Improving financial services organisations their information security

Improving the implementation of the right access controls in IAM systems of organisations within the financial services sector.

T. van de Weijer

Improving financial services organisations their information security

Improving the implementation of the right access controls in IAM systems of organisations within the financial services sector.

by Teun van de Weijer

T. van de Weijer

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on 20-05-2022.

Student number:	4454715	
Project duration:	November, 2021 – May, 2022	
Thesis committee:	Prof. dr. ir. P.H.A.J.M. (Pieter) van Gelder,	TU Delft, chair
	Dr. ir. C. (Carlos) Hernandez Ganan,	TU Delft, first supervisor
	Dr. A.Y. (Aaron) Ding,	TU Delft, second supervisor
	N. (Nicole) Daal Tweeboom,	Ernst & Young, external supervisor

Preface

The Master Thesis report on ’Improving financial services organizations’ information security’ is in front of you. Document analyses, semi-structured interviews with financial services organizations, and expert interviews with multiple IAM experts form the basis of this study. The paper was created as part of the completion of Technical University of Delft’s Master Complex Systems Engineering and Management program. From November 2021 to mid-May 2022, I spent my time researching this issue.

Personally, I have always been interested in technology and all aspects that influence it. Given my constant observations with computers in my youth, the choice for Delft was easily made. Yet my interests went beyond computers and I was also looking for a link to society. I found this in the bachelor Technology, Policy and Management. During my bachelors I always enjoyed resolving problems that have a technical and societal point of view. For the completion of my bachelor, I wrote my thesis on societal acceptance of the Hyperloop. Again, a theme that brings together both technical and social aspects.

After obtaining my Bachelor’s degree, I made the choice to start the Master Complex System Engineering and Management. This choice was mainly based on the fact that this Master’s program includes both technical and social aspects in its questions. Subsequently, this study allows students to solve problems within complex socio-technical systems. Within this study, I was provided with the opportunity to follow the course Cyber Risk Management, which stimulated my interests regarding ICT even more. This course gave me a quick insight into cybersecurity risk management and a conversation with an employee of EY got me interested. During my thesis at EY, a global operating company, I’ve been able to experience what it is like to work in a rapidly changing environment with enthusiastic colleagues. On top of that, it gave me the opportunity to experience not only a theoretical view of cyber security but also a practical application.

I would like to thank my supervisors Pieter van Gelder, Carlos Hernandez Ganan and Aaron Ding, for guiding me and asking me critical questions to improve my thesis project. Also, a big appreciation to my supervisor of the company, Nicole Daal Tweeboom, who has helped me in getting to know the company and the activities the team is engaged in on a daily basis. Together with supervising me, reviewing my work and helping me wherever I needed. Overall, my thesis was an unforgettable experience with ups and downs. However, I look back on an educative experience and I am grateful to everyone who supported me in any way in this process.

T. van de Weijer
Delft, May 2022

Executive summary

In the recent years, the number of reports of cyber-attacks has increased significantly. An important cause for this is the rapid digitisation around the world, especially during the COVID-19 pandemic. As the virus spread around the world, this secondary threat increased within our technology-driven society. Organisation try to protect their valuable information with the use of information security, especially with identity and access management. With identity and access management (IAM), organisations give access to their employees or users and prevent cyber-attacks. Identity and access management mainly serve two purposes, managing the identities and the access to resources within organisations. Based on the permissions, roles or attributes of the users, the IAM system can determine who has access to which documents, applications or other information.

Research has shown that the two most commonly used access control are RBAC and ABAC. However, previous research has focused mainly on the individual models. It often lacks a comparison between different models and a practical perspective. In addition, no research has been found on the use and added value of cyber security principles in existing IAM models. Therefore, this research will focus on comparing the two models from a practical perspective. Ultimately, this research will give an overview and advice for overcoming the identified vulnerabilities within organisations from a business (owner) point of view. On top of that, the added value of cyber security principles on the IAM systems will be investigated. The main research question that follows from this is:

What are the effects of implementing access controls and IAM principles on information security and security challenges that exist within organisations in the financial services sector?

As defined, the main research question investigates how organisations set up the IAM and which vulnerabilities, risks, challenges, and opportunities can be identified. This will require an in-depth analysis of the organisations' current IAM. Secondly, the research question indicates differences in the IAM of organisations in comparison with characteristics of the organisations. In this research, a multiple case study approach will be used. Multiple case studies can be used to clarify whether the findings are practical or not. By comparing different cases with each other, the researcher can make new findings of influences based on the contraries or similarities. The cases can be compared based on their characteristics. The characteristics used in the research are the type of organisation, size, existence, profit/employee, merged or not, and role of the interviewee.

To answer the research questions, data will have to be collected. Data triangulation will be used for each case in this research, which means three data sources are collected per case. The use of data triangulation ensures that more angles are used and thus increases the validity of the case study. The three data sources used are desk research, document analysis and interviews. The interviews include both interviews with organisations and experts. The data is then analysed using Capability Maturity Model Integration (CMMI). The CMMI model is a well-known scale to measure the stage in which an organisation is using new technologies. The variables included in the CMMI model are based on the variables of the TAM-TOE framework.

Results

This study shed light on the maturity levels and challenges of IAM within financial services organisations. On top of that, it included the added value of implementing one IAM principle, namely zero-trust. The effects of implementing the various access controls were examined on the basis of five variables, followed by the characteristics, challenges, and zero-trust.

Variables

From a technology perspective, many organisations have an average maturity score. The explanation for this was given by the fact that organisations constantly have to adapt to new policies and therefore constantly have to be compliant, it is often difficult to fully automate the processes. This leads to most organisations having an average maturity score. The organisational, environmental and perceived usefulness maturity scores were also predominantly average. This can be explained by the research method used. By using interviews, many interviewee will speak more positively about the organisation and their systems. This gives a more subjective view of their IAM system. Also, the role of the interviewee has an impact on these scores because not everyone has the same focus in their daily work. Finally, the adoption intention has a predominantly low maturity score. The interviews showed that many organisations are busy improving their existing systems and are therefore not busy implementing new technologies.

Characteristics

The characteristics used in the research are the type of organisation, size, existence, profit/employee, merged or not, and role of the interviewee. Based on the cross-case analyses the following conclusion can be drawn. Firstly, banks have on average a better IAM system than insurers. Secondly, the size of the organisation has a positive impact on their IAM system and are on average better. Thirdly, the number of employees does not have impact of limit an organisation's IAM system. Fourthly, organisations that have been acquired or merged in the past have a worse IAM system than those that have not been acquired or merged. Finally, organisations that struggle with the technological side of their IAM system are most likely not willing to implement any innovations.

Challenges

Seven information security challenges have been identified during the interviews. The identified challenges are: Lack of knowledge, Manual processes, Education and training, Top management support, Overload of roles, Scalability, and Responsibility. Based on the data, it can be concluded that almost all organisations struggle with a lack of knowledge of both the IT teams and the managers who interact with the system. This is a consequence of another challenge that many organisations face, namely the way in which organisations provide knowledge about information security. However, the expert interviews revealed that they normally see top management support as one of the biggest problems in almost all organisations. An explanation for this could be that not all interviewees have the same role within an organisation and thus do not see this as a problem. In addition, both experts indicated that many of the challenges are caused by lack of support from top management.

Zero-Trust

Finally, this research examined the added value of information security principles in mitigating IAM problems. The literature has shown that due to the increasing complexity within IAM, a new model has been designed know as "zero-trust". The analysis of the data suggests that organisations with a relatively low adoption intention are not or hardly familiar with zero-trust. A number of reasons for this can be found in the literature and expert interviews. First, there is little practical experience and knowledge about zero-trust. Second, many organisation are busy improving their existing system. Third, investments in security solutions do not give a detectable return on investment, which is something that many organisations base their choices on. At last, the lack of support from top management ensures that there is insufficient knowledge, resources and time to implement zero-trust. Although zero-trust appears on paper to be the solution to many of the challenges identified by the organisations, much remains to be done.

To conclude, it is not about the type of access control but about how an organisation has implemented it. Because each type of access control can be implemented so that an organisation is secure and compliant, the difference is mainly in the manner of implementation. In addition, the data shows that a lack of support from top management is one of the most significant challenges within an organisation. Because support from top management is necessary for every choice within an organisation, this has a significant impact on IAM. Finally, the implementation of zero-trust can provide a solution to several challenges. However, the data shows that there are several challenges to overcome before zero-trust can become the standard in information security.

Contents

Abbreviations

Abbreviation	**Meaning**
ABAC	Attribute Based Access Control
ARBAC	Attribute Role Based Access Control
AFM	Autoriteit Financiele Markten
CoSEM	Complex System Engineering and Management
DAC	Discretionairy Access Control
DNB	De Nederlandse Bank
ECB	European Central Bank
IAM	Identity and Acess Management
MAC	Mandatory access control
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
RBAC	Role based access control
TAM	Technology Acceptance Model
TOE	Technology-Organisational-Environmental

List of Figures

List of Tables

1 Introduction

The digitisation of our surroundings significantly changes peoples' everyday lives. The evolution of technology ensures that all of our devices are becoming ”smart”. ”Smart” devices are devices that interact both with users and other devices (Silverio-Fernández et al., 2018). However, new challenges and severe security threats occur with the arrival of these intelligent devices (Atzori et al., 2010). In the recent years, the number of reports of cyber-attacks has increased significantly. An important cause for this is the rapid digitisation around the world, especially during the COVID-19 pandemic. As the virus spread around the world, this secondary threat increased within our technology-driven society (Lallie et al., 2021). With identity and access management (IAM), organisations give access to their employees or users and prevent cyber-attacks.

1.1. Background

Identity and access management mainly serve two purposes, managing the identities and the access to resources within organisations (Puchta et al., 2021). Based on the permissions, roles or attributes of the users, the IAM system can determine who has access to which documents, applications or other information (Samarati and de Vimercati, 2000). To ensure that the correct user has access to the correct information, IAM makes use of access controls. Access controls are models on which the IAM determines which user has access to which information. Examples of this type of model are access control list (ACL), mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC), attribute-based access control (ABAC), and risk adaptive-based access control (RAdAC). Nowadays, two of the most used models in IAM systems are RBAC and ABAC. RBAC is implemented the most out of the two, although it still has a static approximation (Kunz et al., 2019). ABAC is a more dynamic model that compares the identities' attributes to the predefined rules. ABAC originated because RBAC did not include attributes such as time of day and user location for distributed, dynamically changing systems (Coyne and Weil, 2013). Thus, ABAC can be used as both a replacement and an addition to RBAC.

In addition to the access controls, information security also makes use of principles, better known as software design principles. (Whitman and Mattord, 2021). The use of these principles should ensure the quality of the software. Some examples of commonly used principles are: *Economy of mechanism:* keeping the design as simple and small as possible, *Separation of privilege:* protection mechanism should require two keys to unlock, *Least privilege:* every users should operate using the least of privileges necessary to complete the job and *Least common mechanism:* minimize mechanisms common to more than one user and depended on all users.

The models and principles explained are all parts of IAM software such as *SailPoint* or *Okta*. These kinds of IAM systems manage thousands of identities and are the cornerstones of organisations' information security. Due to the essential role of IAM systems, they are often isolated from many other systems. While this makes for a more secure system, it also comes with limitations, such as not being in contact with tools that can track suspicious network activity (Puchta et al., 2021). Registering malicious activities within the network plays an important role in limiting the damage. Different types of malicious actions can be defined, but a general explanation of a malicious action is a human that takes actions to find weak spots in IT systems to compromise them. Malicious actions can be divided into three types. Namely, unintentional actions, a failure to take action where doing something could have prevented the outcome and intentional actions (Cebula and Young, 2010). By identifying the type of action, organisations can take tailored actions when detected. Nevertheless, this research mainly focuses on the access controls, which are preventative tools.

One of the common ways to penetrate an organisation is through its weakest link, humans. This phenomenon is also known as social engineering. The IAM systems have developed enormously from a technological point of view in the recent years and have become more robust. As a result, it has become much more difficult for hackers to attack computer systems or networks successfully. This phenomenon has led many hackers to focus on a different attack methodology, better known as; hacking the wetware. Wetware refers to the human part that is connected to computer systems, which refers to the weak link (Peltier, 2006). Social engineering focuses on several qualities of human nature, such as the desire to be helpful, the tendency to trust people, the fear of getting into trouble and the willingness to cut corners. Because hackers focus on people, both the problem and the solution could lie with people. By creating more awareness around potential threats, basic security procedures, and the organisation's security policy, people are better prepared for these types of attacks (Applegate, 2009).

The people who determine who has access to what and who manages the system are part of the IAM governance. Within each organisation, a person or a group is responsible for the governance of the IAM system. The governance of IAM can be divided into three different functions: reviewing and managing access, providing authority and leadership, and steering the company through changes. Organisations can decide how and by whom they have performed these functions. Organisations often choose to have multiple or all functions performed by one group to make choices as efficient as possible and standardise processes within the organisation. In addition to the advantages of having the processes performed by a group, there are also disadvantages. Because when all power lies with one group, this could also lead to weaknesses in the organisation. For example, insider threats could occur, or when a person is hacked, the hacker has direct access to almost all functions.

This research will investigate where organisations currently stand with their IAM systems and their choices in the past. Research has shown that the most commonly used systems are RBAC or ABAC or a combination of the two. Thus, the differences between the two models will also be examined, which threats they mitigate, and which gaps still exist with the implementations of the models. At last, the different information security principles are introduced, and the added value will be examined of the principles on the models implemented within the companies.

1.2. Research problem

In this section, the research problem will be explored by considering a series of previous studies and the knowledge gaps that appear when analysing previous work relevant to further research. Together, this will result in a description of the project's scope and the main research question.

1.2.1. Prior Research

A series of previous studies have looked at how organisations handle their identity and access management. However, there are plenty of opportunities to conduct innovative, in-depth research.

First of all, research has been done on the limitations of both RBAC and ABAC. The most found limitation of RBAC is the static character of the model. Thus, it is not able to consider the contextual information when making access decisions (Kuhn et al., 2010, Coyne and Weil, 2013). Research into ABAC's limitations has shown that while ABAC is more flexible and scalable, it is limited by a large list of attributes to manage (Coyne and Weil, 2013). Besides the limitations, also benefits of the two have been explored. For example, research has shown that due to the deterministic character of RBAC, it is easier to control who has access to what at what time (Jin, Krishnan, et al., 2012, Soni and Kumar, 2019). The research conducted on the benefits of ABAC systems mainly shows that ABAC can be managed centralised, and the rules are fine-grained and contextual (Kuhn et al., 2010, Coyne and Weil, 2013).

Secondly, plenty of research has been done towards implementing different access controls, most of which have conducted empirical research. For example, many case studies of IAM explain and analyze an implementation of the system as a whole (Partida et al., 2021, Bradford et al., 2014). Nevertheless, no comparison is made between the implementation of RBAC and ABAC. In addition, the case studies often show how an IAM system is implemented and what the advantages and limitations are. However, no research has been done with multiple case studies with overlapping characteristics to compare and generalise the results. Some research mentions the best practices, but it is mostly focused on implementing IAM systems as a whole and mentions only the technology point of view.

Thirdly, the Chair of Information Systems of the University of Regensburg researched the shortcomings of the current IAM architecture and what possible extensions could be (Puchta et al., 2021). The used models in this research are both RBAC and ABAC. The research gives a clear overview of the architecture's current blocks and eventually significantly improves the existing IAM architecture from a theoretical point of view. Soni and Kima (2019), have shown a comparison of the RBAC and ABAC model in a private cloud environment resulting in a hybrid scheme of the two models that is scalable and dynamic (Soni and Kumar, 2019). Finally, research conducted by Das et al. (2018) shines a light on the policy engineering side of the two models (Das et al., 2018). All found research on the two models shows the comparison of the models' technology, policy, and constraints. However, there is no research describing the comparisons based on the application of the models within multiple different organisations. In addition, no research has been found on the use and added value of IAM principles in existing IAM models.

1.2.2. Knowledge gap

Research has already shown that role-based access control and attribute-based access control are the most commonly used models for identity and access management. Although they are the most widely used models within organisations, few studies compare the two models through empirical research within multiple organisations. The first research gap that can be concluded from the literature research and prior research is the non-existence of research using multiple case studies with overlapping characteristics into the weaknesses, vulnerabilities, or gaps of RBAC, ABAC or a combination of the two. The second research gap that can be found in prior research is the added value and use of a combination of information security principles in existing IAM systems. Combining these two research gaps results in the added value of this research from both an academic and societal point of view. Ultimately, this research will give an overview and advice for overcoming the identified vulnerabilities within organisations from a business (owner) point of view. On top of that, the added value of cyber security principles on the IAM systems will be investigated.

1.2.3. Scope

This research will address two access control models, RBAC and ABAC, used for identity and access management. All selected organisations are different and have several overlapping characteristics. By collecting all different information from organisations, conclusions can be drawn from the correlation between the characteristics and their IAM. Characteristics of organisations include #employees, #roles, profits, and activities. The scope of this research also includes the sector in which the research will be conducted. The financial services sector is chosen for this research because the diversity of organisations and the number of valuable assets the organisations need to protect will give a broad insight into their IAM. With the help of contacts from Ernst & Young, a selection of the organisations will be made to interview. The interviewees will all have a connection with cyber security and technical background. At last, this research focuses on looking into the IAM from a corporate point of view, concluding that this research mainly looks into the allocation of rights to the employees within organisations.

1.2.4. Research questions

The main research question to be answered in this thesis project is:

What are the effects of implementing access controls and IAM principles on information security and security challenges that exist within organisations in the financial services sector?

Several sub-questions are formulated after constructing the main research question. Together these questions are used to solve the main research question. Before the first research question can be investigated, knowledge will be needed on data security, especially identity and access management, to create a good foundation for the research. First, with desk research, data is gathered to get an overview of the topic and the interaction between different access controls.

- *SQ1: What actors are involved with identity and access management within financial services organisations, and how do they relate with each other?*
- *SQ2: Which theoretical framework can be used in analysing organizations' choices towards access controls?*
- *SQ3: What are the effects of the type of access control on the IAM of financial services organizations?*
- *SQ4: What are the effects of and correlations between certain characteristics and the IAM of financial services organisations?*
- *SQ5: What information security challenges exist using different access controls, and how are these security challenges overcome?*
- *SQ6: What information security principle could add value in mitigating the IAM problem within financial services organisations?*

1.3. Relevance

In this section, the societal and academic relevance of the research is discussed. In addition, the final subsection will explain the fit of this research project to the CoSEM Master and to the track Information and Communication.

1.3.1. Academic relevance

The protection of organisations' data is a recurring topic in previous studies. However, there is still much uncertainty about how information is protected and the shortcomings of the existing systems. The academic relevance of this research is that it will provide insight into the choices and considerations that organisations have made when implementing their IAM system. These organisation are currently facing challenges and this research will show how IAM principles could overcome these challenges and contribute to protecting data. By first providing a good picture of the implemented systems and the choices involved, the overview can provide a better foundation for applying IAM principles.

In addition to providing insights into the choices made and the challenges faced by organisations in IAM, this research will contribute to decisions in the future. Besides the possible application of IAM principles, every organisation need innovate to protect themselves cybercrime. Transitions from existing systems to new systems will have to be made. The lessons from the past offer organisations a basis of knowledge on how to take these steps in the future.

1.3.2. Societal fit

The problem as described is at the heart of our society. We use digital devices in almost everything we do, many of which keep track of data and directly connect to the internet or other devices. How people manage who gets access to this data is crucial. For example, research by The Global Risk Report of the World Economic Forum has shown that cyber security is an increasing problem (McLennan, n.d.). Today, cyber-attacks occur in sectors such as gas and oil, healthcare, banking and more. This leads to negative consequences in all sectors, such as loss of reputation, costs, and loss of time. Therefore, it is essential to draw attention to a problem that has such an impact on our society.

This research will be of value for controlling current weaknesses and vulnerabilities of corporate identity and access management. Best practices will give guidance for organisations that go through the same process. In this way, organisations with the same problems can immediately work towards a possible solution. The solutions will consist of technical and non-technical elements because the human aspect can often play an important role in cybersecurity. Thus, this study will improve the organisations' IAM, make the users/client/customer less vulnerable and make the organisation more resilient to the future of cybercrime.

1.3.3. Fit with CoSEM

In the Master Complex System Engineering and Management at the Faculty Technology, Policy and Management, all courses focus on solving problems within sociotechnical systems. The Faculty of Technology, Policy and Management combines insights from the engineering sciences with the humanities and the social sciences. Its mission is to develop robust models and designs to solve the complex challenges of today's networked, urbanised knowledge society. In this thesis project, the social and technical parts of the system are, respectively, the owner/employee/client/user of the system and the system itself. To sufficiently cover the problem defined, the interaction between social and technical aspects of the system have to be analysed, resulting in the research's complexity. Eventually, this thesis aims to give recommendations to organisations to improve their current identity and access management, based on the finding of this study. At last, in the Master program CoSEM, the Information and Communication track was chosen. This fits well with this thesis since it focuses on the ICT and the human aspects of a problem.

1.4. Outline

In this report, first the key concepts are explained in chapter 2 in order to give more background knowledge on the subject. After which, in chapter 3, a literature review is carried out which results in a theoretical framework for the research. An overview of the methodology follows in chapter 4 where the research approach, method and design are further explained. Subsequently, in chapter 5, the data analysis will be carried out consisting of a within case and cross case analysis. Subsequently, a discussion of the findings is given in chapter 6, together with the limitations of the research and future research. Finally, in chapter 7, the research will be concluded with a conclusion and recommendation based on the results.

2

Key concepts

Before analyzing Identity and Access management and the factors that influence this system, the main concepts are discussed. The concepts of cybersecurity, Identity and Access management, zero-trust security model, and chapter 1 are elaborated in this chapter.

2.1. Cybersecurity

In recent years, it has become increasingly important to protect IT systems against intruders. In recent years, the number of reports of cyber-attacks has increased significantly. An all-time high of cyber-attacks has been reached hence the rapid digitization during the COVID-19 pandemic. As COVID-19 spread around the world, this secondary threat increased within our technology-driven society (Lallie et al., 2021). According to experts, the frequency and impact will increase further in the coming years as people depend on the internet and connected systems more (Dodge and Kitchin, 2018). Protecting IT systems and information is called cybersecurity. Although the term ”cybersecurity” is widely used in the literature, it has multiple meanings (Craigen et al., 2014). In this study, cybersecurity will be described as; ”the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.” (ITU, 2009).

Within cybersecurity a commonly used concept is information security. The properties protected by cybersecurity are usually referred to as information security. Information security mainly focuses on the confidentiality, integrity and availability of the protected data. Confidentiality ensures that sensitive information is not disclosed to unauthorized persons; integrity ensures that a specified and authorized way is required to read, modify, or destroy data and programs, and availability ensures that the system's resources are available when asked for by an authorized user (Kemmerer, 2003). In the financial services industry organizations are primarily interested in the integrity of their systems. Their information should only be managed by authorized users and should always be accurate, consistent and reliable (Mandke and Nayar, 1999).

Cybersecurity consists of a large number of defensive methods used to protect the systems and detect intruders. Four general approaches can be found to achieve a secure environment (Kemmerer, 2003).

1. Procedural approaches
   The appropriate behaviour that users need to follow when using systems is prescribed by the procedural approach. The user guidelines consist of many restrictions and procedures. For example, the choice of a password that is long enough, not too obvious and not easily guessable. The guidelines show the amount of upper and lower case letters, numbers and special symbols.

2. Functions and Mechanisms
   By using functions or mechanisms in computer systems, the systems can be better secured. The

mechanisms included in this report are authentication mechanisms and access control. Authentication mechanisms are used to assure that a particular user is who he/she claims to be and access controls give access to files based on access control policy to authenticated users.

3. Assurance techniques
   An important aspect of the security of a system is to give someone the confidence that the system will perform as desired. This is done by different assurance technique such as penetration analysis, formal specification and verification, and covert channel analysis. These methods do not directly provide a more secure system. They ensure that confidence in the security of the system is increased.

4. Intrusion detection
   Finally, it is good to monitor what is happening within the computer systems. By means of intrusion detection systems (IDSs), computer systems can keep a record of the activity on the system. The data collected by IDSs is called audit log. By analyzing the audit log suspicious activities can be detected and actions can be taken.

In this research, IAM will be examined, which mainly focuses on how organisations protect and give access to their information. As described in the previous sections, the definition of cybersecurity is visualised in figure 2.1. The figure shows that information security is part of cybersecurity and is influenced by the four approaches. This research will mainly focus on the information security of organisations.

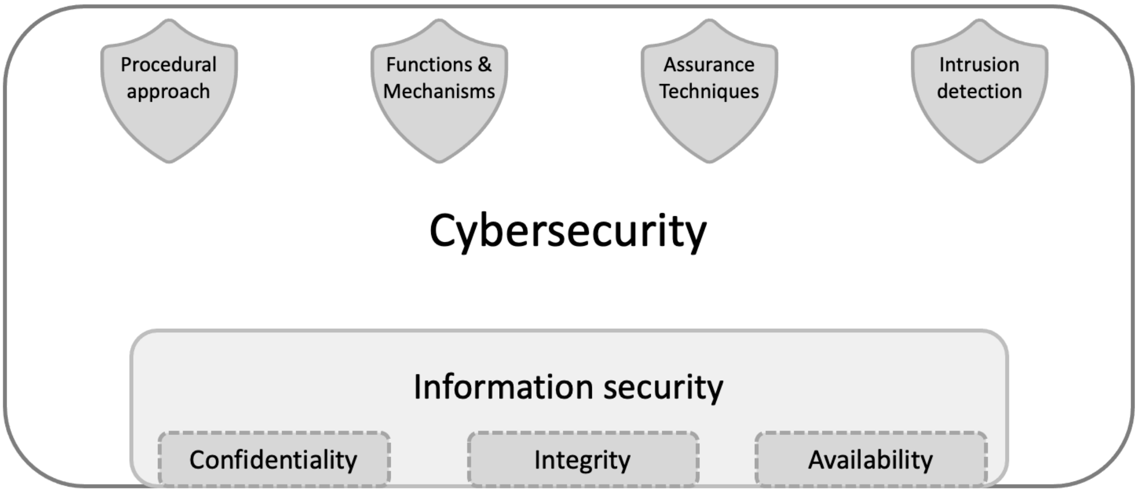


Figure 2.1: Cybersecurity

2.1.1. Malicious actors

The approaches discussed in the previous paragraph share the same purpose; to protect computer systems from intruders. Intruders are actors who try to break into computer systems and are often described as malicious actors. Malicious actors are humans that take action to find weak spots in IT systems to compromise them. A full range of cyber-threats with humans involved are known, but actions that try to compromise IT systems can be divided into three types of actions (Cebula and Young, 2010). Firstly people can take unintentional actions without any malicious or harmful intentions, such as making a mistake or creating an error in the system. Secondly, due to their lack of knowledge or skills, people fail to take action in a situation where doing something could have prevented the outcome. Lastly, people could also act to harm, such as fraud, sabotage, theft and vandalism. This research addressed mainly focuses on the people who have the intention to do harmful things.

