and ensure the integrity of the data. Cost considerations, particularly for smaller companies with fewer clients, were identified as a potential barrier to implementation. Proposals for a customer-centred payment model, where businesses contribute to the database and relieve themselves from the burden of data provision, were discussed as a possible solution. Security emerged as a paramount consideration, given the sensitivity of private information. The study underscores the necessity of a robust security framework to safeguard against potential cyber-attacks, acknowledging the heightened risks in an environment where private

[8] Page 51, Interview 1, Accountancy

information is consolidated, and businesses are unlikely to add information to a database that is not completely secure. The complete data is shown in the table below.

Economic	Advantages	Decreased duplicate work Resource optimization Long-term benefits in aquiring new customers
	Disadvantages	Uncertainty of costs managing a database Upfront investment required
Quality	Advantages	Ability to compare data which increases quality Fewer employees and/or less education of employees required
	Disadvantages	Potential discrepancies in the quality of the data between firms
Legal	Advantages	Provides a framework for quality of data and requirements for security
	Disadvantages	Compliance challenges with GDPR and other regulations Uncertainty about the legality of establishing a centralized database
Security	Advantages	Safeguards against cyber threats to seperate companies Controls added data by companies
	Disadvantages	Vulnerable to large scale cyber-attacks Concers about trust in data quality and ownership

Table 1: *Research Results*

In summary and to answer the main research question: *what are the potential advantages and disadvantages associated with the adoption of a centrally stored database for KYC data in the Netherlands?* While a centrally stored database presents notable advantages in terms of efficiency gains and streamlined processes, addressing the disadvantages related to legislation, trust, costs, and security is necessary for successful implementation. The research provides insight into the complexities and considerations associated with transitioning to and implementing a centralized KYC database in the Netherlands. This leaves the door open for future research into the discussed hurdles.

Chapter 5 – Discussion

In this chapter, several points are discussed. In chapter 5.1, a discussion about the conducted research and the results. After the discussion, the theoretical and practical implications are presented in chapter 5.2. Concluding the study is chapter 5.3, which describes the limitations of this study and suggestions for future research.

5.1 Discussion

In chapter four the results were presented. This section looks back on those results and compares this to the literature review. The discussion is focused on statements from the interviewees on the current- and proposed system. First, a significant observation is the general agreement the interviewees have concerning the current KYC system. In all interviews, the discussed inefficiencies are similar to those in the literature review. The requirement for skilled and/or experienced employees as discussed by the Rabobank is mentioned, as well as the duplicate work caused by the current structure. The increase in workload is mentioned in several interviews and is viewed as a serious issue for the long term. The interviews confirm the background information gathered in the literature review and show that the current KYC structure is in fact viewed as sub-optimal.

When looking at the proposed system, interviewees show doubt in the applicability of such a system. This is something that is not presented in the literature review. The limitations and requirements for successful implementation are complications not exposed by the reviewed literature concerning a centralized database. However, advantages a centralized database could bring compared to the current KYC system are shared between the literature review and the interviews. Examples of advantages mentioned in both are the decrease in costs when looking at personnel and workload, and the potential increase in quality when working together.

The study shows clear interest from the industry and a theoretical potential towards a centralized database for KYC data. A gap remains, focused on the limitations from the study. Though several limitations are deducted from the interviews, there are no solutions to these issues yet.

5.2 Theoretical and practical implications

Theoretical Implications: This study significantly contributes to the burgeoning field of research aimed at enhancing the Know Your Client procedure, within the context of the Netherlands. By testing a proposed solution with the intended target audience, it not only validates the importance of seeking innovative approaches to KYC but also uncovers crucial insights into the limitations that may arise during the implementation of such solutions. These newfound limitations serve as valuable basis for future research endeavours, providing a roadmap for scholars to delve deeper into addressing these challenges and refining proposed solutions. By challenging the prevailing narrative that centrally stored databases are inherently beneficial, the study sheds light on the often-overlooked negative aspects associated with such approaches. This critical examination encourages scholars to adopt a more nuanced perspective, one that acknowledges both the advantages and drawbacks of centralized data repositories in the context of KYC compliance. Also, the findings of this study have broader implications for theoretical frameworks within the field of regulatory compliance and financial services. By showing the complexities and nuances inherent in the KYC process, the study contributes to the ongoing discussion surrounding processes within financial institutions.