By identifying the type of actor that is trying to harm the IT system, organizations can take tailored actions. The type of actor could be different every time. An important part when assessing cyber-threats is the factor of sophistication and competence of the various actors involved. The malicious actors can range from government or resourceful criminal groups to less dangerous and skilful groups of individuals. One of the most serious threats is the insider that gives access to the systems from the inside.

2.1.2. Cyberattack phases and countermeasures

Although every cyberattack is unique, several phases are passed through. MITRE ATT&Ck (2021) has defined all the different stages that are passed through. Going through each stage can better understand how cyber criminals operate and better estimate the impact. MITRE ATT&CK has defined 14 tactics that are gone through when someone commits a cyberattack. The tactics represent the ”why” of someone who has committed a specific attack and are shown in the table 2.1. Each tactic consists of techniques and sub-techniques that a cybercriminal can use. The ultimate goal of the MITRE ATT&CK matrix is to find out the reasoning behind an action. In this research the matrix gives an overview of all the different steps included in a cyberattack.

Name	**Description**
Reconnaissance	Gather information to plan future operations.
Resource Development	Establish resources to support operations.
Initial Access	Get into your network.
Execution	Run malicious code.
Persistence	Maintain their foothold.
Privilege Escalation	Gain higher-level permissions.
Defense Evasion	Avoid being detected.
Credential Access	Steal account names and passwords.
Discovery	Figure out your environment.
Lateral Movement	Move through your environment.
Collection	Gather data of interest to their goal.
Command and Control	Communicate with compromised systems to control them.
Exfiltration	Steal the data.
Impact	Manipulate, interrupt, or destroy your systems and data.

Table 2.1: MITRE ATT&CK matrix

2.2. Identity and access management

The way an organisation manages who gets access to what is called identity and access management. Every business that owns networks, servers, storage’s, services and applications give access to their employees and clients in a certain way. Since every user needs to be identified and given access to the right data, there is a high complexity in these systems, which makes IAM a vulnerable part of every business Nowadays, a large number of data leakage incidents are caused due to these vulnerabilities (Eludiora et al., 2011). IAM systems provide different security measures including authentication, authorization, and provisioning of storage. The system guarantees the security of identities by ensuring that the right users are allowed in the systems. On top of that, the system also helps to manage the access rights by checking if the right user with the right privileges are accessing the data (Sharma et al., 2016).

2.2.1. Access controls

Both, identity management and access management, blocks limit the access to the security context only to authorized roles, modules and algorithms (Repetto et al., 2021). With the use of access control the IAM systems provide a secure mechanism to protect the system. The four main types of access control mechanisms are explained. The first type is mandatory access control which is the traditional mechanism (MAC) to define the access rights of users. MAC gives data owners the ability to give access permission through the operating system (Indu et al., 2018). In MAC models, each file is labelled with a level of access right needed to open is. Each user is assigned a similar level by which they have permission to open a certain amount of files. The problem with MAC models is that it needs careful planning and frequent monitoring to keep the labels up-to-date (Jiang et al., 2016). The second type of access control mechanism is discretionary access control (DAC). DAC is a control mechanism that uses a data owner which permits users to access a certain amount of files. DAC systems perform a security check by validating the username and password of each user. Although DAC is more flexible than MAC, it provides less security because only the username and password are needed to access the files.

The third mechanism is role based access control (RBAC) and is one of the most used mechanisms in IAM systems. RBAC mechanisms provide access right by assigning roles and privileges to users. Two types of roles are defined, application/technical and organizational/business role. An application/technical role has specific entitlements or tasks based permissions which is limited to the specific application. An organizational/business role is divided into different job functions with different access rights (Zhu et al., 2014). One of the downsides of RBAC is that every assigned role that changes over time needs to be checked and validated. At last, attribute based access control (ABAC) is discussed, which is the also one of the most used mechanisms in IAM systems. ABAC provide access right based on a set of subjects, objects, environmental conditions and a set of access control rules (Das et al., 2018).

2.2.2. Access governance

Access governance is a collective term for various methods used to organise authorisation management within an organisation. As described in the previous section, part of access governance is access controls that ensure the organisation of authorisation management within organisations. In addition to access controls, attestation, re-certification, risk management, and compliance policies are also part of access governance. One of the most significant challenges in access governance is dealing with the large quantities of data and their complex structure (Sturm and Kern, 2013).

2.3. Social engineering

As stated in the introduction; a commonly used way to penetrate an organisation is through its weakest link, humans. Illegally getting in into an organisation via humans is called social engineering. While the focus is mainly on the technical development of IAM, this provides a huge opportunity for cyber criminals to exploit social engineering. This phenomenon has led many hackers to focus on a different attack methodology, better known as; hacking the wetware. Wetware refers to the human part that is connected to computer systems, which refers to the weak link (Peltier, 2006).

The impact and complexity of social engineering only really became known after the publication of the book *The Art of Deception: Controlling the Human Element of Security* (Mitnick and Simon, 2003). This book describes the physical, social, and technical aspects of a cyber criminal engaging in social engineering. The following subsections aim to explain the use of different approaches by attackers.

2.3.1. Physical approach

The name gives it away, but the physical approach applies when an attack takes physical action to collect information. The collection of information can range from personal information to system logins. A common technique of the physical approach is dumpster diving, which is explained in more detail in section 2.3.4. Physical actions often include stealing or extortion to gather information.

2.3.2. Social approach

Within social engineering, the social approach is one of the most important. Within the social approach, attackers focus on socio psychological techniques to manipulate a victim. Cialdini's principles of persuasion are examples of methods applied within the social approach (Cialdini, 2001). For example, an attacker could pretend to be someone with more authority and get the victim to perform tasks. In addition to the social approach, there is also an opposite method, reverse social engineering (Cialdini, 2001).

Reverse social engineering

Instead of direct contact with a potential victim, an attacker may also choose to influence him or her indirectly. By making the victim believe that he is trustworthy, the attacker can eventually steal the information he wanted. An example of reverse social engineering is helping a victim with a self-created problem. The attacker pretends to be the one who can solve the problem that he has created himself. In this way, he has gained the victim's trust and can request information from him or even steal it.

2.3.3. Technical approach

Finally, a social engineer also makes extensive use of a technical approach (Mitnick and Simon, 2003). Many attackers go on the internet and try to collect personal information by hacking users. A common method is that hackers combine a technical approach with a social approach. They first use the Internet to gather information about potential victims or send phishing emails to penetrate the system. Then they use this information to gain trust when they are in contact with the victim.

2.3.4. Examples of social engineering attacks

To give a better idea of the ways attackers try to penetrate organisations using social engineering, some examples of types of social engineering will be given. The types of social engineering are limited by the creativity of the attacker (Manske, 2000). By using social engineering in a smart way, the attacker often needs to make little or no investment in technical equipment. A few examples of social engineering are given (Manske, 2000).

- **Phishing:** One of the most common forms of social engineering is phishing. Although people often think this is a technical way of hacking, nothing could be further from the truth. The principle of phishing is based on the creation of a well thought-out message. Phishing is often used as an intermediate step towards the ultimate goal of the attacker, for example gaining access to a user's or organisation's system.

- **Impersonation:** Besides phishing, impersonation is one of the most common forms of social engineering. Impersonation is a social engineering technique that refers to the use of false credentials. This can be as simple as using fake business cards, or as complex as creating counterfeit identification.

- **Persuasion & bribery:** Persuasion and bribery are other forms of social engineering that seek to cleverly circumvent rules. In both cases, the attacker tries to mislead a person with false information or with small gifts. In both cases, the employee is the focus of the attack.

- **Shoulder surfing:** As the name suggests, shoulder surfing involves an attacker looking over the shoulder of an unsuspecting user. The attacker sees her login details and comes back at a later time to penetrate the system with her details. Shoulder surfing is one of the simplest ways to penetrate a system unnoticed.

- **Dumpster diving:** One of the most favourite techniques of hackers and social movers is dumpster diving. Many employees do not realise how much value discarded information can still hold. Thus, an attacker can easily grab the discarded information. This information gives the attacker the chance to impersonate another person because he has more information about the company and its employees. Dumpster diving is often used when applying other social engineering techniques.

2.4. zero-trust security model

The complexity of the described access controls of an enterprise has increased dramatically in recent years. A single enterprise operates several internal networks, local infrastructures, remote (mobile) individuals and cloud services (Stafford, 2020). This increase in complexity has led to the development in 2018 of a new model for cybersecurity known as ”zero-trust”. The zero-trust approach focuses on the protection of data and services. NIST and NCCoE have described the basic concepts of a zero-trust architecture and a demonstration of its implementation. A zero-trust model assumes that the attacker is present in the environment. This ensures no implicit trust and that the organisation is constantly analysing and evaluating risks. Subsequently, the appropriate protective measures are immediately taken to limit the analysed risks. At zero-trust, these measures consist mainly of minimising access to resources to authorised and verified persons.

The zero-trust architecture is an organisation's architecture based on zero-trust principles and designed to prevent data theft. The zero-trust architecture is designed and implemented based on the following zero-trust tenets (Stafford, 2020):

- All data sources and computing services are treated as organisational resources, which must be secured.
- Despite the network location of the access request, all communication is secured. No trust is granted automatically, and no assets requesting access are trusted by default.
- Access to resources is granted per session only.
- Access is determined based on device characteristics, behavioural and environmental attributes.
- Least privilege applies.
- Access is not granted statically but continuously re-evaluated.
- Information about assets, network infrastructure, and communications is collected and used to improve security.

The zero-trust principle has its core idea that nobody on the network is trusted and that every activity on the network can be a danger. Thus, this means that every access is analysed and evaluated. Only if the verification is successful access is granted. The verification is not only done based on someone's password but also the device, current location and time are taken into account in this process. Also, the principle of least privilege applies, which means that the user only gets access to what he needs for his work. Overall, zero-trust is not a technology but a way of thinking that makes use of various principles (Sultana et al., 2020).

3 Literature review

The main goal of cybersecurity is to protect IT systems and information while giving access to the data to the right people. Two access controls are discussed in a technical, organisational, environmental, and user context to achieve this goal and provide effective cybersecurity. Before looking at the access controls, this research will first examine which actors influence the system and their relationship. Finally, it will be examined which framework can be used for this study based on the literature and previous research.

3.1. Actors

All actors and their relationships are described to provide a clear picture of the context of this research. When implementing IAM, mainly actors within an organisation plays a role. However, the implementation of IAM also focuses on how people outside the organisation have access to the system. This means that both internal and external actors are analysed separately.

3.1.1. External actors

The first actors discussed are the external actors that influence an organisation. In this research, an organisation means a company that uses IAM. The organisation itself is, therefore, the first actor to be identified. The organisation will make various choices regarding their IAM based on outside influences. Usually, the IAM system is organised by a service provider within an organisation (Ghaffari et al., 2021). To prevent data from being stolen, misused or modified, service providers provide authentication, management of identity and management of roles/attributes. It then uses software from the service provider to monitor and control the system (Ghaffari et al., 2021). Some examples of IAM service providers are Sailpoint, Okta and OneIdentity.

Next to that, some actors positively try to influence the organisation in IAM development. These are described as supervisors in this study. Supervisors in the Netherlands are De Nederlandse Bank (DNB), Autoriteit Financiële Markten (AFM), European Central Bank (ECB) and the Dutch government. The main tasks of DNB, AFM and ECB are to supervise the financial services organisations (Haas and Vor, 2001). However, there are different types of financial service providers in the Netherlands, namely, banks, insurance companies, pension funds, credit card providers, and asset managers (Ministerie van Financiën, 2022). The DNB and AFM are responsible for the supervision of all financial service providers. In addition, banks in the Netherlands are also supervised by the ECB (De Nederlandse Bank, 2022). Since governments are increasingly aware of the economic impact and problems involved with cyber-attack, they are becoming more involved and tightening their rules and regulations (Anderson and Moore, 2006). The Dutch government has a more regulatory role. This means that the government creates the rules that the DNB then checks.

3.1.2. Internal actors

In addition to the external actors, various actors within the organisations influence the IAM system. Within organisations, a specific department is aware of the IAM system; these are the IT administrators.

They are involved in policy, identity management and maintenance of the systems (Sharma et al., 2016). As an IT administrator, you are often not responsible for allocating employee rights. This task rests with the managers in an organisation, and the IT administrator has a supervisory role (Puchta et al., 2021). Because managers are responsible for who has access to which programs and data, it is crucial that they also have some knowledge about cyber security and the risks (Puchta et al., 2021). Besides the managers, there is always someone responsible for the application/asset that people want to access. An application/asset manager is responsible for accessing the application/asset under his control. Together with the manager, they ensure that the right people have access to the right application/asset in order to do their work.

In addition to controlling and using the IAM system, IAM is also essential to include in the organisation's vision for the future. The organisation's top management plays an essential role in prioritising IAM within the organisation. Management can determine whether there is organisational and financial support. When IAM is higher on the agenda of the management of an organisation, in addition to improvements within the system, it is also possible to make employees more aware of the risks. An overview and the relations between the different actors, both internal and external, is shown in figure 3.1.

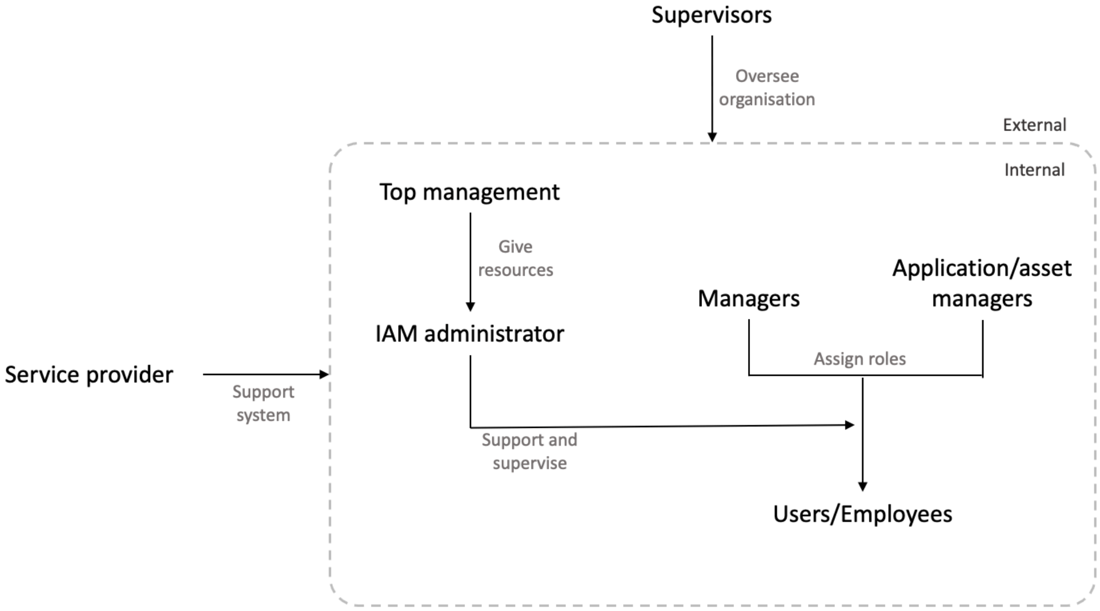


Figure 3.1: Overview actors

3.2. Role based access control

Identity and access management controls and gives access to specific information to authorised persons in organisations. Access controls are an essential part of the IAM system and determine how access is granted to persons within an organisation. There are many different access controls as described in chapter 1. Nevertheless, one of the most commonly used access controls is role-based access control (RBAC). RBAC was first introduced at the end of the 20th century (R. S. Sandhu et al., 1996). In the 1990s, organisations started implementing RBAC features into their security systems. Several RBAC models have been designed without any standardisation of the RBAC features (D. F. Ferraiolo et al., 2001). Therefore, the National Institute of Standards and Technology (NIST) started an investigation into the added value of the RBAC features in the 1990s (Smith et al., 1996, D. Ferraiolo et al., 1993). The research consisted of market analysis, prototype design, and sponsored external research. In addition to the research of the NIST, a lot of research has been done at the university level to develop new RBAC models and applications.

The first attempt at describing a standard for RBAC was made in 2000 (R. Sandhu et al., 2000). In this research, several things are described, including the basic role concept of RBAC, the components of an RBAC mechanism and the principles that an RBAC mechanism must comply with. For example, the purpose of RBAC is to ensure that access is granted via the enterprise based on functional roles and then appropriately assign users to a role or set of roles. The way in which an RBAC mechanism is constructed according to the NIST consists of four layers that build on each other. Each layer adds an additional requirement to the mechanism and thus makes it more complex.

- Flat RBAC
  The first level embodies the essentials of RBAC. The main function is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by admins of the roles (R. Sandhu et al., 2000).

- Hierarchical ARBAC
  The second level adds the first requirement to the system. By adding hierarchy, a layering is created about who has control over who. Senior roles will acquire the permissions of their juniors. A distinction is still made between two forms of hierarchy; general and restricted.

- Constrained RBAC
  The third level of the RBAC mechanism adds the requirement for enforcing the separation of duties (SOD). SOD is a well-known method to reduce the risk of fraud. By spreading responsibilities and authority for an action or task over multiple users, the risk of fraud decreases. Both static SOD (based on user-role distribution) and dynamic SOD (based on role activation) are included in the model.

- Symmetric RBAC
  The fourth level identified by the NIST is the symmetric RBAC. This adds a requirement for effectively supporting the permission-role review performance comparable to user-role review.

The clarification of the model by the NIST provided a foundation on which models could be developed. However, in later literature, there is not much more to be found about the four-layer design described by the NIST. Shortly after the NIST published the city description of RBAC, researcher Elisa Bertino (2003) published her view on the concepts and trends of RBAC. However, she left out the symmetric level in her description. Next, she described RBAC as being too static, making it difficult to use RBAC for organisations where roles have a limited or periodic temporal duration. (Bertino, 2003).

3.3. Attribute based access controls

In contrast to role-based access control, attribute-based access control (ABAC) has a dynamic character. This is the main reason for the arrival of ABAC models in the early 21st century. Subsequently, in 2014, the NIST released a document that federal agencies provide with a definition of ABAC (Hu et al., 2014). This document also consists of reasons to use ABAC to improve the information exchange. The function of an ABAC model relative to RBAC remains unchanged, protecting data from unauthorised users. However, an RBAC model works with attributes of a ”role” whereas ABAC works with attributes of an ”identity”. The most significant change is that ABAC models can be evaluated using a complex Boolean function of logical based analysis (Vijayalakshmi and Jayalakshmi, 2021, Hu et al., 2014). The attributes are part of the user, and based on the assigned attributes, the ABAC model can grant access. This allows for more precise access control by allowing a more significant number of inputs and thereby providing more possible combinations of variables (Hu et al., 2015). Therefore, the limiting factor within ABAC models is the number of attributes assigned to the users. Overall, the ABAC model should be the right fit for today’s complex security requirements due to its flexibility, efficiency and granularity (Vijayalakshmi and Jayalakshmi, 2021).

The high-level definition of ABAC given by the NIST is; *”An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions”* (Hu et al., 2014). The way the model operates is shown in figure 3.2. The user requests access to specific data by sending a query. First, the request is sent to the policy enforcement point (PEP)—the PEP checks with the policy decision point (PDP) whether the requirements for access are met. After checking with the policy administration point (PAP) and policy information point (PIP), the PDP sends permission back to the PEP. The PEP finally gives or does not give the user access to the specific data.

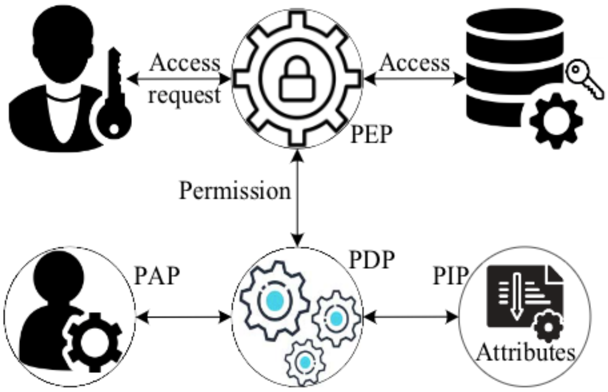


Figure 3.2: ABAC architecture (Salehi et al., 2020)

3.4. From RBAC to ABAC

After the introduction of RBAC at the end of the 20th century, the model was adopted by many organisations. However, apparent weaknesses of the model soon became known. For example, it would be too static and difficult to determine which individual roles there are within an organisation (Kunz et al., 2019). As a result, a new model was designed at the beginning of the 21st century, the ABAC model. ABAC grants access based on attributes. ABAC forces the developers to centralize all authorization decisions and call out at run-time for a decision based on the *Subject*, *Resource*, *Action*, and *Environment* request attributes. Attributes make it dynamic and easier to understand how the rules grant access to a resource. The differences from the literature are divided into four subsections, implementation, governance, maintenance and scalability. The subsections give a more detailed insight into RBAC and ABAC literature.

3.4.1. Implementation

Before an IAM system can be used, it must be implemented. Here, trade-offs must be made between the various access controls. This mainly depends on the technology, environment, desired functions, and organisation structure. In an environment with many different functions and complex requirements, using RBAC is very difficult (R. S. Sandhu et al., 1996). The use of roles makes it more difficult to grant specific access to a user. This leads to users often having more access than is necessary. In this case, the use of the ABAC model is much more pleasant. ABAC is cheaper and simpler to implement in a complex environments (Coyne and Weil, 2013). By linking attributes to the user's identity, rules can be drawn up for the attributes and users therefore only have rights for what they need. Creating the access rules is part of implementing access controls, also known as policy engineering.

In addition to how the access control is technically implemented, the development cost also plays a significant role. In the first place, it is difficult to say which access control is cheaper to implement because it depends on many factors. An RBAC system is cheaper than an ABAC system in relatively less complex organisations. However, when an organisation grows and becomes more complex, it often switches to an ABAC model. This will then be accompanied by high costs to make the switch. However, these costs are saved in the long term because ABAC systems are cheaper to maintain (Hu et al., 2014). As part of the implementation, rules are created to allocate the access rights. This process is called policy engineering.

Policy engineering
Creating the rules for access controls within an organisation is also known as role engineering, which is part of policy engineering. This process is different for each access control and plays a pivotal role in successfully implementing access controls. RBAC uses role mining to draw up the rules (Das et al., 2018). Role mining could be both a bottom-up or top-down technique. The bottom-up technique starts with the consideration of the existing permission assignments of the users of the organisation (Frank et al., 2013). The top-down approach suggests beginning with analysing the organisation's structure. The structure reveals business processes that are composed of different functions. These functions describe the set of permissions required to complete the task. Both approaches are relatively straightforward processes and ensure that each role has specific access.

Unlike role mining, ABAC's policy engineering is much more complicated. Within the implementation of ABAC, policy engineering is the most expensive and challenging part of the implementation of the model (R. Kumar et al., 2010). ABAC creates the rules that can be bottom-up, top-down and via a. The top-down approach is like a clean slate that uses business processes to identify accesses, whereas the bottom-up approach uses the existing rules. Though, both approaches complement each other when it comes to their strengths and weaknesses (Das et al., 2018). Finally, both RBAC and ABAC use mutually exclusive roles that ensure a single user never has permission to perform a sensitive job all by himself (Kuhn et al., 2010).

3.4.2. Governance and maintenance

The collection of methods by which an organisation organises its access control is called access governance. In addition, the maintenance of the system is also often part of the access governance of an organisation. When we compare RBAC and ABAC in terms of the way in which they are managed within companies, we see a number of peculiarities. Firstly, the static nature of RBAC, which was mentioned earlier, makes it difficult to place users in context (Jin, Krishnan, et al., 2012). The context of a user consists of crucial factors that limit access to available resources. From an organisational perspective, this means that it is more challenging to give the user the minimum access needed to do their job. Similarly, RBAC is often described as a non-discretionary control that ensures that users are inevitably constrained by the organisation's protection policies (D. Ferraiolo et al., 1995). In contrast, ABAC uses centralised authorisation policies that make it easier to give users the minimum access they need to do their jobs (Hu et al., 2014).

Secondly, from an administrative point of view, a deterministic model such as RBAC has an advantage over ABAC. A deterministic RBAC model is easier to understand, easier to visualise and more direct (D. Ferraiolo et al., 1995). This makes it easier for the administrator of the system to understand who has access to what at any given moment in time. ABAC is more difficult to understand because it is much more abstract. After all, you work with authorisation policies linked to attributes. However, this does mean that ABAC can be controlled from one central point (Hu et al., 2014). Finally, there is a difference in how access controls must be maintained. Since ABAC models use attributes and policies, they do not rely on a complex structure of roles, resources and locations on which RBAC depends. This makes ABAC models easier to maintain as opposed to RBAC (Hu et al., 2014). However, this does not mean that it is cheaper. The cost can increase in the management of subject attributes and additional system support.

3.4.3. Scalability

In addition to the general operation and maintenance of systems, scalability is an important requirement for modern systems (R. Sandhu et al., 2000). For many organisations, this means that they must already be thinking about possible future changes to the organisation during the implementation of a new system. In the case of IAM, many organisations have implemented RBAC because this method has been known for some time. (R. S. Sandhu et al., 1996). However, RBAC causes many problems within organisations in terms of scalability. For example, RBAC has a static character and does not use personalised access because it is role-based. (Kunz et al., 2019). Besides that, RBAC is also limited to the number of roles a person is able to have (R. Sandhu et al., 2000). As a result, companies have started to include more attributes in their IAM system in recent years. (Jin, Krishnan, et al., 2012). The use of attributes within RBAC provides a more scalable system and is known as role-centric attribute-based access control (RABAC) (Jin, Sandhu, et al., 2012). The next step would then be to switch completely to the implementation of ABAC. However, ABAC makes use of policy sets in which issues could occur. Tracking down these errors is a complex and time-consuming task (Vijayalakshmi and Jayalakshmi, 2021). Therefore, it would be a logical strategy for many organisations to first implement a RABAC system before fully switching to ABAC.

3.5. Zero-trust

As mentioned in section 2.4, an ongoing increase in the complexity of IAM systems has led to the development of a new model for cybersecurity known as ”zero-trust”. Research has shown several vulnerabilities in the existing systems of organisations. First, when an external intruder or malicious actor has gained access to a network, they can access a large part of the organisation. The cause of this is the failure to use segmentation or controls in the internal network (Chen et al., 2019). Secondly, the security level is as weak as the weakest device by using many different devices. (Shlapentokh-Rothman et al., 2020). Finally, log files are often stored locally so that intruders can access them and cover their tracks. Zero-trust could offer a solution for many of these vulnerabilities. However, there are currently mainly theoretical examples of zero-trust applications, and empirical data is still missing. In order to give a clear picture of the possibilities and weaknesses of zero-trust, it is approached from three angles: design, management and users.

3.5.1. Design

The design of a zero-trust implementation consists of several features and critical components. Research has shown several key features that researchers recognise as being essential. Firstly, researchers confirmed that in zero-trust, trust is dynamic and thus always wants to verify when access is requested. Second, the authentication and the enforcement of access policies are controlled by a central controller (Yao et al., 2020). The controller is responsible for accepting connection requests. Third, access is granted based on the access policies, which are defined with the use of the principle of least privilege (Campbell, 2020). Fourth, the principle of least privilege is applied to the whole network, which is segmented into macro-areas to minimise the risk of movement within the network (Rose et al., 2020). Finally, all network usage and logging are monitored, which enables ensuring dynamic responses (Rose et al., 2020). All the features result in limited visibility and traceability of the resources on the network.

Besides the most important features, researchers have also described a number of key components of zero-trust (Buck et al., 2021. The five components described in the literature should ensure that the process flows of zero-trust are achieved. First of all, a single packet authentication (Omar and Abdelaziz, 2020). Single packet authentication ensures that the central controller can discard an access request before a connection has been made to the network. Second, all communication between the components on the network must be encrypted by means of mutual transport layer security. (Omar and Abdelaziz, 2020). The encryption provides a two-way encryption so that only the two communicating components can verify each other. Third, through the use of dynamic firewall, only the approved movements are allowed through (P. Kumar et al., 2019). Fourth, the users on the network and all devices must be validated (P. Kumar et al., 2019). Totally, all use of the network will be isolated when access to the network is granted. (P. Kumar et al., 2019). In this way, all movement can be monitored.

The features and components mentioned indicate how a zero-trust model should theoretically be constructed in order to work correctly. However, for the time being, this is only substantiated theoretically and party examples are lacking. Several limitations and disadvantages are described in the literature. For instance, there is only talk of application within internal networks or other relatively small-scale networks. (Xiaojian et al., 2021). Yan and Wang (2020) even mention that zero-trust is not yet applicable within large-scale networks. Finally, various researchers also mention that the maintenance and implementation of zero-trust architectures and administration require many skilled employees. (Dhar and Bose, 2021).

3.5.2. Management

Besides the opportunities that the design of a zero-trust architecture offers, the implementation also impacts the management and the organisation. First, the implementation of zero-trust ensures a decrease in operational costs. (Cunningham and Pollard, 2017). By making access adjustments easy, network management costs will decrease. Second, because zero-trust offers increased network protection, the chance of a data breach is smaller and therefore, savings will be made in this area. Third, zero-trust allows the organisation to grow or shrink as the system is easily scalable. (P. Kumar et al., 2019). Finally, zero-trust makes use of trusted users and devices, which enables remote working in a safe manner (Osborn et al., 2016). Besides the advantages that zero-trust brings, implementing zero-trust does compromise the speed with which users connect to the network compared to traditional systems (Moubayed et al., 2019). On top of that, investing in new security solutions are difficult to quantify because they do not provide a direct return on investment (Weishäupl et al., 2018). However, it seems that the increase in security outweighs the disadvantages in almost all cases.

3.5.3. Users

Besides the technical and organisational benefits, the implementation of zero-trust also impacts the users. The implementation of zero-trust first reduces the attack surface and ensures constant monitoring. Both of these advantages may have disadvantages for the users of the system. However, the literature hardly focuses on the user's point of view. However, there is a survey by Gigamon that includes the user in the analysis. This shows that the implementation of zero-trust can lead to employees feeling that they are being monitored. (Gigamon, 2020). Thus, it could negatively influence the employee's willingness to adopt zero-trust. Moreover, this could also lead to legal problems because privacy rights could be violated by collecting new data.

3.6. Impact of COVID on cybersecurity

Finally, the impact of COVID-19 is also included in this study. There has been an increase in the number of cyberattacks in the last couple of years. One of the reasons for this change is the rapid digitisation of our environment. An all-time high of cyber attacks was reached during the COVID-19 pandemic due to the rapid change from offline to online work. When the COVID-19 pandemic started at the beginning of 2020, the virus spread rapidly around the world and changed the lives of billions of people. The pandemic resulted in hundreds of millions of people worldwide having to be quarantined. This also meant that the lives of all these people changed from a physical (offline) situation to a digital (online) one. This change directly led to an increase in the attack surface. The attack surface is the sum of all known and unknown vulnerabilities and all hardware, software and network components through which a cybercriminal can attack an organisation (Manadhata and Wing, 2010).

In addition to the enlarged attack surface, the rapid digitisation during the pandemic also led to an increased number of targets. For example, almost everyone had to work from home. This development is visible in the number of users of Zoom, a video communication platform, which grew from 10 million users in December 2019 to 200 million users at the end of March 2020 (Faraj et al., 2021). The increase in users meant an easier target for cybercriminals. The NCSC reported an increase in the use of human-targeted cyber-attacks in both 2020 and 2021 (NCSC, 2020a, NCSC, 2021). This increase is also evidenced by research into the different types of attacks in the UK, where it can be seen that during the pandemic in 86% of the attacks were using phishing and/or smishing (Lallie et al., 2021). Finally, organisations had to protect themselves against these types of attacks. This has led to rapid changes within organisations on the advice of the NCSC. The NCSC issued the advisory on 1 April 2020 due to a perceived increase in the number of cyber attacks (NCSC, 2020b).

3.7. Theoretical framework

It can be concluded from the literature review that technical, organisational and environmental variables influence the perceived usefulness of access controls. In order to present these variables from the theory and the relationships between them in a clear manner, it was decided to look at different frameworks that contain the same variables. This section will provide/give an overview of the of frameworks that form a basis for the framework that will ultimately be used in the research.

3.7.1. Technology-Organisational-Environmental (TOE) framework

The first framework that is considered is the TOE framework, the TOE framework was developed by Tornatzky and Fleischer (1990) to give insight into the adoption of IT within organisations. The framework uses three variables to provide a broad overview of the theoretical view on IT adoption. The three variables are technological, organisational and environmental, which means that IT adoption is examined from many angles. In addition, the framework is independent of industries and firm size. Thus, it provides a holistic view on the adoption of IT, the implementations and the challenges.

However, the TOE framework does not consist of the user's perception. A framework that also captures the attitude from the user is the TAM framework. Perceived usefulness is a variable that is central to the TAM framework. In the TAM framework, the desired ease of use and the perceived usefulness from an adoption intention are captured.

3.7.2. Technology Acceptance Model (TAM)

The TAM model is a widely used model for understanding IT adoption and usage processes (Gangwar et al., 2015). The model uses two concepts to explain user behaviour towards new computing technologies. The first concept is perceived usefulness, which describes the user's perception of increased job performance when using new technologies. This can also be understood as the extent to which the implemented technology meets the organisation's requirements. The second concept is perceived ease-of-use, which indicates whether the user also understands how the technology works. These two concepts lead to an attitude towards the adoption of new technologies.

3.7.3. TAM-TOE framework

Because the TAM framework does not include external factors Gangwar et al. (2015) merged the TOE and TAM framework in a study on determinants of cloud computing adoption. Research has shown that both the TAM model and the TOE framework are a valuable addition to the explanation of technology adoption (Gangwar et al., 2015). Because this research will capture the influences on both the ease of use and usefulness of the implementation of access controls in organisations, merging the two frameworks, like the TAM-TOE framework, will give more insight into the external influences on the eventual adoption of cloud computing.

This is why this research will look at the adoption of access control in organisations. Using the TAM-TOE framework, how access control is implemented is examined from different angles. In this way, statements can be made about the opportunities and vulnerabilities within the IAM of organisations. As shown in figure 3.3, the TAM-TOE framework described by Gangwar et al. (2015) consists of three external influences on usefulness and adoption. These external influences consist of ten sub-variables. The variables are based on the literature found by the researchers. In this research several sub-variables are added to the TAM-TOE, including Ambition, External threats and Willingness. These sub-variables are added due to their relevance for this research. Questions will be formulated based on this framework to provide a overview of organisations' IAM. In table 3.1 all thirteen variables are described and the related questions are shown.

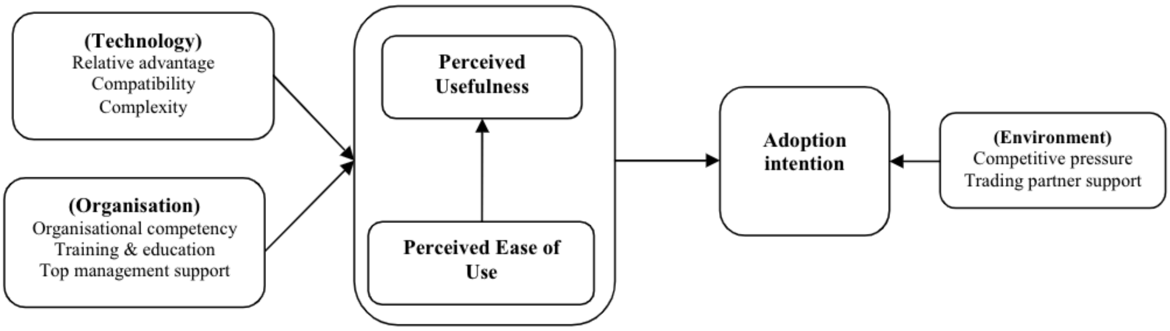


Figure 3.3: TAM-TOE framework (Gangwar et al., 2015)

On top of that, further research has shown that the TOE framework has already been applied in studies on the adoption of access controls (Törnebohm, 2019, Bradford et al., 2014, Lane and Marie, 2010). These studies clearly show the added value of using TOE. Also, TOE has a strong theoretical basis, a lot of empirical support, and a proven added value within the information security domain (Bradford et al., 2014). Like the TOE framework, the TAM framework is widely used in adopting IT innovations. The original version of TAM was first introduced in 1986 (Davis, 1985). There have been minor changes over the years, but the essence of the framework has always remained the same. The framework approaches the adoption of new technologies. Previous studies based on TAM have provided valuable insights into how workers make decisions regarding the adoption and use of new technologies (Venkatesh and Bala, 2008). However, TAM fails to include critical components such as security and threats (Wu, 2011). Thus, merging the two models better substantiate the results.

Category	Code	sub-category	Concepts	Questions
General information		Firm information		
		Participant information		(Q1.1, Q1.2, Q1.3)
Technical	1.1	Relative advantage	The degree to which a technological factor is perceived as providing greater benefit for firms' (costs of implementation, maintenance, scalability, governance)	(Q3.5)
	1.2.	Compatibility	The degree to which the innovation is perceived to be consistent with the potential users' existing values, previous experiences and requirements (requirements of firm/user)	(Q3.4, Q3.1, Q3.6)
	1.3	Complexity	Perceived degree of difficulty of understanding and using a system (time taken for maintenance, time for governance)	(Q3.3, Q3.7)
Organisational	2.1	Organisational competency (readiness)	Organisational current situation	(Q4.4, Q4.8, Q4.1)
	2.2	Top management	Top management's attitude towards the technology (long-term vision, commitment of resources, support)	(Q4.5, Q4.6)
	2.3	Training and education	Degree to which a company instructs its employees in using a tool in terms of quality and quantity (cyber security training, etc)	(Q4.2, Q4.3)
	2.4	Ambition	What is the long-term vision of the organisation	(Q4.7, Q6.1, Q6.2)
Environmental	3.1	Competitive pressure	The degree of pressure that the company feels from competitors within the industry (governmental pressure)	(Q5.1, Q5.2)
	3.2	Trading partner support	If third parties are involved, the way they manage their availability, effectiveness and efficiency is involved in the use of the control.	(Q2.2, Q5.3)
	3.3	External Threats	How coop with external threats	(Q5.4, Q5.5, Q5.6)
Perceived usefulness	4.1	Ease of use (employee)	Does employee understand the impact of using the access control and updating their passwords	(Q4.1, Q3.3)
	4.2	Usefulness (firm)	Does the access control work proporly	(Q3.5, Q3.6)
Adoption intention	5.1	Willingness	In what manner is the company willing to adopt new innovations/principles	(Q6.3, Q6.4)

Table 3.1: Defined variables and concepts

4 Methodology

4.1. Research approach

As defined in the introduction, the main research question is to investigate how organisations set up the IAM and which vulnerabilities, risks, challenges, and opportunities can be identified. This will require an in-depth analysis of the organisations' current IAM. Secondly, the research question indicates differences in access controls of organisations in comparison with characteristics of the organisations. This data used to analyse is empirical and can be collected via interviews. Moreover, the interviewee's experience is also captured in the interview to substantiate the results.

This research aims to explain, describe, and explore the characteristics of organisations in correlation to their IAM. The characteristics used in the research are the type of organisation, size, existence, profit/employee, merged or not, and role of the interviewee. Eventually, conclusions are drawn from the analysis and advice for improvements in the organisations' identity and access management is given. However, there is also a limitation to interviews in research. Designing an interview can be challenging on the validity, correlation and generalisation aspects. In the interview design phase, these limitations need to be considered. The data obtained from the interviews are used to create an overview (case) of each organisation their IAM. At the start of this research, a selection will be made of the potential organisations to be interviewed based on several criteria. By selecting these criteria, the different cases can be compared. Finally, the approach used in this study is also known as a multiple case studies approach.

4.1.1. Multiple case studies

The description of what a case study is is complex to explain. An intensive study on a person, a group of people or a unit is a simple explanation of the method (Tsang, 2013). In this research, a multiple case study approach will be used. Although the way the cases are collected can be the same as for a single case study, the way the results are analysed differs from a single case study. Multiple case studies can be used to clarify whether the findings are practical or not. By comparing different cases with each other, the researcher can make new findings of influences based on the contraries or similarities (Vannoni, 2015). The fact is that results based on a multiple case study are better substantiated and more reliable than single case studies (Tsang, 2013).

Several essential steps can be identified when using case studies. First, a clear case must be defined before any cases can be selected. When the cases have been defined and selected, the data can be collected for the relevant cases via desk research and interviews. Finally, the cases can be analysed and interpreted.

Defining the case

When conducting a case study, the first phase determines the case. The overarching topic in the case studies can be withdrawn from the most important theoretical problems and the existing literature (Stake, 1995). In this way, a case can be formed with a clear scope such as which organisations, type of data will be collected, and the research direction, collecting the data and analysing it (R. K. Yin, 1998). This study already has a straightforward research question, and cases (potential organisations) can be selected for the interviews.

Selecting the case
The second phase of a case study involves selecting the relevant cases(potential organisations). According to Stake (1995), the first criteria maximises learning from a single case. The sentence can also be reversed, which case gives us the most knowledge-based on our purpose. In addition, a maximum variation selecting strategy will be used to select as varied cases as possible within the specified boundaries. Critical cases will also be searched for to make generalised statements about the cases within the boundaries of the research (Shakir, 2002). Using two selection strategies makes it possible to make generalised statements within the boundaries of the research.

Information and data gathering
After the cases have been defined and selected, it is good to make a clear plan in advance for collecting the data. There are many different ways to obtain both quantitative and qualitative data. For example, the researcher can collect information based on interviews, desk research and expert consultations to make a case study. Data triangulation can be used to ensure the validity of the case study. Data triangulation means that data is collected from three sources in order to have more angles and thus increase validity (Triangulation, 2014).

Analysis and interpretation of the case studies
Finally, the created cases can be analysed, interpreted, and reported in the last phase. The analysis will be based on the main research question and sub-questions, and the results can thus be generalised within the boundaries set.

4.2. Research method

This section briefly explains the aforementioned methods and tools to answer the main research question and sub-questions. The research methods and tools are chosen based on the data needed for the research questions. Finally, the expected results are derived from the main research question and sub-questions.

The in-depth analysis includes both qualitative and quantitative analysis. Research has shown that the use of both qualitative and quantitative data has a significant contribution to creating knowledge because the content of the second data source would increase the validity of the findings (Hurmerinta-Peltomäki and Nummela, 2006). Besides increasing validity, researchers have argued that studies using these data types seem to gain an extensive and broader understanding of the topic. Another benefit of using both qualitative and quantitative methods in research is that the integration of the methods creates more confidence in the results and conclusions (O'Cathain et al., 2010). Moreover, Coyle and Williams (2011) state that some researchers need to use mixed methods to ensure findings and interpretations.

Performing a mixture of qualitative and quantitative data is the right fit for this research approach since the data will primarily consist of words, opinions, thoughts, feelings, and behaviour and includes numbers and statistics. The data will be collected via desk research and interviews. Interviews are conducted with the IT department of diverse organisations. The research focuses on the organisations' identity and access management and their implementation of access controls.

4.2.1. Qualitative Research Method

Qualitative data includes words, opinions, thoughts, feelings and behaviours. One of the advantages of using qualitative data is that it gives the researcher a detailed insight into specific cases, people or groups, and it can examine an organisation's underlying assumptions, values, and beliefs. On top of that, the data is collected by open-ended questions in interviews. Open-ended questions tend to give the respondents room for their interpretations, and thus it will show their priorities. The downside of using qualitative data is that it is impossible to make general statements, and it takes more time to analyse the data.

Desk research
In the first phase of the research, getting a clear picture of all the subject's information is essential. The first research method applied in this research is desk research. The research will be done through desk research and sources such as Scopus and WorldCat. The information found will be analysed and form the basis for both the interviews and the cases. In addition to forming a basis for the interviews, desk research will also investigate more information per case. For example, desk research will be used to gather annual reports of each case. The found documents will be analysed with the use of document analysis.

Document analysis
The second data source used in this research is document analysis, which consists of the documents found via desk research. Qualitative research often consists of a process of sorting, categorising, and synthesising multiple angles of a topic (Hodder, 1998). The resources for qualitative data consist mainly of written documents. Written documents are considered a rich source of data from which much can be learned (Love, 2003). With the use of software programs like ATLAS.ti, documents can be analysed and stored easily. Atlas.ti is a tool that helps with coding documents. The codes are linked to pieces of text from the found documents. The documents are analysed using keywords. The words used are; security OR cyber OR risk OR threat. The coding used in this research is linked to the different variables from the CMMI model (appendix C).

Semi-structured interview
The last research method in this research is semi-structured interviews. In-depth research will be conducted through interviews with experts in the field of IAM and IT employees from selected organisations. These interviews will be structured based on a semi-structured interview. Research has shown that interviews give more insight into the subject and a clearer contextual picture because they are interactive (Whiting, 2008). However, there can be a difference in the way interviews are conducted. A face-to-face interview would provide significantly more valuable information than a telephone interview (Sturges and Hanrahan, 2004). Given the situation surrounding COVID-19, this report will use both face-to-face and digital face-to-face interviews. The results from the interviews and the results from the desk research result in the case studies. The case studies form the starting point for answering the sub-questions and, ultimately, the main research question.

4.2.2. Quantitative Research Method

The use of quantitative data has a few significant advantages over qualitative data. First of all, the data collection allows determining the correlation between the organisation's identity and access management and different factors (e.g. profit, revenue, #employees and #roles). Secondly, much more information can be gathered and analysed at once using quantitative data. At last, the amount of time spent analysing the data is much less. A drawback can be found in the lack of depth in the data. With quantitative data, the reasoning, context, emotions, or feelings are missing, which results in fewer drafts. For this reason, qualitative data is used also used in this research.

4.3. Research design

In this research, both quantitative and qualitative research methods are used. In this section, the design of the research is elaborated on. Parts of the research design are the data collection method, preparation, and analysis.

4.3.1. Data collection method

To answer the research questions, data will have to be collected. Data triangulation will be used for each case in this research, which means three data sources are collected per case. The use of data triangulation ensures that more angles are used and thus increases the validity of the case study (Triangulation, 2014). The three data sources used are desk research, document analysis and interviews.

The first data source used in this research is desk research. With the use of desk research, an overview is given on the topic of this research. It will discover what previous researchers have found on the topic and what remains unknown. Besides extracting previous research from source, desk research also form a basis for the cases. The initial data about every organisation is extracted and prepared for analysis. The second data source used in this research is document analysis, as explained in the research method in section 4.2.1. In this research, relevant written documents of the organisations are selected when the document contained at least ten of the following words or a combination of them; security OR cyber OR risk OR threat. The documents are analysed and stored in Atlas.ti, which is a tool that helps with the coding of the documents. The last data source used is a semi-structured interview. With the use of document analysis, historical data and future ambitions of the cases are captured. This information can be of great value to analyse the effects, best practices and ambition of identity and access management. In section 4.3.1 the research design is elaborated on.

Semi-structured interviews design

As a final data source, semi-structured interviews are used to gain insight into the IAM of organisations. An interview protocol is written based on the formulated concepts in section 3.1. The protocol that has been created is aimed at an IT/security employee within a financial services organisation and can be found in Appendix A. By using an interview protocol, the interviewer ensures that the same data is collected from each interview and that the conversation is conducted in the right way (Jacob and Furgerson, 2012). The validation of the protocol was tested with the use of a test interview. The first interview was used to ensure that the interview had the right questions and structure. Doing a test interview makes it possible to check whether the current protocol is working correctly and if any adjustments can be made. Thus, conducting a test interview contributes to the internal validity of the study (Diefenbach, 2009).

Given the COVID-19 situation, all interviews were conducted via Microsoft Teams. Microsoft Teams is software that allows video calls to be made. The participants could choose whether they wanted to use their camera or only have an audio conversation to ensure their privacy. Before the interview was conducted, the participants were given a consent form, shown in Appendix B. After the consent, the interview was started and immediately recorded and transcribed. The researcher used the recordings and transcriptions for the sole purpose of this study. Given the fact that a large number of the participants were of Dutch origin, it was decided to conduct both Dutch and English interviews. A database of the case studies was built up during this research in order to keep an overview of which interviews and documents were used. The use of a database provides a clear structure for the data analysis and allows readers to have an overview of the data used. This increases the reliability of this research (R. K. Yin, 2009). An overview of the data used in this research is shown in table 5.1. Because of the confidentiality of this research, all cases, interviewees and documents have been anonymised.

In addition to the semi-structured interviews with organisations within the financial services sector, interviews are also conducted with IAM experts. These expert interviews are conducted to validate the results found. Because experts have knowledge of the subject in different contexts, they can provide valuable insights (Meuser and Nagel, 2009). The experts can confirm the results found and provide further explanations. However, they may also indicate that the findings are less known or even unknown to them. This may lead to the invalidation of some results or, on the contrary, to new insights for the expert.

4.3.2. Data preparation

After the data has been collected, it will have to be prepared before analysis can be performed. For both desk research and document analysis, the data has already been collected to make it directly analysable. However, the interviews must first be quantified to make them analysable. The interview questions are formulated using a framework as shown in section 4.3.1. To quantify the answers to the interview questions, the Capability Maturity Model Integration (CMMI) is applied, which is a well-known scale to measure the stage in which an organisation is using new technologies (SEI, 2002).

Capability maturity model integration

The Capability Maturity Model (CMM) was first introduced by the researcher W.S. Humphrey in 1987 working for the Software Engineering Institution. Later, the model was published in his 1988 book, Managing the software process (Humphrey, 1988). The model shows how an organisation has currently implemented its process by means of assessments and extensive feedback. In addition, the model is also capable of identifying critical issues and improvements from the current process maturity. In the next few years, improved versions of the CMM were introduced by the Software Engineering Institute (Paulk et al., 1993). The improvements were mainly focused on making the model more usable by removing words like ”effective” or changing the names of some key processes. Eventually, a successor model was designed called the Capability Maturity Model Integration. This model, unlike CMM, also takes the results into account when approaching the maturity level of an organisation (SEI, 2002). An overview of the CMMI as used in this research is shown in figure 4.1.

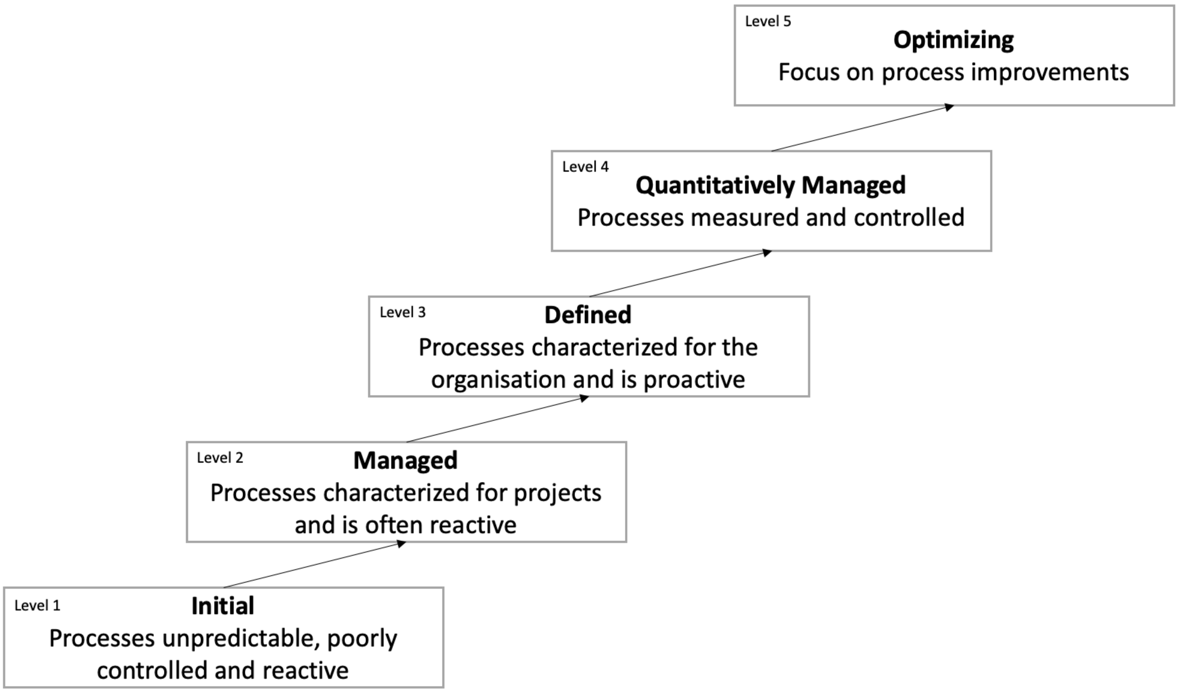

Level 5
Optimizing
Focus on process improvements
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organisation and is proactive
Level 2
Managed
Processes characterized for projects and is often reactive
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Figure 4.1: Capability Maturity Model Integration

As shown in figure 4.1 five stages are defined to capture the organisations’ level of maturity. First, the CMMI must be converted and paraphrased for this research. Second, a standard of each stage for every question should be made prior to the interviews. Thus, the researcher applies the same standard for all interviews. This ensures the validity of the results of all interviews. At last, the interviewee’s answers should be placed in one of the five stages before the interviews can be analysed. In appendix A an overview of the questions and all the descriptions of the stages is shown in appendix C.