Practical implications: The practical implications of this study extend beyond academic discourse, offering benefits for both stakeholders in the financial sector and regulatory authorities. Foremost among these implications is the potential to provide companies and government entities with perspective on the current state of the KYC procedure and avenues for improvement. As the adoption of alternative KYC procedures gains traction, particularly within the Netherlands, this study serves as an effort to initiate meaningful dialogue and catalyse action in enhancing KYC practices. Furthermore, by highlighting the legal challenges associated with the proposed system, this study equips policymakers with insights into potential pitfalls and hurdles that must be navigated when implementing innovative KYC solutions. Using this knowledge, policymakers can develop informed strategies to overcome these obstacles and facilitate the adoption of more efficient and legally compliant KYC frameworks. Additionally, the identification of inefficiencies in resource utilization underscores the imperative for organizations to streamline their KYC processes and optimize resource allocation. By

addressing these inefficiencies, companies can enhance operational efficiency, reduce costs, and ultimately improve the overall efficacy of KYC procedures.

5.3 Limitations and future research

This thesis has some limitations. The first limitation concerns the interviewees of this study. As discussed in the research proposal, the research was focused on KYC within Dutch banks, though experience showed that it was extremely difficult to convince banks to take part in the interviews. The reasoning banks gave was either the lack of time or the inability to share information about their KYC process. Due to this limitation, the interview changed focus from banks to all companies obligated to fulfil a KYC check. This leads to results being more general, though also perhaps applicable in more scenarios. Another limitation is the time that this research has taken. Because more time has passed, new information could be presented that partially overlaps or that is not included within this research. The research does bring several subjects forward regarding future research. The limitations of the KYC procedure discussed in the results and conclusions leave room for interesting future research subjects. The four key limitations and their respective future research goals are defined below.

Legal: When looking at legal limitations, more research can be done regarding the compliance challenges outed by the interviewees, to make sure the proposed KYC database is compliant with laws both national and perhaps even international. This is not only related to the GDPR or the AML but also the Securities Regulations (SEC) and other international agreements and standards yet to be determined.

Trust: The next subject prone to more in-depth research is trust, or the way companies can work together in sharing KYC information; and how this would work in practice. In this study, it became clear that companies are not directly willing to share information. To make a centralized database function, more research must be done regarding who can add, access and change data in a database. Also, who should monitor this database and who is responsible for mistakes in this database?

Costs: The costs are also a subject of discussion when choosing who should finance the operation of designing, developing, and managing the centralized database. This could be done by the government, though perhaps it would be better if the government only monitors the operation while businesses run the database. Each possible solution has its up- and downsides and requires more research to be defined.

References

Accountantweek (2023, October, 23). *Overheid moet vooropgaan bij strijd tegen witwassen.* *https://accountantweek.nl/artikel/overheid-moet-vooropgaan-bij-strijd-tegen-witwassen?utm_source=accountantweek&utm_campaign=nb-23-10-2023&utm_medium=email&utm_content=overheid-moet-vooropgaan-bij-strijd-tegen-witwassen*

Art. 6 GDPR – Lawfulness of Processing - General Data Protection Regulation (GDPR). (2023, 27 January). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-6-gdpr/

Art. 7 GDPR – Conditions for consent - General Data Protection Regulation (GDPR). (2018, 28 March). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-7-gdpr/

Banken.nl (2019, December 3). *CDD en KYC vragen om slimme automatisering.* Banken.nl. https://www.banken.nl/nieuws/22055/cdd-en-kyc-vragen-om-slimme-automatisering

Banken.nl (2022, February 11). *Rabobank investeert deel winst (3.7 miljard) in verbetering KYC-processen).* Banken.nl. https://www.banken.nl/nieuws/23600/rabobank-investeert-deel-winst-37-miljard-in-verbetering-kyc-processen

Banken.nl (2022, August 29). *ING heeft handen vol aan witwascontrole: stichtingen en verenigingen pas 2023 weer welkom.* Banken.nl https://www.banken.nl/nieuws/23984/ing-heeft-handen-vol-aan-witwascontrole-stichtingen-en-verenigingen-pas-2023-weer-welkom

Banken.nl (2019, May 20). *Technologie maakt CDD en KYC-proces efficiënter en effectiever.* Banken.nl https://www.banken.nl/nieuws/21660/technologie-maakt-cdd-en-kyc-proces-efficienter-en-effectiever

Bitsch, V. (2005, January 1). *Qualitative Research: A Grounded Theory Example and Evaluation Criteria*. Journal of agribusiness, 23-1; 75-91.

Chen, J. (2023). Know Your Client (KYC): What It Means, Compliance Requirements. *Investopedia.* https://www.investopedia.com/terms/k/knowyourclient.asp

Compliance Instituut. (2021). *Witwasbestrijding… alle partijen zitten klem.* Nederlands Compliance Instituut. https://compliance-instituut.nl/nieuws/witwasbestrijding-alle-partijen-zitten-klem/

DNB. (2024, 2 januari). *Introductie WWFT*. https://www.dnb.nl/voor-de-sector/open-boek-toezicht/wet-regelgeving/wwft/introductie-wwft/

Elmas, M., Rogozinski, D. & Vis, J. (2019). Praktijkgids Bestrijding witwassen & terrorismefinanciering. Nederlands Compliance Instituut.