4.3.3. Data analysis

After the data is collected and prepared, the analysis can be conducted. Data analysis consists of examining, categorising and tabulating the results (R. Yin, 2003). The findings from the collected data are analysed in two separate phases. First, a within-case analysis is conducted to draw a conclusion from every case. After which, cross-case analysis will show findings from comparing multiple cases. Finally, the results are compared by means of the theoretical model to answer the research questions.

Within-case analysis

The first analysis that will be carried out is of the case itself. All found documents and the interview will be used for this purpose. First, the documents are processed in ATLAS.ti using pre-determined and emergent codes. Next, the concepts are labelled, and with the use of open coding, similar findings are grouped (Strauss and Corbin, 1990). From the proposed framework in section 3.7, five categories could be defined, namely technical, organisational, environmental, usefulness and adoption intention. Together with the information found and the interview, the document analysis can be analysed. The within-case analysis gives an overview of the IAM system of the interviewed organisation, their challenges and ambition. Thus, conclusions can be drawn for each individual case, the phenomena found can then be compared, and patterns can be found across all cases (Eisenhardt, 1989).

Cross-case analysis

After each case has been analysed, a cross-case analysis can be carried out. For this purpose, axial coding is used to find relationships between the individual cases (Strauss and Corbin, 1990). By means of axial coding, categories and their relationships with their subcategories are tested based on the data. In this way, the hypotheses can be confirmed again and again with the collected data. The strength of using cross-case analysis is that the data is viewed and analysed from multiple perspectives. This allows conclusions and findings to be drawn that were not clear in a single case. The use of cross-case analysis, therefore, leads to increased reliability of the research (Strauss and Corbin, 1990). However, there is also a risk in using this method. The research can become long-winded and unstructured, which makes it difficult for the reader to understand (R. K. Yin, 1981. This risk will be avoided by using visualisations and maintaining the same structure between individual cases.

5
Data analysis

After collecting the data, a data analysis will be carried out. The analysis is divided into two parts as described in chapter 4. First, each independent case will be analysed using the maturity model based on the framework explained in section 3.7. Subsequently, the cross-case analysis will be carried out in which the data is analysed and compared with the help of the maturity framework. Yin (1982) describes in his paper that one of the risks of analysing case studies is it becoming a long and unstructured story. This will be dealt with with the use visualisations together with a separate sections. An overview of the ten interviews and their characteristics is shown in table 5.1. The characteristics of the cases are type of organisation, size, existence, profit/employee, merged or not and role of interviewee.

Case nr.	Type	Size	Existence	Profit /employee	Merged	Role
Case A	Insurer	Large (10.000+)	>30	€40 - €80k	No	First-line
Case B	Insurer	Medium (2.000 – 10.000)	5 to 30	€0 - €40k	Yes	First-line
Case C	Bank	Medium (2.000 – 10.000)	5 to 30	€40 - €80k	Yes	Team leader
Case D	Insurer	Small (0 – 2.000)	5 to 30	€40 - €80k	Yes	Team leader
Case E	Insurer	Large (10.000+)	5 to 30	€0 - €40k	Yes	Middle management
Case F	Bank	Medium (2.000 – 10.000)	>30	€80k+	No	Team leader
Case G	Insurer	Small (0 – 2.000)	5 to 30	€80k+	Yes	Middle management
Case H	Payroll	Small (0 – 2.000)	<5	€0 - €40k	No	Middle management
Case I	Insurer & Bank	Large (10.000+)	>30	€80k+	No	First-line
Case J	Asset manager	Small (0 – 2.000)	>30	€80k+	No	Middle management

Table 5.1: Overview cases and characteristics

5.1. Within cases analysis

This sub-chapter provides ten within-case analyses to overview each case's current situation on IAM. Each case is introduced with a few characteristics, followed by a spider chart of the different parameters' maturity levels compared with the average maturity level found. The values displayed in the spider webs refer to the maturity levels of each associated variable which are elaborated on in appendix C. Furthermore, the challenges faced by financial institutions regarding implementing their IAM are elaborated on. Finally, a more in-depth analysis is shown, structured on five aspects: technological, organisational, environmental, perceived usefulness and adoption intention. The in-depth analyses include a justification of the maturity levels found for each variable.

5.1.1. Case A

Case A is a relatively large insurer in the Netherlands that has been in existence for more than 30 years. Figure 5.1 gives an overview of the general characteristics and the IAM maturity levels of case A. The overall maturity level of case A is lower than the industry average.

Case A - Characteristics

Type of financial institution	Insurer
Size of the company	Large (10.000+)
Existence	>30 years
Net income/employee	€40 - €80k
Merged	No
Document analysed	Annual report 2020
Management level	First-line

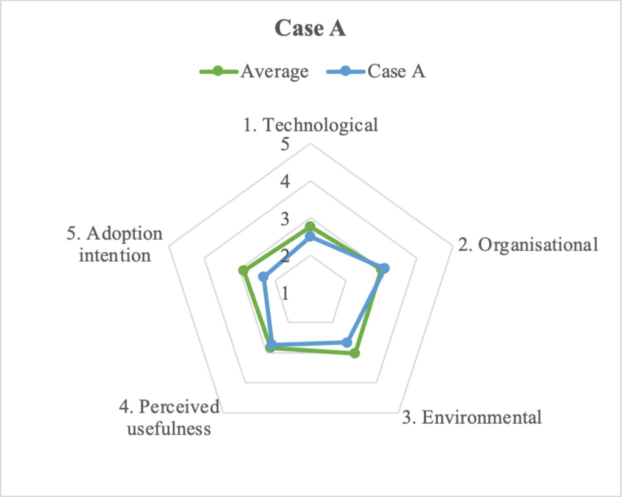


Figure 5.1: Results case A

Context - Case A appointed a new CISO several years ago who wants to make great strides in improving the IAM system. One of the reasons for this is a warning from the regulator a few years ago. As a result, they have started implementing Sailpoint in recent years. However, the Dutch branch of the organisation was already ahead of the international branches when it came to IAM, so in the Netherlands, the 'old' system, SecureID, is still used.

Technological - Case A has been using a role-based model for years. However, case A noticed that the model did not scale well, and the interviewee even talked about an explosion in the number of roles. The model worked well for case A but has become a complex overload of roles. In terms of automatic processes, case A also lags behind the trend and still does much manual work. On top of that, the lack of knowledge and incorrect distribution of responsibilities have a significant impact on the renewal of the systems. Consequently, since the arrival of the new CISO, steps have been taken toward an ABAC model.

Organisational - Case A's system fits well with its current organisational structure. They make use of a fundamental role that gives everyone access to the basic applications and data of the organisation. Besides that, case A uses a pyramid for role allocation where they start with the department, then the team and finally the function of each employee. The responsibility of assigning the roles lies with the managers. In case A, the managers often have insufficient knowledge of the system and take poor ownership. On top of that, the organisation provides too little training on applications/systems and cyber security, which is not compulsory. To conclude, a significant lack of knowledge is one of the main organisational problems within case A. However, the focus within case A is currently on improving that: *"The priority of information security is high, and because of this, you can clearly see that we are now busy improving the maturity of the system on a worldwide level, and NL is also benefiting from this."* (interviewee A).

Environmental - The way case A deals with its environment is quite reserved. There are no or hardly any discussions with companies within the sector, and they mainly lean on their Security Operation Centre (SOC) when it comes to external threats. The regulator in the Netherlands, the DNB, has indicated that the maturity level of case A was insufficient. This has created a clear incentive for improvement. Finally, interviewee A explicitly mentioned that they are aware of new technologies for automating their processes.

Perceived usefulness - The role-based model that case A uses fits the organisational structure well. However, the interviewee did indicate that the system is still unclear to many employees and therefore does not work optimally. In addition, the interviewee mentioned several times that much manual work is involved. Therefore, the automation of several processes has one of the highest priorities.

Adoption intention - In terms of willingness to implement innovations, case A lags behind the industry average. Their focus is on improving the existing systems rather than implementing new ones. Interviewee A said they inspect their surroundings in order to know what the trends are and what their competitors are implementing. In addition, the zero-trust principle and its implementation are not known to the interviewee. However, case A currently has the ambition to implement network segmentation, improve the knowledge of the employees and move away from manual work. Nevertheless, interviewee A indicated that much needed to change for this to happen; *"The culture within the organisation needs to change and many people are of the old school which makes change difficult."*.

5.1.2. Case B

Case B is a relatively medium insurer in the Netherlands that has been in existence for 5 to 30 years. Figure 5.2 gives an overview of the general characteristics and the IAM maturity levels of case B. The overall maturity level of case B is lower than the industry average.

Case B - Characteristics

Type of financial institution	Insurer
Size of the company	Medium (2.000 - 10.000)
Existence	5 - 30 years
Net income/employee	€0 - €40k
Merged	Yes
Document analysed	Annual report 2020
Management level	First-line

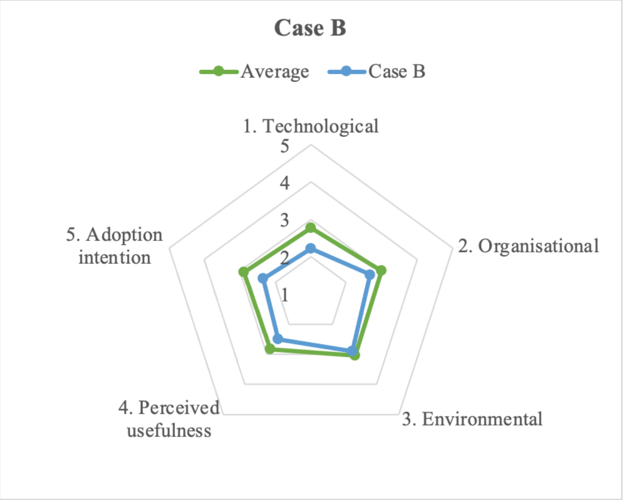


Figure 5.2: Results case B

Context - The organisation consists of multiple sub-organisation that need to be connected through the system. Case B uses Sailpoint and has linked all critical applications to it. The main reason for choosing Sailpoint is because of its automation capabilities.

Technological - One of the particularities of case B is the use of a partially discretionary access control (DAC) model. Since the existing model is compliant and fits well with the organisational structure, it was decided to keep it partly discretionary. Thus, they have a lower technological score than the industry average due to the vulnerabilities of a DAC model. However, they also realised that the system should be improved soon using an RBAC system. So they are taking concrete steps toward the implementation of RBAC. One of the challenges for case B is to create an overarching fundamental role between the sub-organisations.

Organisational - In case B, the managers are responsible for requesting rights for their teams. They do both the requesting and the checking of the rights. In addition, they are also responsible for transferring knowledge of the rights allocation process to their employees. This leads to problems when the managers have too little knowledge about the process and the impact of errors. The annual rights review process is a lengthy, step-by-step process in which they must check the rights of each employee. The employees are happy with the system, but a move to Single Sign-On (SSO) would make it easier. Another problem is the way in which employees are educated: *”There is still a lot to be done here because there are no more than a few voluntary training courses that can be followed. We want to change this in the near future, and there will be mandatory training for those with more authorisations within the organisation.”* (interviewee B). The management of case B takes the subject very seriously, but there is a lack of commitment. For example, a clear strategy with IT as a lead is not present. Interviewee B also indicated that this is often because business processes take precedence over cyber security. In addition, the knowledge of top management also plays a role in prioritisation.

Environmental - As an organisation, case B is part of an alliance in which periodic discussions take place to exchange information on cyber security. However, apart from the periodic talks, there are no moments when information is exchanged. Case B is an insurer who plays a central role in society and is under strict supervision. The pressure from the supervisory authority is felt, but this only forms the minimum above which they must be. Most of the improvements and protections they implement are made because they want to protect themselves better against the outside world. Interviewee B also mentioned that they try to do this by giving people more knowledge through campaigns. However, these courses are not compulsory training courses, and people have to learn them on their initiative.

Perceived usefulness - The model of case B is currently used for authorisations separate from each sub-organisation. However, even for a discretionary model, it does not remain easy to grant authorisations spread across different sub-organisations. From an employee perspective, the model is easy to understand. Nevertheless, many employees within case B have too little knowledge. The logical step to implementing an RBAC model is made complicated due to the same two problems. Thus, case B has to change more than just the system.

Adoption intention - The main improvements that case B wants to implement in the coming years are the implementation of RBAC, increasing the number of controls in the system, automation of processes and increasing knowledge within the organisation. However, there is a lack of support from management in making choices. This leads to few innovations and therefore a lower adoption intention maturity score. Besides that, interviewee B was familiar with zero-trust and its implementation. However, it was clearly stated that the infrastructure is not yet ready for this. First, the innovations mentioned earlier will be implemented. The main challenges for case B are the lack of involvement and knowledge within the organisation. By growing in this, the team of interviewee B can focus more on directing the system instead of only working on the operational processes. This will result in more time and attention for innovating the systems.

5.1.3. Case C

Case C is a relatively medium (online) bank in the Netherlands that has been in existence for 5 to 30 years. Figure 5.3 gives an overview of the general characteristics and the IAM maturity levels of case C. The overall maturity level of case C is approximately the industry average.

Case C - Characteristics

Type of financial institution	Bank
Size of the company	Medium (2.000 - 10.000)
Existence	5 - 30 years
Net income/employee	€40 - €80k
Merged	Yes
Document analysed	Annual report 2020
Management level	Team leader

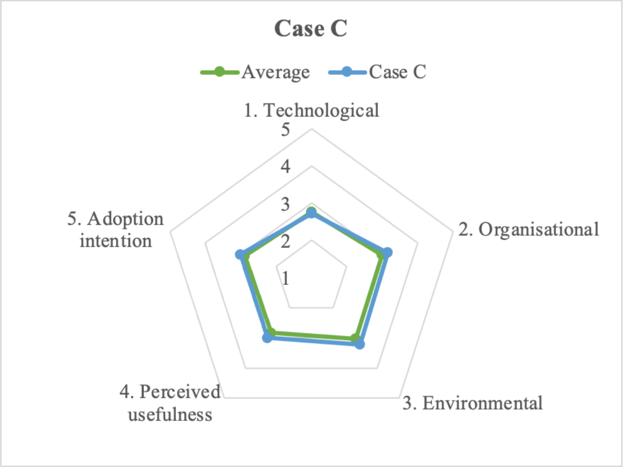


Figure 5.3: Results case C

Context - Case C is a bank that has merged with another bank in recent years. This has led to many complications in the area of IAM. Merging two different systems with different labels, authorisations and applications often causes many problems. On the other hand, merging two entities often increases the number of FTEs working on IAM. In this way, more significant steps can be taken.

Technological - Within the merged organisations of case C, they use RBAC. Interviewee C indicated that the systems showed their static nature during the merge. When the two entities merged, both systems had to merge as well. Initially, this caused many problems because the data could not be adapted appropriately into the system of the leading bank. As a result, much information became available to everyone because the system could not link it to existing users. As a result, case C directly linked an ambition to this shortcoming, namely the use of ABAC in more places in the organisation. Currently, case C mainly focuses on improving their existing system and solving problems due to the merge.

Organisational - In terms of organisation, case C is slightly ahead of the industry average. Firstly, top management has sufficient support and financial resources to set up the systems correctly. Secondly, case C is aware of the education they have to give to employees. As a result, they have several learnings, and the month of October is used as a cyber month. Finally, the existing system fits in well with the organisational structure of case C. The use of an RBAC model provides a clear overview, and large groups can be served with it. However, the step towards an ABAC model for the critical systems would fit in better with the desired security level.

Environmental - Within the team of case C, there is no direct contact with other organisations about the use of IAM. However, the interviewee did indicate that, as a bank, they are part of an alliance in which information about external threats and vulnerabilities is shared. On top of that, as an international bank, they have to comply with more rules and regulations. These guidelines are slightly different from the DNBs, so they often have to be more compliant to pass the requirements. This way, case C is aware of the policies of their surroundings. In addition, interviewee C indicated that they are constantly looking for innovations around them because there are more risks involved in being an entirely online bank.

Perceived usefulness - The model that case C uses is currently working well, and the interviewee indicated that, for the time being, the RBAC model fits well to the organisation's size. The merging of the two organisations has resulted in little room for innovation, and the focus is on improving and controlling the existing systems.

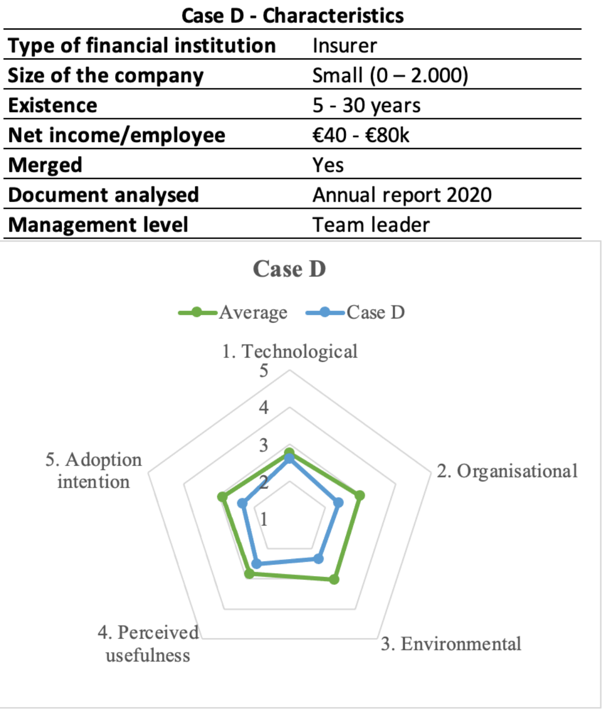
Adoption intention - One of the things that came up several times was that the merger of the two organisations meant a decrease in innovation. The interviewee indicated that the highest priority was to get the systems to work well together first. Next, steps can be taken to the innovation of the systems. However, the interviewee described their organisation as a fintech that has to grow along with the ever-changing environment. Because of this attitude, case C still has an average adoption intention score. In addition, the interviewee was familiar with zero-trust but immediately indicated that knowledge is a limiting factor in the growth of IAM within the organisation. A lot would have to change within Case C to implement zero-trust.

5.1.4. Case D

Case D is a relatively medium (health) insurer in the Netherlands that has been in existence for 5 to 30 years. Figure 5.4 gives an overview of the general characteristics and the IAM maturity levels of case D. The overall maturity level of case D is below the industry average.

Context - The health insurance company has been using an RBAC model for years, with the use of Sailpoint. However, case D has noticed that it scales a little less sufficiently nowadays due to the static nature of RBAC in a dynamic world. This has led to the ambition to move towards an ABAC model. The interviewee indicates that this is an intensive process and, therefore, not so easy. On top of that, the interviewee mentioned that the team currently has a mere reactive character and does not take the lead in innovations.

Technological - As mentioned, case D makes use of an RBAC model. Authorisation granting is done via an authorisation matrix and is mainly automated. Due to the dynamic nature of the organisation, the model will eventually be improved to an ABAC model. Nevertheless, interviewee D mentioned: *"We are currently in the early stages of an ABAC."*.



Case D - Characteristics

Type of financial institution	Insurer
Size of the company	Small (0 – 2.000)
Existence	5 - 30 years
Net income/employee	€40 - €80k
Merged	Yes
Document analysed	Annual report 2020
Management level	Team leader

Figure 5.4: Results case D

Organisational - The managers assign the authorisations within the organisation through profiles. The IAM team and the managers set up the authorisation profiles, and the profiles will be automatically assigned to employees. The manager himself can assign additional authorisations to his employees within each profile. However, the managers of case D often have neither the interest nor the knowledge of what the impact is of incorrectly granting authorisations. Interviewee D indicated that there is still a lot to be gained here.

Unfortunately, the top management of case D does not pay much attention to IAM. The interviewee described it as follows: *"They will not immediately think that IAM is the essential thing, they rather see IT as water coming out of the tap"*. In addition, the interviewee indicated that they should have a facilitating role while they now also have complete responsibility for both the system and allocation of roles.

Environmental - Looking at the attitude towards the environment of case D, it appears that they are mainly focused on themselves and improving the existing processes. Interviewee D indicated that communication with the outside world could be improved. In addition, as a health insurer, they have to comply with quite a few regulations from the government and supervisors. The interviewee indicated that this often feels like an obligation and significantly influences how they arrange things. In case D, the supervisors provide the proper pressure to keep improving.

Perceived usefulness - Interviewee D indicates that employees often have little knowledge of the systems at the moment and therefore experience it as problematic. In addition, the implemented model is now too static for the organisation. Therefore, the step towards a more dynamic model should occur in the near future. However, concrete steps have been taken to grow in the last few months.

Adoption intention - The focus of case D is currently on the use of ABAC and Azure, which should offer many advantages, also from a risk-reducing behaviour point of view. In addition, they have learned a lot from the arrival of COVID-19 in the field of remote working and trusted devices, and here too, steps still need to be taken. Since case D is mainly focused on improving their current system and not keep an eye on their surroundings, they have a lower adoption intention score. Finally, the interviewee said that zero-trust is not a topic at the moment within their team but that it is on the agenda for the near future.

5.1.5. Case E

Case E is a relatively large insurer in the Netherlands that has been in existence for 5 to 30 years. Figure 5.5 gives an overview of the general characteristics and the IAM maturity levels of case E. The overall maturity level of case E is a bit above the industry average.

Case E - Characteristics

Type of financial institution	Insurer
Size of the company	Large (10.000+)
Existence	5 - 30 years
Net income/employee	€0 - €40k
Merged	Yes
Document analysed	Annual report 2020
Management level	Middle management

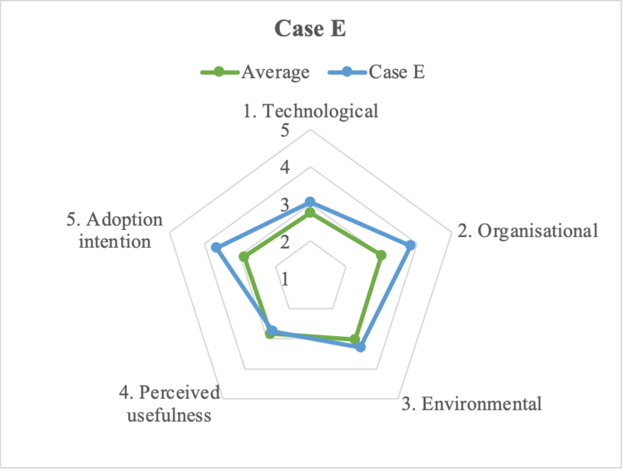


Figure 5.5: Results case E

Context - Case E is an insurer that has focused on digitalising in recent years. The changing world and the tightening of laws and regulations are the reason for this. In addition, Case E wants to become more trustworthy, more integer, more secure and more ethical for its customers.

Technological - Interviewee E indicated that the step to working fully online comes with many challenges. As a result, case E is in the process of creating an entirely new architecture. This leads to the fact that the systems are not working correctly, creating uncertainties. At the moment, case E uses an RBAC system which consists of a relatively large amount of manual work. The interviewee indicated that they will automate as many processes as possible in the near future, and there will be a shift towards ABAC. The ultimate goal of digitalising case E is to connect more applications and devices and become more flexible, secure and scalable.

Organisational - Within Case E, a lot has changed in recent years. In the past, management paid little attention to cyber security and nowadays, security is seen as a lead within the organisation's strategy. This means that with every innovation, thought is given to the impact on the cyber security level. A clear strategy for cyber security has also been included in the roadmap of case E, and financial resources are available to achieve these goals. However, interviewee E did indicate that there is still a gap in the knowledge of employees. At the moment, there are no compulsory training courses for this, but it is on the roadmap to be implemented soon. Next, the managers are responsible for granting the authorisation within case E. In this process, HR leads and gives the employees a basic set of rights and can assign the managers the roles they need for their job. However, almost all of these processes should be automated, and the authorisations cannot just be a copy of another person. Finally, the interviewee indicated that they would like to keep the focus on setting up the basis properly: *"I have concerns about the fact that we think we are focusing mainly on new technologies and we are leaving the basis for what it is"*.

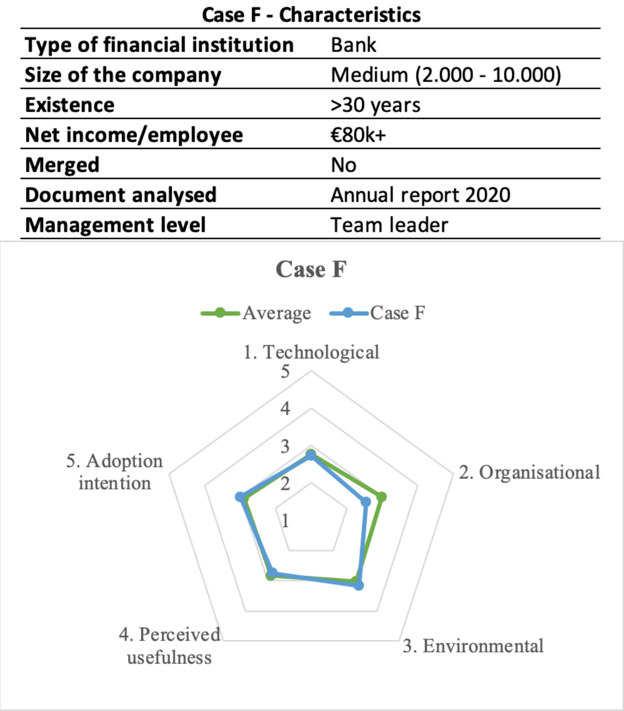
Environmental - There is a transparent exchange of information between sector colleagues of case E. This is mainly in the operational area of threat management. Various groups have also been organised for this purpose by third parties. In addition, the government always plays a role in legislation and regulations. However, this is more of a minimum requirement for case E than a real motivator of innovations. Finally, case E keeps a close eye on their environment. The interviewee indicated that they are well aware of the dangers around them and actively respond to them.

Perceived usefulness - As already mentioned, case E is in the process of digitalising and renewing its architecture. However, the software they use is good and can also be used with the new architecture. Also, a lot of the processes within the software of case E that can be automated are automated. Therefore, the software currently fits the needs of case E well, but as mentioned by the interviewee, more processes should be automated.

Adoption intention - Looking at the adoption intention of case E, they are ahead of the industry average. Case E have plans to move towards a more fragmented network with self-sovereign identity (SSI). In addition, they will use third-party identity software to protect their sensitive data. They are aware of the new technologies around them and want to make use of them wherever possible. That is why they also hire external parties, because they focus entirely on improving the systems. However, they still retain ownership of the system and what innovations they want to implement. Finally, interviewee E indicated that zero-trust is embedded in their strategy. The interviewee described it as a spider web of sensors that automatically communicate with each other to detect deviant behaviour. Case E hopes to give employees and customers the smoothest possible experience with all these improvements.

5.1.6. Case F

Case F is a relatively medium bank in the Netherlands that has been in existence for more than 30 years. Figure 5.6 gives an overview of the general characteristics and the IAM maturity levels of case F. The overall maturity level of case F is a bit below the industry average.



Case F - Characteristics

Type of financial institution	Bank
Size of the company	Medium (2.000 - 10.000)
Existence	>30 years
Net income/employee	€80k+
Merged	No
Document analysed	Annual report 2020
Management level	Team leader

Figure 5.6: Results case F

Context - Case F is a bank that has been around for a long time in the Dutch market. At the moment, there is a renewal of the organisational structure. As a result, a lot will change soon in IAM on both an organisational and technical level. However, since case F has been through a few mergers before, they are used to some aggravations.

Technical - At the moment, case F mainly uses a model that is based on roles. As the organisational structure is modernised, case F will also improve their IAM. In the background, case F implements an ABAC model that uses the Azure active directory. The way in which roles are currently allocated is not scalable. Given that many roles within case F transcend teams, new roles have to be cre-

ated all the time. As a result, case F has al-
most as many roles as employees. Finally, interview F indicated that the focus for the coming period would mainly be on automating processes since the amount of manual work causes problems within the team.

Organisational - One of the points that interviewee F immediately mentioned was the lack of knowledge. Given the renewal of the organisational structure, it is crucial to have the knowledge to deal with this renewal. A solution would be that more training is given to create more knowledge within the team and the entire organisation. However, interviewee F immediately indicated that this was not a priority for the business. Then the interviewee added: *"We have poor contact with the business side of the organisation, and this causes many problems. We are a kind of island within the organisation"*. Finally, interviewee F also mentioned the way ownership was dealt with. Since the managers do not take ownership, there is much more pressure on the team. This leads to much reactive work within case F, where they would instead be engaged in innovations.

Environmental - Interviewee F indicated that they often exchange information with other organisations within the financial services industry. However, it is challenging to receive valuable information for IAM because it has an organisation-specific implementation. In the area of supervisors, stricter controls ensure more support within the organisation, according to interviewee F. Because supervisors provide a measurement moment, it is also essential for management that the systems work properly. Finally, the interviewee stated that they constantly monitor their environment. However, this falls within another team, and the interviewee could not tell too much about it.

Perceived usefulness - As mentioned earlier, case F is currently in the process of changing its organisational structure. This leads to problems in the use of the existing system. One of the examples of this problem is an increase in controls and administration, which many employees are not happy about. However, interviewee F mentioned that they had experienced several mergers and previously had a worse system. So although it is not yet ideal, steps are constantly being taken to improve the system.

Adoption intention - Within case F, they are focused on simplifying the system, creating more awareness, automating processes and using ABAC. However, the changes within the organisation do create problems in terms of innovation of systems. Given the changes within the organisation, interviewee F indicates that the points mentioned are now the focus. The use of zero-trust is therefore not included in the strategy. In addition, the interviewee also indicated that innovations often take a very long time because they have to go through many layers within the organisation.

5.1.7. Case G

Case G is a relatively small insurer in the Netherlands that has been in existence for 5 - 30 years, but due to mergers and acquisitions, the organisation is relatively new. Figure 5.7 gives an overview of the general characteristics and the IAM maturity levels of case G. The overall maturity level of case G is below the industry average.

Case G - Characteristics	
Type of financial institution	Insurer
Size of the company	Small (0 - 2.000)
Existence	5 - 30 years
Net income/employee	€80k+
Merged	Yes
Document analysed	Annual report 2020
Management level	Middle management

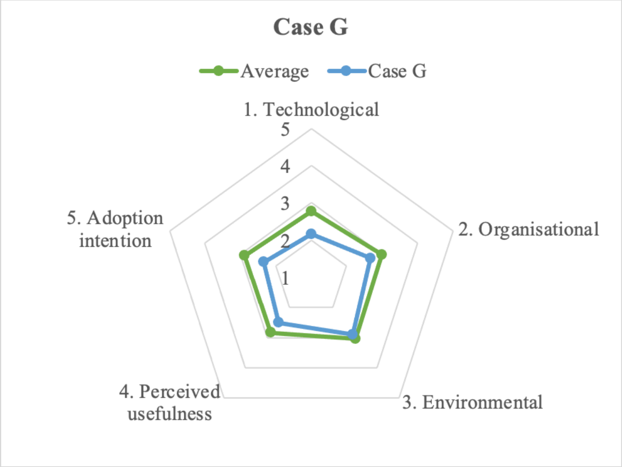


Figure 5.7: Results case G

Context - Case G is an insurer that has been acquired and merged several times in recent years. As a result, case G used to consist of more employees and is now scaling down. From the conversation with interviewee G, it also appeared that they might be scaling back even further in terms of employees in the future.

Technological - Although case G has gone through several mergers, they have always used an RBAC model. However, the interviewee immediately indicated that although they use RBAC, they still grant access manually because not everyone needs the same access. This leads to them constantly creating new roles and often having more roles in the system than there are employees. The managers within case G are responsible for granting the rights. To support them in this, case G has developed a dashboard that gives managers a quick overview of the rights of their employees. However, hardly any use is made of the dashboard. In addition, reminders to implement the controls have to be sent to the managers several times. Interviewee G indicated that automation of these processes is their ambition. Finally, the interviewee emphasised that information security is not seen as a lead within the innovations of case G.

Organisational - The software that case G uses for assigning rights is mainly intended for managers. The managers are responsible for granting and controlling the rights. One of the immediate problems that the interviewee mentioned was the number of rights that new employees receive. Because they give the rights of an existing profile to a new employee, he or she often has too many rights. On top of that, there is relatively little support for information security from the top management side of case G. The business has other interests and would like to have a system that is as simple and fast as possible. This leads to case G making roles more manageable and more generic, and as a result, employees often have too many rights. The ambition of case G is to automate more, but this requires financial resources that top management does not always make available. Finally, interviewee G also mentioned that perhaps the organisation's size would be scaled down further in the future. This means that the implemented tool may become too expensive and that they are looking at possible solutions. This also means that a decrease in the organisation's size will have consequences on the knowledge within the organisation.

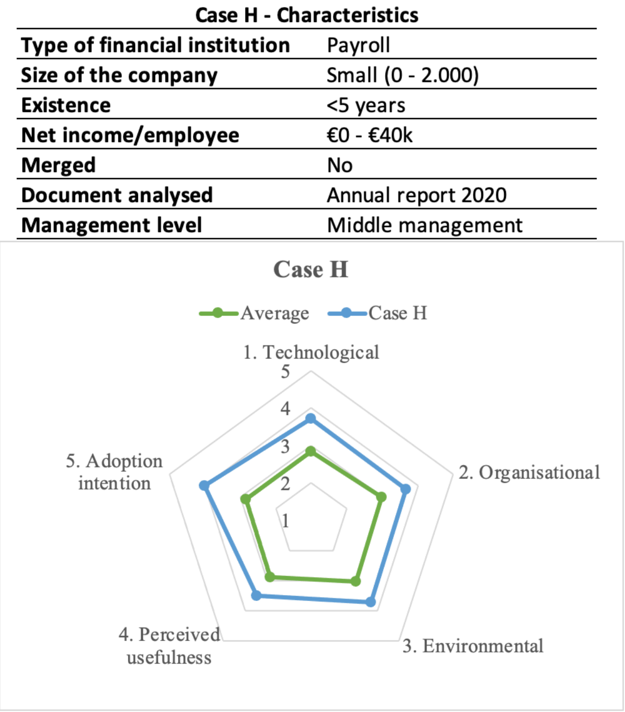
Environmental - Case G exchanges almost no information with organisations in their sector. In the past, this was done on the initiative of the software provider. However, given the poor support from the provider, case G stopped doing this. Luckily, this has changed because several organisations have started complaining, and the software provider has improved their support. In addition, case G is aware of what is happening around them and the risks. So they adjust systems based on audit results and are working on an initiative to increase employees' awareness. On top of that, they let external parties try to penetrate their systems to expose weaknesses.

Perceived usefulness - The system used within case G works appropriately. However, the problem is rather that many employees have too little knowledge and interest in how to use the software properly. This leads to many managers granting rights based on poorly defined profiles. As a result, the system does not work as well as it should. The solution lies mainly in the organisation's education rather than changing the system.

Adoption intention - As mentioned before, the focus of case G is mainly on automating the system, creating a more extensive set of controls, moving to the cloud and increasing the knowledge of the employees. However, interviewee G immediately indicated that this is difficult because it costs time and money, two practically non-existent things. Then the interviewee added: *"We are mainly busy keeping the business going, innovations are in second place because security is not the highest priority"*. This also means that the possible implementation of zero-trust is not on the agenda for case G.

5.1.8. Case H

Case H is a relatively small payroll company based worldwide and has been in existence for less than five years. Figure 5.8 gives an overview of the general characteristics and the IAM maturity levels of case H. The overall maturity level of case H is above the industry average.



Case H - Characteristics

Type of financial institution	Payroll
Size of the company	Small (0 - 2.000)
Existence	<5 years
Net income/employee	€0 - €40k
Merged	No
Document analysed	Annual report 2020
Management level	Middle management

Figure 5.8: Results case H

Context - Case H is a new organisation that is mainly focused on payroll software. This case is included because it has a lot of opposite characteristics since it is a new organisation. Besides that, the number of employees in case H quadrupled last year, which could lead to problems in the scalability of their IAM.

Technological - Case H uses Okta, in which they have implemented an RBAC model. The roles within the organisation are based on the metadata of the system, which consists of attributes of the employees. Case H created groups of people based on the metadata and then defined the rights of the roles based on this data. The system of case H is fully automated. Interviewee H indicated that when a person is hired, based on his attributes and function, he can immediately be added to a group and thus receive the correct authorisations. The system that case H designed is very scalable, and so far, it has not led to any problems with the number of new employees. Interviewee H added: *"When you link scalability to the number of people in the IAM team, you are doing it wrong"*.

Organisational - One of the biggest challenges of case H is the ever-changing organisation. The speed at which the organisation changes is constantly decreasing, but flexibility plays an important role. In addition, interviewee H indicated that they spend much time explaining to employees what IAM is and why they do it. The goal is to make employees understand that the IAM team is trying to simplify and speed up processes. According to interviewee H, the best way to create awareness is to let everyone be part of it and keep them informed of changes. Transparency is vital, according to interviewee H: *"We will always be clear on why we do something and how it will affect the employees in the future. We work a bit differently because we think they better understand it by giving everyone all the information behind any decision."*. Finally, in case H, there is much trust from top management.

According to interviewee H, top management is confident that this is necessary to improve the work whenever something has to change.

Environmental - Since case H is a new organisation, it immediately adapted to the existing laws and regulations. However, interviewee H indicated that they are now compliant in a new way that many authorities do not yet understand. This itself sometimes leads to simplified systems being implemented so that regulators understand. According to interviewee H, one reason is that regulators do not pay their employees enough and therefore do not employ the best people. In addition, case H keeps a close eye on his environment and systems. When the system thinks an employee is not the right one, the account will automatically be blocked. Only after the employee has identified himself and the manager has approved will the account be usable again. Interviewee H also added: *”Social engineering is mainly a people problem, and you need to have them invested in the action you take”.*

Perceived usefulness - One of the biggest challenges of case H is that they have no office and, therefore, no central point to start and build from. This also creates difficulties in security and device management. These difficulties have resulted in case H using the latest software from day one, which can deal with these problems. In addition, the system that case H now uses is highly scalable and, as much as possible, has been automated. As interviewee H himself said: *”At the moment, there is no reason to switch to other software because the system works extremely well”.*

Adoption intention - In terms of innovation, case H would still like to take steps towards multi-platforms. Currently, Case H only uses Apple products and is a single platform; a logical step would be to connect multiple platforms. On top of that, we are constantly looking for improvements within our systems. Because we already use the latest software, these are often only minor adjustments. Thus, the adoption intention of case H is much higher than the average. In addition, case H already works almost entirely from a zero-trust principle, but the problem here is that it is still very new to the platform. That means that it is tough to get every application to use zero-trust. Interviewee H concluded with *”I think it will take about two years when zero-trust becomes the standard”.*

5.1.9. Case I

Case I is a relatively large insurer and bank in the Netherlands and has been in existence for more than 30 years. Figure 5.9 gives an overview of the general characteristics and the IAM maturity levels of case I. The overall maturity level of case I is a bit above the industry average.

Case I - Characteristics

Type of financial institution	Insurer & bank
Size of the company	Large (10.000+)
Existence	>30 years
Net income/employee	€80k+
Merged	No
Document analysed	Annual report 2020
Management level	First-line

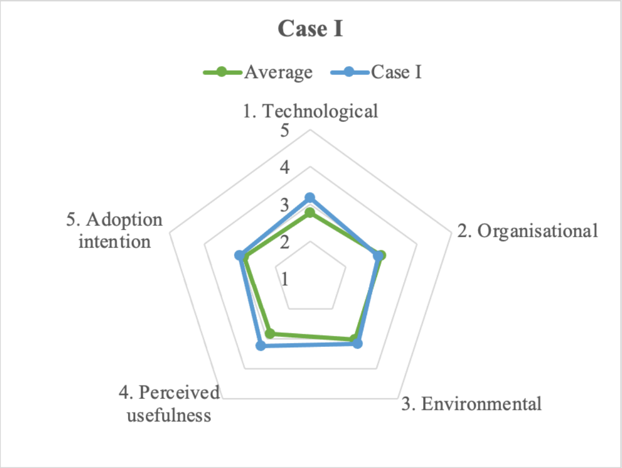


Figure 5.9: Results case I

Context - Case I is an insurance company and bank that was split off from another large organisation a long time ago. This means that quite a few changes have taken place in recent years. In addition, as an insurer, you often have to deal with outdated applications that are used for policies. Finally, there has been a new CISO who has been progressive in information security for a few years.

Technological - Case I is currently using several software programs and is in the process of making a significant switch to a new system. At the moment, they use an RBAC model that already uses attributes in some places in the system. In addition, many processes have already been automated, but different software makes it difficult to link everything together. The switch to a new program is necessary not to have a large on-prem system and maintain it. This frees up FTEs in the future and can be used for innovations. Before case I made the switch to the new software, it outsourced most of its IT. Interviewee I added: *”Management saw IT as water coming out of the tap”.* With the arrival of the new CISO, significant steps are being made in the right direction.

Organisational - In terms of organisation, case I suffer from a lack of knowledge and support. The knowledge deficit lies mainly in the users of the systems of case I. The employees often have too little knowledge and interest to know the impact of their behaviour within the system. In addition, there is also a lack of support from the top management of case I. This leads to the systems often being compliant instead of secure. The lack of support also leads to a shortage of financial resources and, therefore, a shortage of FTEs. For example, interviewee I mentioned the following: ”*According to our management we have to be compliant above all”.* The interviewee indicated that there has been a shortage of FTEs within the team for a long time.

Environmental - According to case I, exchanging experiences in IAM is not always beneficial. The interviewee indicated that IAM is mainly about yourself, so it is difficult to learn from the situation of other organisations. Furthermore, the interviewee indicated that they keep a close eye on their environment. They also keep a constant eye on their employees and almost always conduct campaigns to raise awareness. Finally, the interviewee mentioned that they are constantly working on any new software. Thus, they are now implementing the Azure active directory. Unfortunately, it remains difficult to constantly innovate, having a shortage of knowledge and FTEs.

Perceived usefulness - Case I is still using a lot of different software, and therefore they are not satisfied with the systems. A new system will be implemented in the near future, which will ensure that all applications can be linked to each other again. This will simplify the system and make it easier for employees to understand.

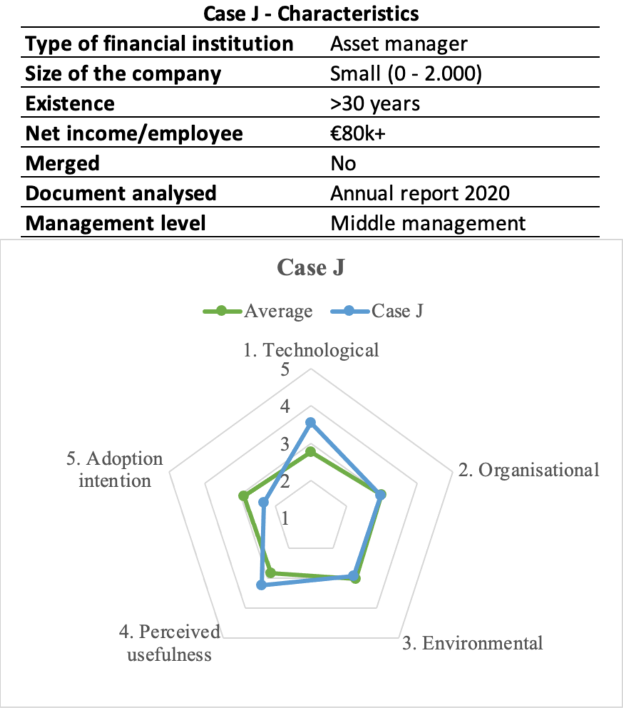
Adoption intention - Since the arrival of the new CISO, we have constantly been looking for new ways to improve the system. The focus is on using the new software, automating as many processes as possible and making employees more aware. Case I was also familiar with zero-trust but have not implemented it. Interviewee I explained zero-trust as a typical problem everyone understands but is still primarily based on academic knowledge. It is just a matter of time until there is enough practical experience with zero-trust.

5.1.10. Case J

Case J is a relatively small asset manager in the Netherlands and has been in existence for more than 30 years. Figure 5.10 gives an overview of the general characteristics and the IAM maturity levels of case J. The overall maturity level of case J is a bit above the industry average.

Context - Case J, in contrast to the other cases, is very small. Because they are so small, the amount of trust embedded in the organisation is very high. In addition, it is relatively more expensive for a small organisation to implement an IAM system. As a result, case J has outsourced its IAM to a third party.

Technological - Case J uses an RBAC system in which many processes have been automated. In addition, they use Azure to manage the functional groups. Because case J has its IAM system set up by an external party, they can pass on their wishes. In this way, the supplier of the system will meet the wishes of case J. This leads to them being able to innovate quickly. In addition, it is a small organisation, and changes can therefore be implemented relatively quickly.



Case J - Characteristics

Type of financial institution	Asset manager
Size of the company	Small (0 - 2.000)
Existence	>30 years
Net income/employee	€80k+
Merged	No
Document analysed	Annual report 2020
Management level	Middle management

Figure 5.10: Results case J

Organisational - From an organisational point of view, case J is not directly concerned with IAM because they purchase the service from an external party. This means that case J goes to the service supplier when they want to make adjustments to their IAM. This creates a significant dependency. In addition, interviewee J indicated that they had the same roles and rules within the organisation for years, and this static character fits well with RBAC. Finally, the interviewee approached that IAM has a high priority from the top management. This is reflected in the interviewee's complete support of his choices with his team.

Environmental - The way in which case J looks after its environment again lies primarily with the supplier of the system. The dependence on the supplier is noticeable in everything around the IAM system of case J. The interviewee emphasised again that if the supplier does not meet the requirements of case J, they can always switch to another party. This relationship ensures commitment on both sides.

Perceived usefulness - As described earlier, for case J, it is a matter of passing on their wishes to the supplier of the system. As a result, case J is very satisfied with using their IAM system. However, there is always room for improvement, and the interviewee indicated that it is essential for the organisation to stay sharp. Therefore, the interviewee always tries to challenge the supplier of the system to show why the implemented system still works properly.

Adoption intention - Again, case J is not directly innovating the systems. However, case J does have the opportunity to indicate to the supplier when they would like to implement adaptations. In addition, the supplier is constantly busy improving and innovating the system. For now, case J wants to automate as many processes as possible and improve contact with the supplier. The interviewee indicated that they would also like to be more in control of their system in this way.

5.2. Cross-case analysis

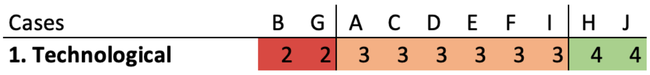
This sub-chapter will examine the empirical findings from each case with a cross-case analysis. The cross-analysis is separated into four different analyses: different variables, general characteristics, challenges, average willingness to innovate vs compatibility maturity level, and relations between characteristics and variables. The average willingness to innovate vs compatibility analysis include the organisations' attitude towards the use and implementation of zero-trust. The findings can be generalised, and cross-case analysis can find patterns.

5.2.1. Different variables

The first analysis is based on the five variables from the TAM-TOE framework and will investigate whether any patterns can be found within each of the variables. The five variables are technological, organisational, environmental, perceived usefulness, and adoption intention. The maturity levels of each variable will be analysed separately. Thus, statements can be made about the individual variables.

Technological

From a technological point of view, table 5.2 shows that the maturity levels are divided. There are two cases in which their IAM system is *quantitatively managed* on a technological level (case H and J). This means that they are actively working on improving and automating their systems. The majority of the cases have a maturity score of 3, which means that they have a *defined* technological level (cases A, C, D, E, F and I). This means that, as an organisation, they are still partly working on making the systems less complex and ensuring that they meet the set requirements. Finally, two cases are at a *managed* level from a technological point of view (cases B and G). This means their system does not yet fully meet the requirements and is often too complex. Complexity and compatibility are two critical factors for the technological maturity level. From the interviews, mainly two problems emerge. (1) Organisations have a system that is compatible but is often too complex, or (2) organisations have a system that is not complex but also not compatible. This implies that often IAM systems become complex in order to be compatible. Expert A showed another perspective on the results: *"Because organisations constantly have to adapt to new policies and therefore constantly have to be compliant, it is often difficult to fully automate the processes. This leads to most organisations having an average maturity score."* (expert A)

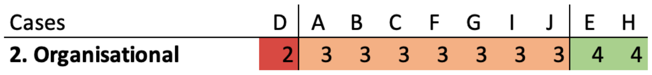


Cases	B	G	A	C	D	E	F	I	H	J
1. Technological	2	2	3	3	3	3	3	3	4	4

Table 5.2: Maturity level technological

Organisational

Table 5.3 shows that, in general, all organisations have a *defined* level of maturity from an organisational point of view. A logical explanation for this is that one of the items measured was the organisation's competency, which mainly measures the organisation's current situation. Since an interviewee will not quickly speak very negatively of his or her employer, it is logical that this has an average score. However, case D explicitly mentioned that their connection with management was difficult. The interviewee even talked about the feeling that the IT team was on an island within the organisation. As a result, case D has *managed* level of maturity. In addition, two cases have a higher maturity level (cases E and H). As discussed in the cross-case analysis by the function of the interviewee, both E and H have a function in middle management. Therefore, they will be relatively more optimistic about the support from top management than an interviewee who has less contact with top management. Expert B gave as explanation for the results that: *"By using interviews to collect data, you will find that many interviewee will talk more positively about the organisation and top management. Thus, you will find mainly average values."* (expert B)

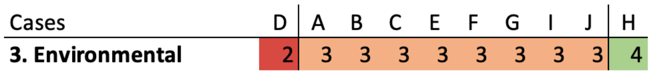


Cases	D	A	B	C	F	G	I	J	E	H
2. Organisational	2	3	3	3	3	3	3	3	4	4

Table 5.3: Maturity level organisational

Environmental

Table 5.4 shows that overall, most financial institutions have a *defined* level of maturity from an organisational point of view. Since the environmental variables measured the competitive pressure, trading partner support, and awareness of external threats, almost all organisations have the feeling that they are aware of their surroundings. One case mentioned that they were mainly focusing on themselves and could grow even more in this (case D). There was also a case where almost everything was automated, including monitoring their environment (case H). A striking finding, which was the same in almost all cases, is that organisations in the financial services sector exchange little or no information with each other about IAM. Almost every interviewee indicated that they still see opportunities here and are open to discussions with other organisations.