George, D., Wani, A., Bhatia, A. (2019, January 1). *A Blockchain-based Solution to Know Your Customer (KYC) Dilemma*. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). DOI: 10.1109/ANTS47819.2019.9118042.

InFinance. (2023). *FTE-vreter CDD kost branche vermogen.* Redactie InFinance. https://www.infinance.nl/artikel/fte-vreter-cdd-kost-branche-vermogen/

Isherwood, N. (2022). Moving to a perpetual KYC model: The benefits and the challenges. Journal of Financial Compliance, 228-236 (2022), 5 (3).

Klopper, H.C. (2008, December). *The qualitative research proposal.* School of Nursing Science, North-West University, South Africa. https://doi.org/10.4102/curationis.v31i4.1062

Kosten klantonderzoek – ING. (n.d.). https://www.ing.nl/zakelijk/betalen/tarieven/kosten-klantonderzoek

Kosten klantonderzoek – Rabobank. (n.d.). Rabobank. https://www.rabobank.nl/bedrijven/service/kyc/kosten-klantonderzoek

Kosten voor klantonderzoek. (n.d.). ABN AMRO. https://www.abnamro.nl/nl/zakelijk/producten/kosten-klantonderzoek.html

Malhotra, D. (2021, August 25). *How Blockchain Can Automate KYC: Systematic Review*. SpringerLink. https://link.springer.com/article/10.1007/s11277-021-08977-0?error=cookies_not_supported&code=dce09fed-1b0b-4cd6-b4b5-051f38cff067

Marktaandeel. (n.d.). Banken.nl. https://www.banken.nl/bankensector/marktaandeel#:~:text=De%20vijf%20grootste%20banken%20%E2%80%93%20ING,totale%20assets%20in%20hun%20bezit.

McGhee, G., Marland, G.R., Atkinson, J. (2007, July 25). *Grounded theory research: literature review and reflexivity.* Journal of Advanced Nursing 60(3), 334-342. DOI: 10.1111/j.1365-2648.2007.04436.x

Moyano, P. J., Thoroddsen, T., & Ross, O. (2019). Optimized and dynamic KYC system based on blockchain technology. *International Journal of Blockchains and Cryptocurrencies*, *1*(1), 85. https://doi.org/10.1504/ijbc.2019.101854

Moyano, P. J. (2017, December 8). *KYC Optimization Using Distributed Ledger Technology*. SpringerLink. https://link.springer.com/article/10.1007/s12599-017-0504-2?error=cookies_not_supported&code=0da2af23-2430-4b23-84e2-e4f73b6d6f02

Pai, A. (2013, January 20). *Know your compliance.* Business Standard. https://www.business-standard.com/article/pf/know-your-compliance-110101700024_1.html

Rajput, V. U. (2013). *Research on Know Your Customer.* International Journal of Scientific and Research Publications. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c24ae816b255a550328de0f6f6c6d344739f219d

Sinha, P., Kaul, A. (2018, August). *Decentralized KYC system.* Irjet. https://www.researchgate.net/profile/Ayush-Kaul-/publication/333827703_Decentralized_KYC_System/links/5d07e259458515ea1a6d6634/Decentralized-KYC-System.pdf

Stichting BKR. (2022). Maatschappelijk jaarverslag 2021. *Maatschappelijk Jaarverslag 2021, 2021*. https://www.bkr.nl/over-stichting-bkr/

Sundareswaran, N., Sasirekha, S., Joe Louis Paul, I. Balakrishnan, S., Swaminathan, G. (2020). *Optimised KYC blockchain system.* 2020 International Conference on Innovative Trends in Information Technology (ICITIIT). https://ieeexplore.ieee.org/abstract/document/9071533?casa_token=M68TYmSF87UAAAAA:wGw_7NMzF-9aB2TS2XaruOvQ9Q6iG5E2TpF6TCCl5Gj5s24uq4A4Jzctj5tzkXb7MgLr2wZC

Van Ooij, D. (2022, 19 oktober). Aantal cyberaanvallen op gemeenten verdubbeld. NOS. https://nos.nl/nieuwsuur/artikel/2449019-aantal-cyberaanvallen-op-gemeenten-verdubbeld

Wetten.nl – Regeling – Uitvoeringswet Algemene Verordening Gegevensbescherming – *BWBR0040940.* (2018, May 25). https://wetten.overheid.nl/BWBR0040940/2018-05-25

Winkel, Rik. (2021, June 20). *Markt voor compliance specialisten kookt droog.* Financieel Dagblad. https://fd.nl/economie-politiek/1388607/markt-voor-compliancespecialisten-kookt-droog