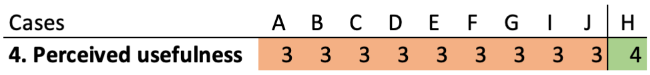


Cases	D	A	B	C	E	F	G	I	J	H
3. Environmental	2	3	3	3	3	3	3	3	3	4

Table 5.4: Maturity level environmental

Perceived usefulness

Table 5.5 shows that most financial institutions have a *defined* level of maturity considering their perceived usefulness of IAM. The perceived usefulness measures to what extent the implemented IAM system meets the expected usefulness. This is done using ease of use (employee) and usefulness (firm). In this way, both the experience of the employees and that of the organisation are taken into account. The interviews show that there are often differences between the usefulness from an employee's point of view and that of a top management point of view. The top management will often have a more optimistic attitude towards the perceived usefulness than the employees. On top of that, top management gives higher priority to the business side of the organisation and will therefore be easily satisfied with the IAM system. An expert recognised this and described it as follows: *"Because the top management often makes less use of the systems, they will also encounter fewer problems. This leads to a predominantly more optimistic attitude than employees who often encounter these problems."* (expert A). Expert B gave a similar statement but added: *"An organisation will always speak positively about the system they use because they understand it. When you present new systems to them, they will initially react negatively because they do not see the added value."* (expert B)

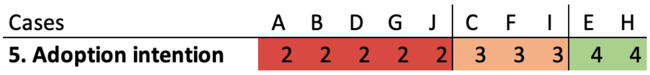


Cases	A	B	C	D	E	F	G	I	J	H
4. Perceived usefulness	3	3	3	3	3	3	3	3	3	4

Table 5.5: Maturity level perceived usefulness

Adoption intention

Adoption intention is measured by the willingness to innovate in each case. Table 5.6 shows that the maturity levels of adoption intention of financial institutions are very divided. Looking at the results, five cases have a relatively low maturity score (cases A, B, D, G and J). Three cases score *defined* which is a relatively average maturity level (cases C, F and I). Finally, two cases scored *quantitatively managed*, which is a relatively high maturity score (cases E and H). A reason that frequently came up during the interviews is that many organisations are busy improving the existing systems. Consequently, they are neither busy nor willing to implement entirely new systems. In addition, the interviewee's position also plays a role in the attitude towards adoption intention. When a person is involved in the organisation's strategy, he or she tends to have a more positive attitude towards the adoption of innovations. A justification for the values found was described by expert B: *"Organisations are mainly concerned with being compliant and making existing systems secure. As a result, people are often less concerned with the implementation of new technologies. It also depends on who you talk to within the organisation. Someone who is not involved in the strategy will score less well on adoption intention."* (expert B)



Cases	A	B	D	G	J	C	F	I	E	H
5. Adoption intention	2	2	2	2	2	3	3	3	4	4

Table 5.6: Maturity level adoption intention

5.2.2. By general characteristics

Type of financial institution

The first angle from which patterns will be found is the type of financial institution. In this multiple case study, three types of financial institutions are included: (1) insurers, (2) banks, and (3) others. Patterns are identified using a heat map of the maturity levels per institution (table 5.7). It can be concluded from the heat map that, on average, insurers have a lower adoption intention maturity level compared to other financial institutions. In addition, it can be concluded from table 5.7 that banks, on average, have a defined maturity level of their IAM. An expert in IAM also recognises this: *”Insurers in the Netherlands are supervised by the DNB. On the other hand, banks are supervised by both the ECB and the DNB. So they have to meet more requirements and, therefore, score higher on average.”* (expert A).

	Insurers					Banks			other	
Cases	A	B	D	E	G	C	F	I	H	J
1. Technological	3	2	3	3	2	3	3	3	4	4
2. Organisational	3	3	2	4	3	3	3	3	4	3
3. Environmental	3	3	2	3	3	3	3	3	4	3
4. Perceived usefulness	3	3	3	3	3	3	3	3	4	3
5. Adoption intention	2	2	2	4	2	3	3	3	4	2

Table 5.7: Heat map type of financial institution

By size of the organisation

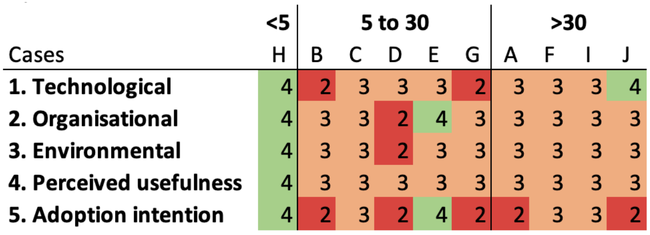
The second approach is used to examine whether patterns between the cases can be found in the size of the cases based on the number of employees. In order to distinguish between the size of the cases, three groups were identified: (1) small (0 - 2.000), (2) medium (2.000 - 10.000), and (3) large (10.000+). Using a heat map of the maturity levels per size of the case pattern are identified. The only statement that can be made based on the size of an organisation is that, on average, the larger an organisation is the higher average maturity score it has in comparison with smaller organisations. However, this is not a strong assumption based on the results. A possible explanation by an expert would be that: *”Many organisations struggle with the problem of not having the resources to improve their maturity level. As a result, relatively small organisations choose to be compliant or only improve the risky parts. Relatively large organisations have more resources and can therefore opt to improve less risky components. This leads to higher average maturity scores for larger organisations.”* (expert A).

	Small				Medium			Large		
Cases	D	G	H	J	B	C	F	A	E	I
1. Technological	3	2	4	4	2	3	3	3	3	3
2. Organisational	2	3	4	3	3	3	3	3	4	3
3. Environmental	2	3	4	3	3	3	3	3	3	3
4. Perceived usefulness	3	3	4	3	3	3	3	3	3	3
5. Adoption intention	2	2	4	2	2	3	3	2	4	3

Table 5.8: Heat map size of cases

By years of existence

The third angle used to find patterns is the years of existence of the cases. In the research, three groups were made based on the number of years of existence of an organisation: (1) 0 - 5 years, (2) 5 - 30 years, and (3) >30 years. Patterns are identified with a heat map of the maturity levels per year of existence. Based on the time of existence, it can be concluded from the heat map that older companies have relatively more average maturity levels. It is also striking that a relatively young organisation has very high maturity levels. An expert gave the following reason for this: *”The young/new organisations have a better overview of the requirements. Thus, they can immediately implement the right systems to be compliant. In addition, they also often look for ways to improve and automate systems, giving them a significantly higher maturity level.”* (expert B)

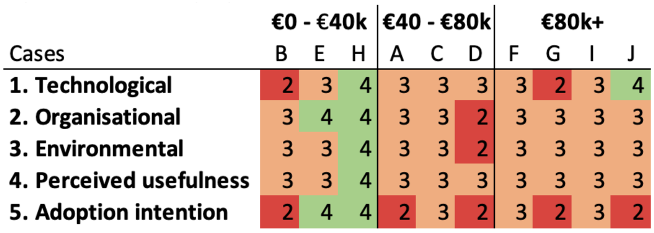


	<5	5 to 30					>30			
Cases	H	B	C	D	E	G	A	F	I	J
1. Technological	4	2	3	3	3	2	3	3	3	4
2. Organisational	4	3	3	2	4	3	3	3	3	3
3. Environmental	4	3	3	2	3	3	3	3	3	3
4. Perceived usefulness	4	3	3	3	3	3	3	3	3	3
5. Adoption intention	4	2	3	2	4	2	2	3	3	2

Table 5.9: Heat map existence of cases

By profit per employee per year

The fourth angle used to find patterns is the profit per employee per year of the cases. In this research, the profit per employee per year is divided into three categories: €0 - €40k, €40 - €80k and €80K+. Patterns are identified using a heat map of the maturity levels per profit per employee per year. The only thing that stands out is that the highest maturity score is an organisation with a relatively low profit per employee per year. However, this can be explained because it is a relatively young company that invests in its growth and has not yet optimised its business processes. Consequently, the profit is lower. Furthermore, there are only minor differences between the maturity scores found; it can be concluded that no exciting patterns can be found based on the profit per employee per year. This outcome was confirmed during the interviews with the experts.



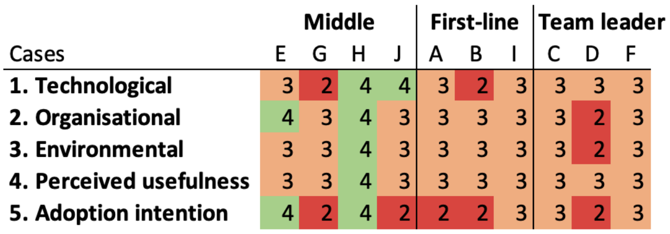
	€0 - €40k			€40 - €80k			€80k+			
Cases	B	E	H	A	C	D	F	G	I	J
1. Technological	2	3	4	3	3	3	3	2	3	4
2. Organisational	3	4	4	3	3	2	3	3	3	3
3. Environmental	3	3	4	3	3	2	3	3	3	3
4. Perceived usefulness	3	3	4	3	3	3	3	3	3	3
5. Adoption intention	2	4	4	2	3	2	3	2	3	2

Table 5.10: Heat map profit per employee

By the type of function of the interviewee

The fifth approach of the general characteristics is the function of each interviewee. All cases are analysed based on the function of the interviewed person. Different results are expected based on a person's role within an organisation. A distinction of the functions is made using three layers of management: middle management, first-line management and team leaders. Each case consists of an interviewee whose role is placed in one of the three layers of management as shown in Table 5.11. The top management level has been left out since none of the interviewees belonged to that management level.

From the results in table 5.11 it can be concluded that the interviewee with a middle management function has a relatively higher maturity than first-line management or team leader functions. The two most exciting findings are the higher scores on the organisational and adoption intention variables. The reason for this is reasonably evident according to an expert: *"Because middle management is closer to top management, they can communicate better with each other, and they will also think more about the strategy of the organisation. Thus, they will feel the support from top management and have a more open attitude towards implementing new technologies."* (Expert B)

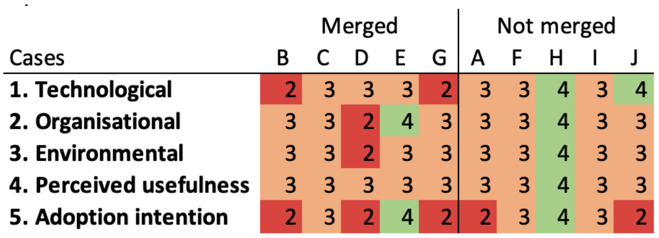


	Middle				First-line			Team leader		
Cases	E	G	H	J	A	B	I	C	D	F
1. Technological	3	2	4	4	3	2	3	3	3	3
2. Organisational	4	3	4	3	3	3	3	3	2	3
3. Environmental	3	3	4	3	3	3	3	3	2	3
4. Perceived usefulness	3	3	4	3	3	3	3	3	3	3
5. Adoption intention	4	2	4	2	2	2	3	3	2	3

Table 5.11: Heat map function interviewee

By merges and acquisitions from the past

The last approach of the general characteristics is the company's history of mergers and acquisitions. Several interviewees indicated that they had been taken over by or merged with other organisations in recent years. They indicated that this could significantly impact the organisational structure and, thus, indirectly on IAM. All cases are analysed based on their past, and the results are shown in table 5.12. It can be concluded from the heat map that organisations that have undergone a merger in recent years have, on average, a lower maturity score than those that have not. During an interview with an expert, the expert gave the following explanation for this: *"Companies are mostly merged to achieve business benefits. However, this causes many problems for IT. As a result, these organisations spend much time trying to merge systems and make them compliant again. In conclusion, this leads to a lower maturity score."* (Expert A)



	Merged					Not merged				
Cases	B	C	D	E	G	A	F	H	I	J
1. Technological	2	3	3	3	2	3	3	4	3	4
2. Organisational	3	3	2	4	3	3	3	4	3	3
3. Environmental	3	3	2	3	3	3	3	4	3	3
4. Perceived usefulness	3	3	3	3	3	3	3	4	3	3
5. Adoption intention	2	3	2	4	2	2	3	4	3	2

Table 5.12: Heat map merged and acquired

5.2.3. By the challenges

During the interviews, several challenges were mentioned (Figure 5.11). When at least two cases mention a challenge, it is included in this analysis. Based on the found challenges, relations between the cases are investigated. This section elaborates on the seven challenges found during the interview.

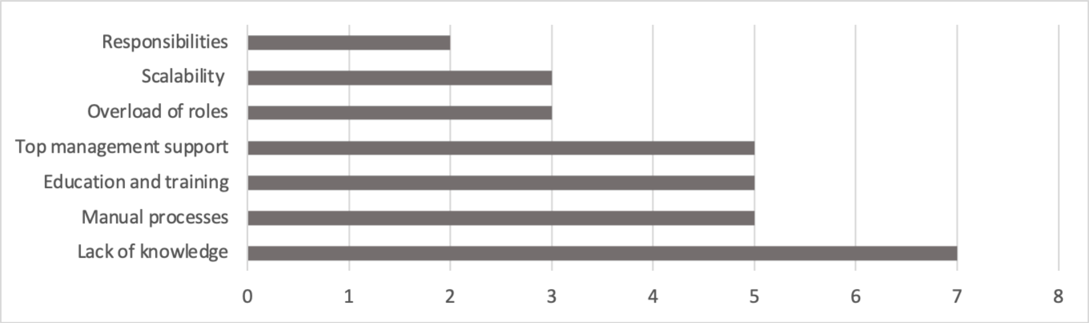


Figure 5.11: Challenges mentioned

Lack of knowledge
Firstly, a lack of knowledge of the IT team and managers (mainly responsible for distributing rights) was mentioned as a challenge in at least 7 out of 10 interviews. Secondly, as lack of knowledge of the employees of the organisation.

First, the lack of knowledge of the IT team (IAM administrators) and managers refers to the problem that many organisations lack the knowledge to improve or maintain their IAM. A lack of knowledge can overlook vulnerabilities or opportunities to improve the system. In addition, a lack of knowledge among managers can lead to incorrect interaction with the system. For example, they may incorrectly allocate authorisations, resulting in employees receiving too many or too few rights.

Secondly, there is also a lack of knowledge among the organisation's employees. The employees are the people who do not interact with the system but receive access through the system. When employees lack knowledge, this can lead to many problems. For example, employees may not see the importance of IAM and thus become a vulnerability of the organisations or even an easy target for cybercriminals. In addition, this can also cause problems in the communication between the employees and the IT employee/manager because employees do not understand how the systems work.

Manual processes
During the interview, it was mentioned several times that organisations had problems with the number of manual processes. For the IT employee, this makes it very difficult to find the time to improve the system in addition to the large amount of manual work. This leads to a lack of time for the IT employees to improve the system or implement new technologies. This problem could be solved by automating more. However, this improvement requires sufficient time, knowledge, and support from top management, which are often challenges these organisations already have. Finally, automating processes can also partially solve the problem of responsibilities because automating processes can take over some of the managers' responsibilities.

Education and training
Another challenge that organisations often face is the education and training of their employees in the field of information security. As already mentioned, there is often a lack of knowledge within organisations. However, improving the knowledge within the organisations is also a problem in itself. In 5 out of 10 interviews, the interviewee indicated that they had problems educating and training their employees. A common reason for this is that the training is often voluntary and therefore many employees do not attend to them. This is also because many employees are only concerned with the business and therefore take the systems in which they work for granted.

Top management support
A frequently mentioned problem is the support from top management. The top management determines the strategy and thus the allocation of financial resources. The allocation of their financial resources dramatically influences the company and their IAM. In 5 out of 10 interviews, the interviewee indicated that they had insufficient support from top management. This leads to a shortage of employees within the IT team, overdue maintenance and, thus, vulnerabilities. Several interviews showed that

the main problem is that top management underestimates the importance of information security and gives higher priority to business processes. Interviewee D even described it like this: *"They will not immediately think that IAM is the essential thing, they rather see IT as water coming out of the tap"*.

The cases that indicated that the support from management was present often gave one of two reasons for this. (1) A person within top management has a background in IT and therefore knows how important it is. (2) The organisation has received a warning from a supervisory body in the past or has even experienced a cyber attack. During an expert interview, the following explanation was given: *"In general, a warning from a regulator only provides an incentive to be compliant and not to make a real improvement. Improving the systems requires the presence of support from top management. Since top management consists of a small group of employees, the knowledge and interest of these people play a significant role in the priority they give to information security."* (expert A)

Overload of roles

An overload of roles is one of the common challenges of RBAC. In 3 out of 10 interviews, it was explicitly mentioned that the organisation had problems with the number of roles created. In cases A and G, the interviewees even indicated that they had more roles than employees. The basis of this problem starts with the creation of the generalise roles. The manager often requests an entirely new role because the correct rights are not given to a role. This leads to new roles being created all the time. The old roles will be removed since employees who have been working for an organisation for a long period time often receive different roles on top of the old role. In addition, managers often lack knowledge because they do not realise the impact of the way they deal with the IAM system.

Scalability

The overload of roles is also one of the scalability problems of an RBAC model. In 3 out of 10 interviews, the organisation suffered from scalability problems. Especially when an organisational structure changes due, for example, mergers and acquisitions (section 5.12), many problems occur in the system. Because of the static character of RBAC, many roles have to be completely rearranged. It is also challenging to create a fundamental role, primarily when the organisation consists of several sub-organisations. This often leads to a more complex system, making it more difficult for the employees to understand. A solution to this could be the switch to ABAC and the automation of the allocation of authorisations because it is a more dynamic system and can therefore cope better with changes. However, the switch to an ABAC model can be expensive and costs much time, which top management most of the time prefers to spend on other things.

Responsibilities

The last challenge mentioned twice or more during an interview is the incorrect distribution of responsibilities. As also described earlier with the manual processes, many organisations have problems with correctly distributing the responsibilities of allocating rights. In almost all organisations, managers should take responsibility for this, but unfortunately, this is not the case. In two of the ten interviews, the interviewee emphasised that they had taken on the responsibility while they should have had a facilitating role. One of the reasons why IT teams take on more ownership is the managers' lack of knowledge. As a result, the managers do not interact the system correctly (e.g. wrong allocation of authorisations) and hardly carry out any checks.

5.2.4. By average willingness to innovate vs. compatibility maturity level

The maturity level of the cases' ambition is based on the willingness to innovate (sub-variable of adoption intention) and compared with the compatibility (sub-variable of technological) of the current system of the case; both were measured during the interviews. Thus, statements can be made about their intention to adapt to new technologies based on the compatibility of their current system. The results are shown in Figure 5.12 and the dotted line indicates the mean of the analysed cases.

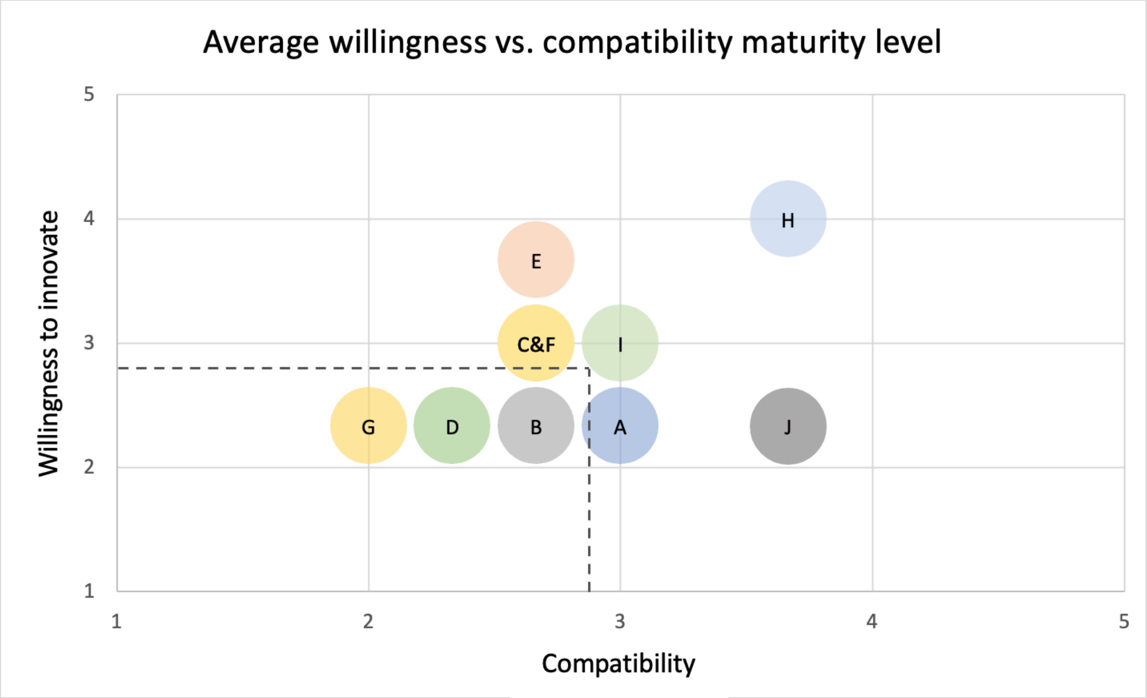


Figure 5.12: Plot willingness vs. compatibility

The figure shows all cases based on their compatibility maturity score and their willingness to innovate maturity score. These two variables have an exciting relationship since the expectation is that an organisation with a low compatibility score would be willing to innovate and vice versa. However, there are several peculiarities in the figure. First, it is visible that case G has the lowest compatibility score and a relatively low willingness to innovate score. One reason for this could be that case G has gone through several mergers and acquisitions in recent years and is still looking for improvements in the system. Secondly, case J has a relatively high compatibility score and a low willingness to innovate. One explanation for this could be that, since case J purchases its IAM entirely from an external party, they are mainly concerned with the system's compatibility. As a result, they do not focus on innovations as this responsibility lies with the external party.

Thirdly, case E has an exciting position within the figure. Case E has a relatively low/average compatibility score and a relatively high willingness to innovate. The interview with case E showed that they were aware that their IAM was not good enough. As a result, they drew up a clear strategy in which IAM is a vital component. As a result, case E has a high willingness to innovate score. Finally, case H has a unique position within the figure since it has relatively high compatibility and willingness to innovate. The interview with case H showed that they are ahead in their IAM. They immediately set up appropriate systems to properly implement their IAM as a relatively young company. In addition, they are constantly looking for new technology to improve and automate their systems.

Zero-trust

During the interviews, the interviewee was asked to what extent they were familiar with the zero-trust principle and whether they were already implementing it. In this way, Figure 5.13 shows the answers to the different cases. In this way, it can be seen that cases A and D were not familiar with zero-trust. In order to be able to apply the method in practice, the respondents had to be familiar with the concept of zero-trust and had to be able to apply it in practice. The interviewees gave reasons that their infrastructure was not yet ready for zero-trust, that they were still too busy improving the existing system, or that there was too little knowledge. Finally, cases E and H indicated that they focus on zero-trust in their strategy and that this has already been (partly) implemented. Both parties indicated that IAM has a high priority because there is sufficient knowledge within top management.

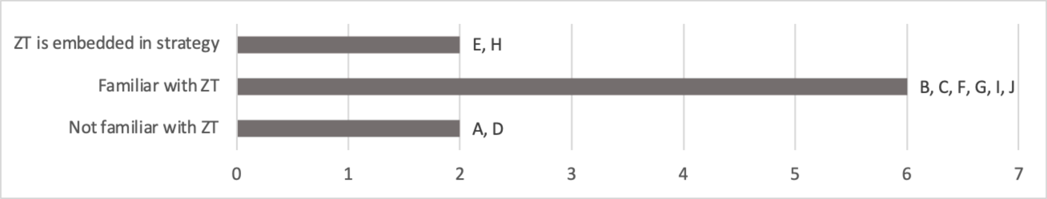
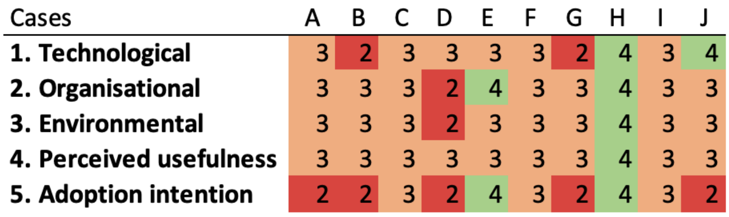


Figure 5.13: zero-trust mentioned

5.2.5. Relations between characteristics and variables

In the previous sections, the different characteristics and variables were analysed. Thus, the results found also suggest interrelationships. In this section, the interrelationships between the characteristics and variables will be generalised. Figure 5.13 is shown to give a overview of all the found maturity scores.



Cases	A	B	C	D	E	F	G	H	I	J
1. Technological	3	2	3	3	3	3	2	4	3	4
2. Organisational	3	3	3	2	4	3	3	4	3	3
3. Environmental	3	3	3	2	3	3	3	4	3	3
4. Perceived usefulness	3	3	3	3	3	3	3	4	3	3
5. Adoption intention	2	2	3	2	4	3	2	4	3	2

Table 5.13: Overview variables

Role interviewee & organisational

Based on the table 5.11, it can be concluded that the role of the interviewee has an influence on the organisational maturity score. When an interviewee has a role that is closer to top management, on average they speak positively about the way top management of the organisation supports them. This leads to a higher organisational maturity score.

Organisational & adoption intention

From the overview of the maturity scores found in table 5.13, it is clear that there is a correlation between the maturity scores of organisational and adoption intention. It could be concluded that the higher the maturity score of organisational, the higher the maturity score of adoption intention. When an organisation has strong support from top management and therefore has a high organisational maturity score, this often means that they also focus on IAM in their strategy. As a result, high organisational scores go hand in hand with a higher adoption intention score.

Technological & adoption intention

Based on the overview of the maturity level, it can be concluded that there is a slight correlation between technological and adoption intention. A lower maturity score for technological often goes hand in hand with a lower score for adoption intention. A possible explanation is that organisations with a low technological maturity score are often only concerned with improving their existing systems. This subsequently leads to a reduced focus on innovation and, consequently, a lower adoption intention maturity score. Case J is a separate case in view of the fact that they have completely outsourced their IAM system to an external party. As a result, they have a lower score for adoption intention because the external party takes care of improving and renewing the systems.

Merged & technological/adoption intention

In section 5.2.2 the impact of a merger or acquisition of an organisation on the IAM maturity scores is analysed. Based on the values found in the table 5.12, it can be concluded that there is a correlation between whether an organisation has merged or been acquired and both the technological and adoption intention maturity scores. Because the merger of organisations leads to the merger of systems, many organisations spend less time improving and merging their systems. This leads to a lower technological maturity score. It also means that they do not or hardly work on renewing the system, which results in a lower adoption intention maturity score.

6

Discussion, limitations & future research

6.1. Discussion

This research aims to gain insight into the effects of implementing access controls and IAM principles on the financial services sector's information security and security challenges. A multiple case study was applied to determine the current maturity status of the financial institutions. All institutions included in this research have a branch or operate in the Netherlands. This section provides a discussion of the main findings of the study, followed by limitations and suggestions for future research.

6.1.1. General characteristics

The first interesting finding is that the data suggests that insurers have a lower average maturity score within the financial services industry than other institutions. This could be explained by how the various institutions within the financial services sector are supervised. In the Netherlands, all financial institutions are supervised by DNB and AFM (Ministerie van Financiën, 2022). This means that every financial institution has to meet the requirements set by DNB and AFM. However, banks in the Netherlands are besides by the DNB and AFM, also supervised by the ECB. (De Nederlandse Bank, 2022). Thus, banks have to comply with more and stricter regulations set by the ECB. Consequently, this results in an overall higher maturity level. The findings were confirmed during the interviews with experts. However, expert B did say that the supervisors communicate the policies and try to harmonise them to make them easier to implement for the organisations.

The second finding supported based on the data is that the size of an organisation has a positive effect on the IAM maturity levels. However, based on the data found, no strong assumption could be made of correlation between the size of an organisation and the way they implement its IAM. The only statement that can be made based on the size of an organisation is that, on average, the larger an organisation is the higher average maturity score it has in comparison with smaller organisations. Expert A explained the finding as follows: *"Many organisations struggle with the problem of not having the resources to improve their maturity level. As a result, relatively small organisations choose to be compliant or only improve the risky parts. Relatively large organisations have more resources and can therefore improve less risky components. This could leads to higher average maturity scores for larger organisations."* (expert A).

In addition to the maturity levels in comparison to the size of an organisation, one can also look at the scalability of the IAM system on the basis of the size of an organisation. Sandu et al. (2000) explains in his research what the relationship is between the number of persons within an organisation and the IAM system. In their research, they talk about the limitations of the RBAC model. Here, no limitation is given to the number of persons using the IAM system. However, the researchers only limit the number of roles a user can have within the system. Also, the NIST (2014) report on the standardisation of ABAC gives no limitations for the number of users on the IAM system. It can be concluded that there is no difference between the size of an organisation and how the IAM is implemented. Interviewee H described it as follows: *"When you link scalability to the number of people in the IAM team, you are* *doing it wrong".* Based on this findings, the size of an organisation is not the limiting factor for an IAM system.

In addition to the organisation's size, there is also no correlation with the organisation's profit per employee per year. The statement above already partly confirms that the profit per employee does not influence the IAM maturity levels because the size (number of employees) has a powerful influence on the profit per employee. A refutation of this statement lies in the fact that time, knowledge and money are limiting factors for improving and maintaining IAM (Vijayalakshmi and Jayalakshmi, 2021, Dhar and Bose, 2021). This would indicate that a higher profit per employee per year should have a higher maturity level.

A third finding that stands out from the data is that relatively young organisations have better IAM than organisations that have been around for several years. An explanation for this can be given from two perspectives. First, the literature shows that RBAC was first introduced in the 90s (R. S. Sandhu et al., 1996), whereas ABAC was designed at the beginning of the 21st century (Hu et al., 2014). Thus, the relatively older organisation did not know about ABAC and its more dynamic character when they first organised their IAM. Secondly, it takes time and money for organisations to innovate or make the transition from an RBAC to an ABAC system (Hu et al., 2014). Although ABAC will save maintenance and governance costs in the long run, this research shows that it is not a priority for many organisations. On the other hand, a relatively young organisation can immediately use the latest technologies when setting up their IAM.

A fourth finding that can be made on the basis of the data is the fact that the role of the interviewee is a confounding variable. The data shows that interviewees with a role at middle management level have a higher average maturity level than interviewees with a relatively 'lower' level in the organisation. An explanation for this is given by expert B: *"Because middle management is closer to top management, they can communicate better with each other, and they will also think more about the strategy of the organisation. Thus, they will feel the support from top management and have a more open attitude towards implementing new technologies."* (Expert B). Thus, it can be concluded that the role of an interviewee is a confounding variable when measuring IAM maturity levels.

Finally, based on the results of this study, a fourth finding can be made. In recent years, organisations acquired or merged have a lower average maturity score than those that have not. The expert's explanation indicated that merging organisations can lead to problems within companies' systems. Expert A: *" Companies are mostly merged to achieve business benefits; however, this causes many problems for IT. As a result, these organisations spend a lot of time trying to merge systems and make them compliant again. In conclusion, this leads to a lower maturity score."* (expert A). However, there is no direct explanation for this in the literature. However, several studies describe the static character of RBAC (Bertino, 2003, Kunz et al., 2019). When merging two organisations, this static character can lead to problems. As a result, organisations spend a long time trying to merge their systems.

6.1.2. Challenges

Based on the results of the interviews, several challenges were identified for the organisations. The seven challenges identified to give a good picture of how the interviewees view problems within IAM. From the found challenges and the interviews with experts, it can be concluded that the support from top management plays an essential role in the information security of an organisation. A lack of support can lead to the aggravation of other challenges. Expert A described it as follows: *"When top management does not provide sufficient support, this will directly lead to a shortage of resources needed to implement the IAM system correctly. Thus, it will lead to a lack of knowledge, problems with education and training, and failure to automate manual processes."*

The lack of knowledge is seen as a significant challenge in many organisations. This finding has been recognised in the literature as an essential part of information security (Applegate, 2009). By increasing employees' awareness, an organisation is better prepared for potential threats. In addition, studies by Dhar and Bose (2021) and Sandhu et al. (2000) show that knowledge plays an essential role in the improvement and innovation of IAM systems. In addition, a shortage of knowledge can also strengthen or cause other challenges. For example, it can lead to a misallocation of responsibilities because people within the organisations do not take ownership of the system. Likewise, a shortage of knowledge can cause managers to create new roles constantly. Here too, employees cannot assess the impact of their actions due to a lack of knowledge. Thus, it can be concluded that besides the support from top management, the lack of knowledge plays the most crucial role in the information security of an organisation.

Since one of the challenges is the lack of knowledge within an organisation, this often leads to social engineering. As described in chapter 2, social engineering is a form of hacking where the hacker tries to penetrate the organisation via a person. The moment an employee is aware of the dangers of information security, he or she is more likely to be wary of this type of attack. As a result, they are less likely to click on a malicious email or share their data. An organisation should focus more on the weakest link, the employees. By doing so they will directly reduce some of the risks.

6.1.3. Zero-trust

One of the variables from the applied TAM-TOE framework is adoption intention. This variable describes how the organisation is willing to adopt innovations/principles. During the interview, several questions were used to determine to what extent an organisation is open to and looking for innovations for their systems. In addition, the interviewee was also explicitly asked to what extent he or she was familiar with zero-trust. The analysis of the relation between the two variables identifies that organisations with a relatively low adoption intention are not or hardly familiar with zero-trust. A number of reasons for this can be found in the literature and expert interviews.

Firstly, one of the results of the interviews is that many organisations are busy improving their existing system. As a result, they are less concerned with the potential added value of an innovation like zero-trust. This fits well with the second reason: there is still little practical experience and knowledge about zero-trust. At this moment, there is mainly descriptive literature about the implementation and possible added value of zero-trust, but it lacks substantiation from practice (Xiaojian et al., 2021). Expert A described it as follows: *"Because many organisations are busy improving their existing systems, it will be a long time before they see the added value of zero-trust. Consultancies will play an important role in educating these organisations. In addition, many organisations will also wait until their competitors start using zero-trust."*. Thus, external parties can play an essential role in the attitude of organisations toward zero-trust.

Thirdly, it appears from the interviewees that many organisations do not yet have an architecture ready to implement zero-trust. Since zero-trust makes use of a number of key components, the architecture must also be ready for it (Buck et al., 2021). On top of that, investments in security solutions do not give a detectable return on investment (Weishäupl et al., 2018). Thus, many organisations find it challenging to make budgets for these improvements. Finally, the data suggest that many organisations are currently struggling with a lack of knowledge. Knowledge is essential when it comes to implementing zero-trust (Dhar and Bose, 2021). Based on the results and discussion, there must be both organisational and technical developments before zero-trust can become the standard.

Added value of zero-trust

Within the IAM, several improvements have already been proposed in recent years with the advent of RBAC and ABAC (R. S. Sandhu et al., 1996, Hu et al., 2014). Not every improvement brings the same added value. However, the advent of zero-trust could significantly positively impact organisations' IAM. First, zero-trust makes use of trusted users and devices, which enables remote working in a safe manner (Osborn et al., 2016). Secondly, the implementation of zero-trust reduces operational costs (Cunningham and Pollard, 2017). Thirdly, the modular design of zero-trust networks makes them easily scalable (P. Kumar et al., 2019). Finally, network usage and logging are constantly monitored, which enables ensuring dynamic responses (Rose et al., 2020).

Although zero-trust appears on paper to be the solution to many of the challenges identified by the organisations, much remains to be done. First of all, more practical research needs to be done to prove that zero-trust is the future. In addition, there is currently a significant gap in the literature on user experience (Gigamon, 2020). Finally, it is a matter of time before zero-trust will become the standard according to interviewee H: *”I think it will take about two years when zero-trust becomes the standard”.*

6.1.4. Relations between characteristics and variables

As discussed in the cross-case analyses, several relationships can be identified based on the results found. First, there is a correlation between the function of an interviewee and the organisational maturity score. An explanation for this can be found in the fact that an interviewee with a position closer to top management has more interaction with top management. As a result, they will often have more information about the company’s strategy and therefore also look more positively at problems. This finding was validated in both expert interviews. Second, a correlation was found between the maturity scores of organisational and adoption intention. This is also in line with the previous finding because a higher organisational maturity score is often the result of more knowledge about strategy and a more open attitude towards innovations.

Thirdly, the results showed that the maturity score of technological has a correlation with the adoption intention. This correlation was directly validated by the experts and the explanation was as follows: *”because an organisation is busy improving their IAM in the technological area, this leads to a less open attitude towards innovations.”* . Finally, a correlation was found between whether companies have merged or acquired in the past and their technological/adoption intention maturity level. Again, this is closely related to the previous correlation. Because as described by the expert: *”when a company merges or is acquired, it costs them a lot of time and money to make all the systems go together, so they have a worse system for a while.”*

Future statistical analyses

In addition to the qualitative research carried out, a number of statistical analyses could also be carried out. Based on the type of data and the question, a number of tests can be carried out. Given the fact that the used CMMI model has an ordinal scale the following tests can be performed; Mann-Whitney U Test and the Kruskal-Wallis Test (Neideen and Brasel, 2007). By means of the Mann-Whitney U Test, ordinal data from two independent populations can be analysed. Thus, statements can be made about the correlations between the two groups. The Kruskal-Wallis Test can approximate whether more than two groups are similar to each other. In this way, statements can be made about the groups that are similar to each other.

6.2. Limitations

The limitations of this study provide opportunities for future research. First of all, this study uses exploratory research, which means there is a limited generalisation of the findings. More research is needed to validate the patterns and influences found. In addition, this study provides a broad overview of the various influences on an organisation’s IAM; future research could focus on a specific influence within the framework. In doing so, a possibly larger sample size could be used, making the findings more generalisable. Also, the results from future research could be fed back to the maturity model, which could increase the model’s reliability.

Moreover, since this study is focused on the financial services sector, generalising the findings to other sectors is difficult. This is because not every sector tries to protect risky information in the same way. In addition, each sector has a different regulator, and in the case of the financial services sector, there are many laws and regulations that an organisation must comply with. A follow-up study could apply this same research method to another sector. Because every organisation, independent of the sector, uses an IAM system (Samarati and de Vimercati, 2000), every sector can be investigated. However, geographical demarcations could influence the laws and regulations in that area and thus on the IAM. This could be investigated further in future research.

Furthermore, this study makes use of documents and interviews from the organisations. Both sources are self-reported sources that question the validity of the study’s findings. The documents consist mainly of the annual reports of the organisations. Because the documents have to be readable for everyone, they are often less technical, and themes such as cyber security are not or hardly dealt with. In addition, information security is not always high on the agenda of top management and is then omitted from an annual report. Finally, not all interviewees have the same role within the interviewed organisations. These, in section 6.1, described confounding variables that may lead to a difference in the interviewee's knowledge. In addition to the size of the sample, future research could also take into account the interviewee's role within the organisation.

6.3. Future research

This research was conducted within the financial services sector in the Netherlands. Therefore, this research could be conducted in another sector in the Netherlands or the same sector in other parts of the world. This allows the usefulness of the model to be validated for other sectors and findings to be generalised or invalidated for other sectors. In addition, interviews were conducted with only one employee of the organisation. Future research could increase the number of interviewee per case to increase the reliability of each case. Also, the number of individual cases (samples) could be increased to increase the reliability of the findings. Finally, future research could take into account the different roles of interviewees, given its impact on the results.

Next to that, this research provides a broad overview of the maturity levels of IAM within the financial services industry. Future research could focus more on one variable of the framework resulting in a detailed view of one variable of IAM. In addition, future research should focus more on implementing zero-trust. At the moment, there is still a lot of knowledge missing regarding the practical application and user experience of zero-trust. In this way, besides the academic foundation of zero-trust, a more practical foundation of zero-trust can be developed.

6.4. Reflection on scientific and societal relevance

6.4.1. Reflection on scientific relevance

The scientific value of this research would, as described at the beginning of this research, mainly be aimed at providing insight into the choices and considerations of organisations when implementing IAM systems. In addition, the current challenges within information security within organisations are mapped out. Finally, this research would provide insight into how organisations could improve their IAM system.

Looking back at the research carried out and the results, it can be concluded that the aforementioned expectations have been met. The within-case analyses provide insight into the current situation regarding IAM within the organisations. They also describe the choices or arguments made by the interviewee. During the interviews, challenges within the different variables were asked at different times. The challenges found provide a good picture of the problems within the organisations. This gives sufficient reason for future research. Finally, this research also has scientific value for the use of the TAM-TOE framework. In this research, the variables ambition and external threats were added to gain more insights. Future research could make use of the same variables that have been used in this research.

6.4.2. Reflection on societal relevance

In the introduction of this thesis the problem was described which is at the heart of our society. Digital devices are used in our everyday activities and are crucial for organisations. As described, one of the most important aspects is that only those who have authorisation can access, modify or erase any data within an organisation. This research shows the challenges and shortcomings of the current systems as well as the organisational challenges that exist within organisations.

The challenges give a clear picture of the problems within the organisations. Almost all challenges have in common that the people within the organisation have a direct influence on them. This also means that people play one of the most essential roles in the information security problems within organisations. The lack of cyber knowledge and support for top management are the most important findings. If organisations invest in their employees and technologies, their users/client/customer will be less vulnerable and the organisation becomes more resilient to the future of cybercrime.

7

Conclusion & recommendation

7.1. Conclusion

This study shed light on the maturity levels and challenges of IAM within financial services organisations. On top of that, it included the added value of implementing one IAM principle, namely zero-trust. This research was conducted through multiple case study based on semi-structured interviews with employees of the organisations. The research question to be answered is:

What are the effects of implementing access controls and IAM principles on information security and security challenges that exist within organisations in the financial services sector?

To answer the main research question, six sub-questions have been formulated in section 1.2.4. To answer the first sub-question, the actors within the system had to be identified. In section 3.1 all internal and external actors and their relations are elaborated on. The external actors consist of the supervisors (DNB, AFM and ECB) and the service providers. The supervisors have a supervisory role and draw up laws and regulations with which the organisations must comply. The service providers supply and support the IAM software used by the organisations. The internal actors consist of top management, IAM administrator, managers, application/asset manager and users/employees. Within an organisation the IAM administrators are the facilitators of the system used by the managers, application/asset managers and users/employees. Finally, top management provides the resources for the IAM administrator to set up the system.

The second sub-question focuses on the framework that will be used for this research. Based on the literature review, a theoretical framework was selected to be used for the study of access controls. The literature review revealed several perspectives that provide a clear overview of an organisation's IAM. The framework that includes the point of view is the TAM-TOE framework consisting of variables like technological, organisational, environmental, perceived usefulness, and adoption intention. In order to be able to compare the organisations, the capability maturity model integration (CMMI) was used based on the variables from the TAM-TOE framework. CMMI is a well-known scale to measure the stage in which an organisation utilises new technology with the use of five maturity levels.

The third sub-question focuses on the effects of the type of access control on the IAM based on the interviews and within case analysis. A number of conclusions can be drawn regarding the correlation of the type of access controls and the IAM of an organisation. First of all, it can be concluded from the results that organisations within the financial services industry mainly use RBAC. This was also suggested by the literature (Kunz et al., 2019). Secondly, it is noticeable that the organisations with, on average, a better IAM system are in the process of implementing ABAC at various places in their systems or even look into the possibilities of zero-trust. An explanation for this is that organisations with a better IAM system are often more concerned with innovations to keep the system running smoothly. Finally, it can be concluded that the type of access control has no direct influence on the maturity levels.

This is because being secure or compliant does not depend on the type of access control but on the way in which an organisation implements it.

The fourth sub-question focuses on the effects of and correlations between certain characteristics and the IAM of financial services organisations. Based on the interviews, this was investigated by means of a cross-case analysis. Based on the analysis of the interviews and the discussions with the expert, the following conclusions can be drawn.

- Banks have a higher average maturity score than insurers. Since banks are supervised by more institutions, this implies that the amount of supervision has a positive effect on average maturity scores.
- The size of the organisation has a positive impact on the average maturity scores. Because relatively larger organisations, compared to relatively smaller organisations, have more resources to improve their IAM, they can make more improvements and therefore have a higher average maturity score.
- The number of employees does not limit the scalability of the IAM system. The IAM system is not limited to the number of people using the system or receive authorisation via the system. However, there is one limitation found in the literature with the use of RBAC, namely the number of roles that can be linked to a person.
- Relatively younger companies have higher average maturity scores. Because a young company is smaller and therefore more flexible, they can implement changes quickly. In addition, they have a better idea of how to be compliant and secure with the techniques that are currently available.
- Organisations that have been acquired or merged in the past have a lower average maturity level than those that have not been acquired or merged. Since merging two organisations also means that all systems must be merged, this leads to many problems. As a result, organisations spend a long time merging their existing systems and do not focus on improvement and renewal.
- Organisations with a low technological maturity score often also have a low adoption intention maturity score. Discussions with the expert have revealed that organisations with a poor technological maturity score only focus on improving the existing system. As a result, they are less involved in innovations and consequently have a lower adoption intention maturity score.

The fifth sub-question examines the information security challenges of organisations in the financial services sector. On the basis of the interviews, seven information security challenges have been identified. Each challenge has a short explanation and it states how many cases it has been mentioned.

- Lack of knowledge (7 out of 10): A lack of knowledge in IAM of both the IT teams and managers causes problems in terms of maintenance, improvement and interaction with the IAM system.
- Manual processes (5 out of 10): A large amount of manual processes leads to a lack of time for improving and maintaining the system and to mistakes due to human error.
- Education and training (5 out of 10): Many organisations have difficulties in providing information security education and training to their employees.
- Top management support (5 out of 10): The fact that top management in many organisations pays too little attention to information security can cause many risks within IAM.
- Overload of roles (3 out of 10): By constantly creating new roles to give employees the right authorisations, some organisations have more roles than employees.
- Scalability (3 out of 10): As organisations change over the years, this can lead to scalability issues for the IAM models.
- Responsibility (2 out of 10): Some organisations struggle with incorrect distribution of responsibilities/ownership in the area of IAM.

Based on the data, it can be concluded that almost all organisations struggle with a lack of knowledge of both the IT teams and the managers who interact with the system. This is a consequence of another challenge that many organisations face, namely the way in which organisations provide knowledge about information security. However, the expert interviews revealed that they normally see top management support as one of the biggest problems in almost all organisations. An explanation for this could be that not all interviewees have the same role within an organisation and thus do not see this as a problem. In addition, both experts indicated that many of the challenges are caused by lack of support from top management. For example, when there are insufficient financial resources to automate processes or provide training, this reinforces several of the challenges described.

The sixth and final sub-question focuses on the added value of information security principles in mitigating IAM problems. The literature has shown that due to the increasing complexity within IAM, a new model has been designed know as ”zero-trust”. The zero-trust approach focuses on the protection of data and services with the use of various principles instead of being a standalone technology (Sultana et al., 2020). A zero-trust model assumes that the attacker is present in the environment thus constantly minimising access to resources to authorised and verified persons. Based on the literature the use of zero-trust has several benefits. First, zero-trust makes use of trusted users and devices, which enables remote working in a safe manner (Osborn et al., 2016). Secondly, the implementation of zero-trust reduces operational costs (Cunningham and Pollard, 2017). Thirdly, the modular design of zero-trust networks makes them easily scalable (P. Kumar et al., 2019). Finally, network usage and logging are constantly monitored, which enables ensuring dynamic responses (Rose et al., 2020).

In addition to the conclusion based on literature that zero-trust could offer a possible solution, this research also examined the organisations’ attitude towards this innovation. The analysis of the data suggests that organisations with a relatively low adoption intention are not or hardly familiar with zero-trust. A number of reasons for this can be found in the literature and expert interviews. First, there is little practical experience and knowledge about zero-trust. Second, many organisation are busy improving their existing system. As a result, they are less concerned with the potential added value of an innovation like zero-trust. Third, investments in security solutions do not give a detectable return on investment, which is something that many organisations base their choices on. At last, the lack of support from top management ensures that there is insufficient knowledge, resources and time to implement zero-trust. Although zero-trust appears on paper to be the solution to many of the challenges identified by the organisations, much remains to be done.

To conclude, the answer on the main research question can be given based on the results found and the literature. The different types of access controls have different influences on organisations’ information security and security challenges. First of all, it is not about the type of access control but about how an organisation has implemented it. Because each type of access control can be implemented so that an organisation is secure and compliant, the difference is mainly in the manner of implementation. Secondly, the interviews show that a lack of support from top management is one of the most significant challenges within an organisation. Because support from top management is necessary for every choice within an organisation, this has a significant impact on IAM. Finally, the literature shows that zero-trust could be a solution to several challenges that organisations currently face. However, the data shows that only a few organisations already implement zero-trust. The perceived reasons for this are too few practical examples of zero-trust, focus on improving existing systems, lack of knowledge, and too little support from top management. Much is possible from a technological point of view, but it has to be driven from within the organisation. It is just a matter of time until organisations realise that steps need to be taken to protect themselves against external threats.

7.2. Recommendations

This study aimed to provide more insight into the effects of implementing access controls and IAM principles on the financial services sector's information security and security challenges. A multiple case study was applied to determine the current maturity status of the financial institutions. The ultimate goal was to find out the organisation's attitude towards zero-trust and the added value of implementing zero-trust. As a result of this study, several recommendations can be made.

The first and most important change is to increase top management support. Since an organisation is run by top management, this is where the most significant opportunities for change lie. A number of possible changes are described:

- Ensure IT expertise in top management, so that every choice is also approached from an information security point of view.
- Transparency, make sure that every choice is communicated to the whole organisation. This way, employees feel part of the process and understand it better.
- Clear strategy, a clear strategy with information security as a lead ensures that you, as an organisation, are prepared for changes. In addition, this strategy must be supported by the entire organisation (transparency).
- Make systems scalable and don't just think in the now. With everything changing around us, it is important to be prepared for these changes.

Secondly, it is important that there is a clear division of responsibilities within the organisation. Because the information security team has a facilitating role, they must also ensure the comprehensibility of the systems. A number of recommendations are:

- By designing the systems in such a way that the user understands them, you as an information security team can take a more supporting role. This can already be achieved by making simple manuals and simplifying the systems.
- Automatic checks and reminders, by automating the checks and reminders as much as possible, you make sure that you are not constantly checking people and reminding them of their tasks.

Thirdly, the main focus should be on the level of knowledge within the organisation in the field of information security. This applies to both employees and the information security team. Several recommendations are:

- Invest in the information security team, by freeing up a budget for training and education, people within information security are triggered to train themselves. In this way, they can also encourage each other to gain more knowledge about various subjects.
- Ensure more interaction with students, because the knowledge of new themes is mainly given to students, it is important to have enough new employees. You can already achieve this by having students graduate at your organisation and thus receive more insights within the organisation.
- Annual training and simulated hacks, by providing mandatory annual training to the entire organisation you ensure that everyone is aware of the impact of poor information security. It also helps to do this by using practical examples such as simulating an actual hack. This can lead to more support and knowledge about the risks and impact.

Finally, it remains to be seen whether a new technology will be seen as the new standard. But above all the difference is how you implement and make use of the technology. As Thomas Edison once said:

Just because something does not do what you planned it to do does not mean it's useless.

Bibliography

Anderson, R., & Moore, T. (2006). The economics of information security. *science*, *314*(5799), 610–613.

Applegate, S. D. (2009). Social engineering: Hacking the wetware! *Information Security Journal: A Global Perspective*, *18*(1), 40–46.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787–2805.

Bertino, E. (2003). Rbac models—concepts and trends. *Computers & Security*, *22*(6), 511–514.

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and erp systems: A multi-case analysis using the technology organization environment framework. *International Journal of Accounting Information Systems*, *15*(2), 149–165.

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436.

Campbell, M. (2020). Beyond zero trust: Trust is a vulnerability. *Computer*, *53*(10), 110–113.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks* (tech. rep.). Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Chen, Y., Hu, H.-c., & Cheng, G.-z. (2019). Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*, *20*(2), 238–252.

Cialdini, R. B. (2001). The science of persuasion. *Scientific American*, *284*(2), 76–81.

Coyne, E., & Weil, T. R. (2013). Abac and rbac: Scalable, flexible, and auditable access management. *IT professional*, *15*(03), 14–16.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Cunningham, C., & Pollard, J. (2017). The eight business and security benefits of zero trust. *Forrester Reseach November*.

Das, S., Mitra, B., Atluri, V., Vaidya, J., & Sural, S. (2018). Policy engineering in rbac and abac. *From database to cyber security* (pp. 24–54). Springer.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation). Massachusetts Institute of Technology.

De Nederlandse Bank. (2022). Europees toezicht op grote banken. https://www.dnb.nl/betrouwbare-financiele-sector/toezicht-op-financiele-instellingen/europees-toezicht-op-grote-banken/

Dhar, S., & Bose, I. (2021). Securing iot devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1), 18–34.

Diefenbach, T. (2009). Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews. *Quality & Quantity*, *43*(6), 875–894.

Dodge, M., & Kitchin, R. (2018). The challenges of cybersecurity for smart cities. *Creating smart cities* (pp. 205–216). Routledge.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532–550.

Eludiora, S., Abiona, O., Oluwatope, A., Oluwaranti, A., Onime, C., Kehinde, L., et al. (2011). A user identity management protocol for cloud computing paradigm. *Int'l J. of Communications, Network and System Sciences*, *4*(03), 152.

Faraj, S., Renno, W., & Bhardwaj, A. (2021). Unto the breach: What the covid-19 pandemic exposes about digitalization. *Information and Organization*, *31*(1), 100337.

Ferraiolo, D., Cugini, J., Kuhn, D. R., et al. (1995). Role-based access control (rbac): Features and motivations. *Proceedings of 11th annual computer security application conference*, 241–48.

Ferraiolo, D., Gilbert, D., & Lynch, N. (1993). An examination of federal and commercial access control policy needs. *NIST-NCSC National Computer Security Conference*, 107–116.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 224–274.

Frank, M., Buhman, J. M., & Basin, D. (2013). Role mining with probabilistic models. *ACM Transactions on Information and System Security (TISSEC)*, *15*(4), 1–28.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated tam-toe model. *Journal of enterprise information management*.

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2021). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management*, e2180.

Gigamon. (2020). *The IT Security Landscape for 2020 and Beyond and the Role of Zero Trust* (tech. rep.). https://www.gigamon.com/content/dam/gated/ar-zerotrust-surveyreport.pdf

Haas, R. d., & Vor, M. d. (2001). Financial stability: The role of de nederlandsche bank. *Economisch Statistische Berichten Jaargang*, *86*(4323), 696–699.

Hodder, I. (1998). The interpretation of documents and material culture (pp. 110-130). *Collecting and interpreting qualitative materials. SAGE Publications, London, Thousand Oaks*.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., et al. (2014). Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, *800*(162), 1–54.

Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control. *Computer*, *48*(2), 85–88.

Humphrey, W. S. (1988). Characterizing the software process: A maturity framework. *IEEE software*, *5*(2), 73–79.

Hurmerinta-Peltomäki, L., & Nummela, N. (2006). Mixed methods in international business research: A value-added perspective. *Management International Review*, *46*(4), 439–459.

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, *21*(4), 574–588.

ITU. (2009). Overview of cybersecurity. https://www.itu.int/rec/T-REC-X.1205-200804-I

Jacob, S. A., & Furgerson, S. P. (2012). Writing interview protocols and conducting interviews: Tips for students new to the field of qualitative research. *Qualitative Report*, *17*, 6.

Jiang, R., Wu, X., & Bhargava, B. (2016). Sdss-mac: Secure data sharing scheme in multi-authority cloud storage systems. *Computers & Security*, *62*, 193–212.

Jin, X., Krishnan, R., & Sandhu, R. (2012). A role-based administration model for attributes. *Proceedings of the First International Workshop on Secure and Resilient Architectures and Systems*, 7–12.

Jin, X., Sandhu, R., & Krishnan, R. (2012). Rabac: Role-centric attribute-based access control. *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, 84–96.

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715.

Kuhn, D. R., Coyne, E. J., Weil, T. R., et al. (2010). Adding attributes to role-based access control. *Computer*, *43*(6), 79–81.

Kumar, P., Moubayed, A., Refaey, A., Shami, A., & Koilpillai, J. (2019). Performance analysis of sdp for secure internal enterprises. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–6.

Kumar, R., Sural, S., & Gupta, A. (2010). Mining rbac roles under cardinality constraint. *International Conference on Information Systems Security*, 171–185.

Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *Journal of information security and applications*, *44*, 64–79.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lane, M., & Marie, M. (2010). The adoption of single sign-on and multifactor authentication in organisations-a critical evaluation using toe framework. *Information in Motion*, *7*, 161.

Love, P. (2003). Document analysis. *Research in the college context: Approaches and methods*, *83*, 96.

Manadhata, P. K., & Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371–386.

Mandke, V. V., & Nayar, M. K. (1999). Modeling information flow for integrity analysis. *IQ*, 38–57.

Manske, K. (2000). An introduction to social engineering. *Inf. Secur. J. A Glob. Perspect.*, *9*(5), 1–7.

McLennan, M. (n.d.). The global risks report 2021 16th edition.

Meuser, M., & Nagel, U. (2009). The expert interview and changes in knowledge production. *Interviewing experts* (pp. 17–42). Springer.

Ministerie van Financiën. (2022). Wet op het financieel toezicht (Wft). https://www.rijksoverheid.nl/onderwerpen/financiele-sector/wet-op-het-financieel-toezicht-wft#:%7E:text=De%20Rijksoverheid%20houdt%20toezicht%20op,geld%20toevertrouwen%20aan%20deze%20instellingen.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Moubayed, A., Refaey, A., & Shami, A. (2019). Software-defined perimeter (sdp): State of the art secure solution for modern networks. *IEEE network*, *33*(5), 226–233.

NCSC. (2020a). Cybersecuritybeeld Nederland (CSBN) 2020. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020

NCSC. (2020b). Factsheet Uw thuiswerkfaciliteiten zijn nu onmisbaar. https://www.ncsc.nl/onderwerpen/veilig-thuiswerken/documenten/publicaties/2020/april/1/factsheet-uw-thuiswerkfaciliteiten-zijn-nu-onmisbaar

NCSC. (2021). Cybersecurity Beeld Nederland 2021. https://www.ncsc.nl/documenten/publicaties/2021/juni/28/csbn-2021

Neideen, T., & Brasel, K. (2007). Understanding statistical tests. *Journal of surgical education*, *64*(2), 93–96.

O'Cathain, A., Murphy, E., & Nicholl, J. (2010). Three techniques for integrating data in mixed methods studies. *Bmj*, *341*.

Omar, R. R., & Abdelaziz, T. M. (2020). A comparative study of network access control and software-defined perimeter. *Proceedings of the 6th International Conference on Engineering & MIS 2020*, 1–5.

Osborn, B., McWilliams, J., Beyer, B., & Saltonstall, M. (2016). Beyondcorp: Design to deployment at google.

Partida, A., Criado, R., & Romance, M. (2021). Identity and access management resilience against intentional risk for blockchain-based iot platforms. *Electronics*, *10*(4), 378.

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). Capability maturity model, version 1.1. *IEEE software*, *10*(4), 18–27.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal*, *15*(5), 13.

Puchta, A., Groll, S., & Pernul, G. (2021). Leveraging dynamic information for identity and access management: An extension of current enterprise iam architecture. *ICISSP*, 611–618.

Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An autonomous cybersecurity framework for next-generation digital service chains. *Journal of Network and Systems Management*, *29*(4). https://doi.org/10.1007/s10922-021-09607-7

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (tech. rep.). National Institute of Standards and Technology.

Salehi, A., Rudolph, C., & Grobler, M. (2020). Attribute-based data access control for multi-authority system. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1834–1841.

Samarati, P., & de Vimercati, S. C. (2000). Access control: Policies, models, and mechanisms. *International School on Foundations of Security Analysis and Design*, 137–196.

Sandhu, R., Ferraiolo, D., Kuhn, R., et al. (2000). The nist model for role-based access control: Towards a unified standard. *ACM workshop on Role-based access control*, *10*(344287.344301).

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38–47. https://doi.org/10.1109/2.485845

SEI. (2002). Capability maturity model® integration (cmmi sm), version 1.1. *CMMI for systems engineering, software engineering, integrated product and process development, and supplier sourcing (CMMI-SE/SW/IPPD/SS, V1. 1)*, *2*.

Shakir, M. (2002). The selection of case studies: Strategies and their applications to is implementation case studies.

Sharma, D. H., Dhote, C., & Potey, M. M. (2016). Identity and access management as security-as-a-service from clouds. *Procedia Computer Science*, *79*, 170–174.

Shlapentokh-Rothman, M., Hemberg, E., & O'Reilly, U.-M. (2020). Securing the software defined perimeter with evolutionary co-optimization. *Proceedings of the 2020 Genetic and Evolutionary Computation Conference Companion*, 1528–1536.

Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device?-a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering*, *6*(1), 1–10.

Smith, S. E., Coyne, J., Youman, C. E., & Ganta, S. (1996). *Charles I*.

Soni, K., & Kumar, S. (2019). Comparison of rbac and abac security models for private cloud. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 584–587.

Stafford, V. (2020). Zero trust architecture. *NIST Special Publication*, *800*, 207.

Stake, R. E. (1995). *The art of case study research*. sage.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research*. Sage publications.

Sturges, J. E., & Hanrahan, K. J. (2004). Comparing telephone and face-to-face qualitative interviewing: A research note. *Qualitative research*, *4*(1), 107–118.

Sturm, D., & Kern, A. (2013). Permission path analysis based on access intelligence. *Proceedings of the 18th ACM symposium on Access control models and technologies*, 253–256.

Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, *20*(1), 1–10.

Törnebohm, J. (2019). Organisational adoption of innovation: A qualitative study on role-based access control in the physical setting of a data centre.

Triangulation, D. S. (2014). The use of triangulation in qualitative research. *Oncol Nurs Forum*, *41*(5), 545–7.

Tsang, E. W. (2013). Case study methodology: Causal explanation, contextualization, and theorizing. *Journal of international management*, *19*(2), 195–202.

Vannoni, M. (2015). What are case studies good for? nesting comparative case study research into the lakatosian research program. *Cross-Cultural Research*, *49*(4), 331–357.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision sciences*, *39*(2), 273–315.

Vijayalakshmi, K., & Jayalakshmi, V. (2021). A similarity value measure of abac security rules. *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, 565–571.

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, *77*, 807–823.

Whiting, L. S. (2008). Semi-structured interviews: Guidance for novice researchers. *Nursing Standard (through 2013)*, *22*(23), 35.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.

Wu, W.-W. (2011). Developing an explorative model for saas adoption. *Expert systems with applications*, *38*(12), 15057–15064.

Xiaojian, Z., Liandong, C., Jie, F., Xiangqun, W., & Qi, W. (2021). Power iot security protection architecture based on zero trust framework. *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, 166–170.

Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020). Dynamic access control and authorization system based on zero-trust architecture. *2020 International Conference on Control, Robotics and Intelligent System*, 123–127.

Yin, R. (2003). Designing case studies. *Qualitative Research Methods*, *5*, 359–386.

Yin, R. K. (1981). The case study as a serious research strategy. *Knowledge*, *3*(1), 97–114.

Yin, R. K. (1998). The abridged version of case study research. *Handbook of applied social research methods*, *2*, 229–259.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.

Zhu, Y., Huang, D., Hu, C.-J., & Wang, X. (2014). From rbac to abac: Constructing flexible data access control for cloud storage services. *IEEE Transactions on Services Computing*, *8*(4), 601–616.

A Interview

Interview protocol (Dutch)

Ten eerste, hartelijk dank dat u wilt meewerken aan mijn thesisonderzoek. Zoals toegelicht in ons eerdere contact, doe ik onderzoek naar de invloed van access controls op security dreigingen en security challenges die bestaan binnen organisaties in de financiële dienstverlening. Het doel van mijn onderzoek is om uitspraken te doen over de manier waarop organisaties binnen de financiële dienstverlening hun IAM systeem hebben geïmplementeerd. Om hier uitspraken over te doen analyseer ik de keuzes/afwegingen, best practises, challenges en toekomstvisie/ambitie van verschillende organisaties. Het interview zal gestructureerd zijn aan de hand van een framework bestaande uit 4 onderwerpen; technisch, ambitie, organisatie/bestuurlijk, omgeving (dreigingen). Aan de hand literatuuronderzoek heb ik al een aantal factoren geïdentificeerd die mogelijk invloed hebben op de implementatie van access controls. Dit interview wil ik gebruiken om vast te stellen of mijn bevindingen uit de literatuur kloppen en om meer inzicht te krijgen in het gebruik van IAM binnen de financiële diensverlening.

Het interview zal ongeveer 45-60 minuten duren en zal tijdens het gesprek worden getranscribeerd. Daarnaast zal er ook een opname gemaakt worden om valide uitspraken en een adequete transcript te realiseren. De opnames worden na analyse direct verwijdert. De opname is alleen beschikbaar voor de mijzelf en zal op geen enkele manier worden gebruikt anders dan voor de analyse van dit onderzoek. In het resulterende thesis wordt uw deelname (en die van uw organisatie) standaard geanonimiseerd.

Interview vragen

1. **Bedrijfs-/persoonsinformatie**

   1.1 Wat is uw rol binnen de organisatie?

   1.2 Uit hoe veel mensen bestaat uw team (het IAM team)?

   1.3 Hoe lang bent u al werkzaam binnen dit domein?

2. **Context**

   2.1 Binnen de IAM wordt er gebruik gemaakt van access controls, welke access control(s) worden er op dit moment gebruikt binnen organisatie X? Sinds wanneer maakt organisatie X gebruik van dit model?

   2.2 Maakt de organisatie gebruik van software van een derde partij? Zo ja, hoe gaan zij om met de availability, effectiveness en efficiency van hun systeem (op welke manier heeft dit invloed op jullie systeem)?

   2.3 Wat zijn de overwegingen vanuit organisatie X om dit model te gebruiken?

3. **Technisch**

3.1 Wat is de organisatie structuur? In hoeverre sluit de op dit moment geimplementeerde access control aan op deze structuur?

3.2 RBAC/ABAC: Hoe veel rollen of attributen heeft uw organisatie ongeveer geidentificeerd binnen het geïmplementeerd model?

3.3 In hoeverre wordt het toegang geven van werknemers tot bepaalde bestanden/mappen als makkelijk ervaren binnen uw team?

3.4 Hoe vaak en op welke manier controlleert uw organisatie de rechten van personen?

3.5 Wat vindt u de voordelen van het gebruik van de op dit moment geimplementeerde access control t.o.v. andere controls? Wat de nadelen?

3.6 Voldoet access control aan alle requirements(organisatie structuur) van de organisatie?

3.7 Wat zijn de concrete problemen/uitdagingen op technisch vlak waar jullie tegen aanlopen?

4. **Organisatorisch**

4.1 Wat is de houding van de werknemers richting het gebruik van deze access control?

4.2 Op welke manier(en) geven jullie je werknemers (hele organisatie) voorlichting in cybercrime?

4.3 Op welke manier zijn werknemers binnen het cyber team van bedrijf X ingelicht en geeduceerd over de bestaande access controls en innovaties?

4.4 Wat is het prioriteit/draagvlak van het information security team binnen de organisatie (#werknemers, ondersteuning)?

4.5 Wat is de houding volgens u vanuit het management richting de access control en cyber security in het algemeen?

4.6 Hoe kijkt het management op financieel gebied naar cyber security binnen organisatie X?

4.7 Wat zou u willen veranderen binnen het cyber security team van uw organisatie?

4.8 Wat zijn de organisatorische problemen/uitdagingen waar het cyber security team nu tegen aanloopt?

5. **Omgevingsinvloeden**

5.1 In hoeverre kijken jullie naar de systemen die jullie concurrenten gebruiken en wordt hier informatie over uitgewisseld?

5.2 Voelen jullie enige druk vanuit de overheid om verbeteringen aan te brengen? (maintenance/governance/improvements)

5.3 Wat is de invloed van nieuwe access control software van de afgelopen jaren geweest op de access control binnen het bedrijf?

5.4 In hoeverre is de organisatie bekend met (nieuwe) externe gevaren?

5.5 Hoe gaat de organisatie om met social engineering (de mens)?

5.6 Hoe gaat uw organisatie om met externe invloeden?

6. **Toekomst**

6.1 Waar wil organisatie X de komende jaren (5 jaar) in groeien binnen information security (wat is nu jullie focus)?

6.2 Welke concrete stappen moeten er gezet worden om dit doel (vorige vraag) te bereiken?

6.3 Ben je bekend met Zero Trust? Zijn jullie binnen de organisatie bezig met de implementatie van Zero Trust?

6.4 Welke problemen/uitdagingen verwacht u te ervaren met Zero Trust?

7. **Afsluiting**

7.1 Vraag om aanvullende informatie of opmerkingen.
7.2 Nogmaals bedankt voor de tijd en waardevolle inzichten.
7.3 Vraag of u de expert later in het proces kunt benaderen als er een andere vraag is.
7.4 Vraag of de expert de case study wil ontvangen na afronding van het onderzoek.

Interview protocol (English)

First of all, thank you for your willingness to participate in my thesis research. As explained in our previous contact, I am researching the influence of access controls on security threats and security challenges that exist within organisations in the financial services industry. My research aims to make statements about how organisations within the financial services have implemented their IAM system. To make statements about this, I analyse various organisations' choices/considerations, best practices, challenges, and future vision/ambition. The interview will be structured based on a framework consisting of 4 topics; technical, ambition, organisation/administrative, environment (threats). Based on a literature review, I have already identified several factors that may influence the implementation of access controls. I want to use this interview to determine whether my literature findings are correct and gain more insight into the use of IAM in financial services.

The interview will last approximately 45-60 minutes and will be transcribed during the interview. In addition, a recording will also be made to realise valid statements and an adequate transcript. The recordings are immediately deleted after analysis. The recording is only available to me and will not be used other than for the analysis of this research. In the resulting dissertation, your participation (and that of your organisation) is anonymised by default.

Question interview

1. **Company/Personal Information**

   1.1 What is your role within the organisation?
   1.2 How many people do your team (the IAM team) consist of?
   1.3 How long have you been working in this domain?

2. **Context**

   2.1 Access controls are used within the IAM, which access control(s) are currently used within organisation X? Since when has organisation X been using this model?
   2.2 Does the organisation use a third-party software? If so, how do they deal with the availability, effectiveness and efficiency of their system (how does this affect your system)?
   2.3 What are the considerations from organisation X to use this model?

3. **Technical**

   3.1 What is the organisational structure? To what extent does the currently implemented access control match this structure?
   3.2 RBAC/ABAC: Approximately how many roles or attributes has your organisation identified within the implemented model?
   3.3 To what extent is giving employees access to certain files/folders experienced as easy within your team?
   3.4 How often and how does your organisation check the rights of individuals?
   3.5 What do you think are the advantages of using the currently implemented access control over other controls? What are the cons?
   3.6 Does access control meet all requirements(organisational structure) of the organisation?
   3.7 What are the concrete technical problems/challenges that you encounter?

4. **Organizational**

- 4.1 What is the attitude of the employees towards the use of this access control?
- 4.2 In what way(s) do you provide your employees (entire organisation) with information about cybercrime?
- 4.3 How are employees within the cyber team of company X informed and educated about the existing access controls and innovations?
- 4.4 What is the organisation's priority/support of the information security team (#employees, support)?
- 4.5 What is the attitude of management towards access control and cyber security in general?
- 4.6 How does the financial management view cyber security within organisation X?
- 4.7 What would you like to change within your organisation's cyber security team?
- 4.8 What are the organisational problems/challenges that the cyber security team is currently facing?

5. **Environmental influences**

   - 5.1 To what extent do you look at your competitors' systems, and is information exchanged about this?
   - 5.2 Do you feel any pressure from the government to make improvements? (maintenance/ governance/improvements)
   - 5.3 What has been the influence of new access control software in recent years on access control within the company?
   - 5.4 To what extent is the organisation aware of (new) external hazards?
   - 5.5 How does the organisation deal with social engineering (people)?
   - 5.6 How does your organisation deal with external influences?

6. **Future**

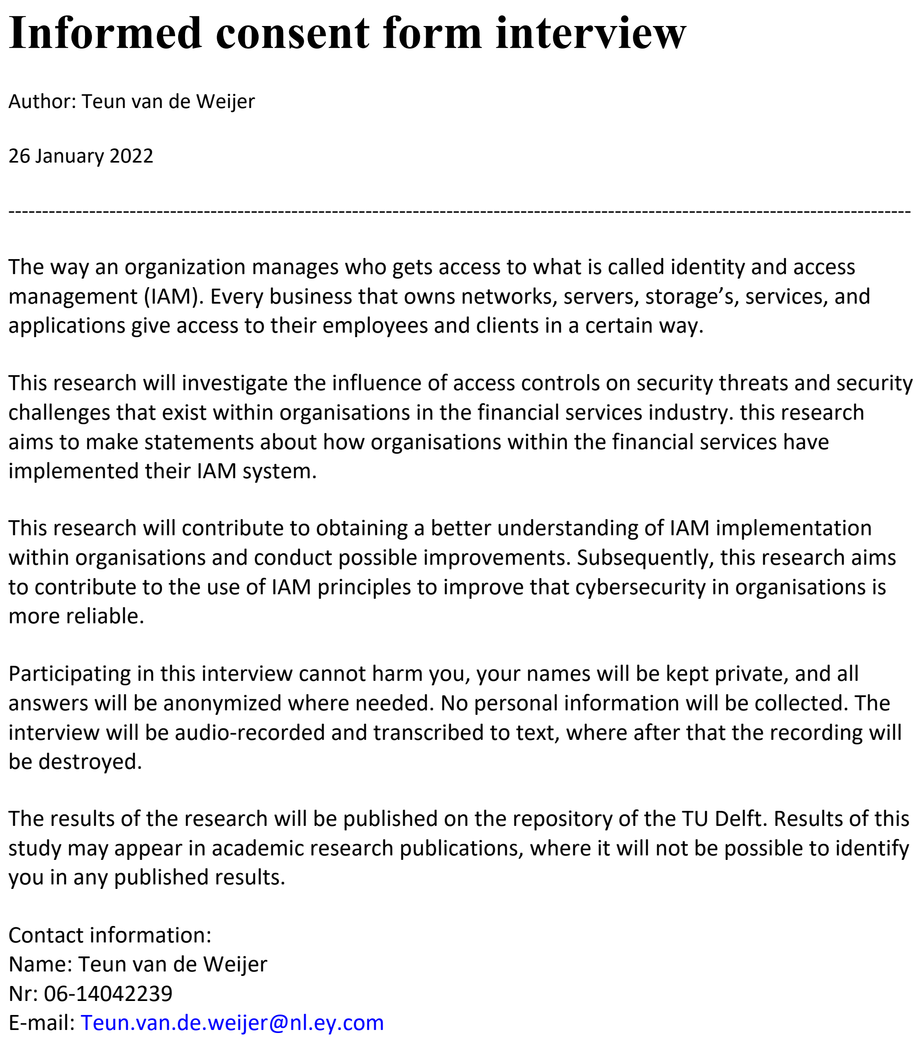
   - 6.1 Where does organisation X want to grow in the coming years (5 years) within information security (what is your focus now)?
   - 6.2 Which concrete steps must be taken to achieve this goal (previous question)?
   - 6.3 Are you familiar with Zero Trust? Are you working on the implementation of Zero Trust within the organisation?
   - 6.4 What problems/challenges do you expect to experience with Zero Trust?

7. **Closing**

   - 7.1 Ask for additional information or comments.
   - 7.2 Thank again for the time and valuable insights.
   - 7.3 Ask if you can approach the expert later on in the process if there is another question.
   - 7.4 Ask if the expert wants to receive the case study after the completion of the research.

B

Informed consent form



Informed consent form interview

Author: Teun van de Weijer

26 January 2022

The way an organization manages who gets access to what is called identity and access management (IAM). Every business that owns networks, servers, storage’s, services, and applications give access to their employees and clients in a certain way.

This research will investigate the influence of access controls on security threats and security challenges that exist within organisations in the financial services industry. this research aims to make statements about how organisations within the financial services have implemented their IAM system.

This research will contribute to obtaining a better understanding of IAM implementation within organisations and conduct possible improvements. Subsequently, this research aims to contribute to the use of IAM principles to improve that cybersecurity in organisations is more reliable.

Participating in this interview cannot harm you, your names will be kept private, and all answers will be anonymized where needed. No personal information will be collected. The interview will be audio-recorded and transcribed to text, where after that the recording will be destroyed.

The results of the research will be published on the repository of the TU Delft. Results of this study may appear in academic research publications, where it will not be possible to identify you in any published results.

Contact information:
Name: Teun van de Weijer
Nr: 06-14042239
E-mail: Teun.van.de.weijer@nl.ey.com

C

Definitions variables

	Initial	Managed
1. Technological		
1.1 Relative advantage	The organisation is not aware (not actively searching) for of any disadvantages or advantages of the IAM system in place	The organisation is aware (not actively searching) of a few disadvantages and advantages of their IAM system in comparison to other IAM systems but the organisation are not actively trying to improve the IAM system
1.2 Compatibility	The organisation is not aware of any shortcomings of their IAM system, only via third party assessments do these come to light	The organisation is aware that the IAM system should meet the requirements, protocols are in place when problems occur
1.3 Complexity	The IAM system is complex and therefore is not maintained and supervised by the organisation	Although the IAM system's complexity the organisation maintains and supervises the system themselves
2. Organisational		
2.1 Organisational competency (readiness)	The IAM strategy is not defined and responsibilities are not assigned for some aspect of IAM	IAM strategy is loosely defined, responsibilities are loosely assigned for some aspect of IAM, there is a shortage of cyber security employees
2.2 Top management	IAM strategy is not defined, executive management is not involved in IAM and no financial resources are being allocated	IAM strategy is loosely defined, executive management is informed of IAM strategy but are not involved and, if needed, few financial resources are made available
2.3Training and education	Organization offers no form of IAM training or education	Organization offers online (voluntary) IAM training (mostly for new joiners)
2.4 Ambition	IAM strategy is not defined, no steering committee, architecture review board or similar design authority in place to approve IAM policy, strategy, procedure or initiatives	IAM strategy is loosely defined; may not be comprehensive or consistent across the enterprise, IAM governance is provided in silos reside in business lines in various forms
3. Environmental		
3.1 Competitive pressure	The organization is not aware of what its competitors are doing and compliance procedures are ad-hoc and inconsistent	The organization is aware of what its competitors are doing but does not care much about them and the compliance procedures exist but are not documented or communicated
3.2 Trading partner support	The software supplier offers no support for the IAM software	The software supplier offers little support for the IAM software
3.3 External Threats	The organisation is not aware of the external threats and is actively monitoring it's environment	The organisation is aware of external threats but not actively monitoring and mitigating them
4. Perceived usefulness		
4.1 Ease of use (employee)	Employees do not understand the IAM system, employees do not know what is expected from them on risk mitigation and are not helped in understanding the system and risks	Employees do understand the use of the IAM system and do not mitigate any risk, but they do know the risks involved
4.2 Usefulness (firm)	Inconsistent IAM processes may be in effect across business lines and the processes have not been defined or documented	Similar IAM processes are adopted across business units, however, they are not consistent, and may not be documented or effectively communicated, IAM processes and procedures are mostly manual and not transparent to the end user
5. Adoption intention		
5.1 Willingness to innovate	The organisation do not know about and is not actively searching for new technologies that could improve their IAM system	The organisation do not know about new technologies that could improve their IAM system, but is not actively searching for new technologies, but has an open attitude towards IAM improvements/innovation

Table C.1: Definitions of the variables per maturity level 1/3

	Defined	Quantitatively Managed
1. Technological		
1.1 Relative advantage	The organisation is aware (actively searching) of advantages and disadvantages of the IAM system and the IAM system control has a balanced number of advantages and disadvantages compared to other access controls	The organisation is aware (partly autonomous searching) of the advantages and disadvantages of the IAM system and the organisation is continuously improving the system
1.2 Compatibility	The organisation is continuously monitoring their IAM system to check whether it still meets the requirements	The organisation is continuously monitoring and improving their IAM system
1.3 Complexity	The IAM system is, although it's complexity, understandable and the system is maintained and supervised by the organisation	The understanding of the complexity of the IAM system is continuously improved making it less time consuming to maintain and supervise
2. Organisational		
2.1 Organisational competency (readiness)	IAM strategy and roadmap has been clearly defined and communicated, responsibilities for IAM are clearly assigned, managed, and enforced	IAM strategy and roadmap has been clearly defined and communicated, progress is constantly monitored and improvements are made when needed
2.2 Top management	IAM strategy and roadmap has been clearly defined and communicated, executive management is informed of state of IAM program and few financial resources are made available	IAM strategy and roadmap has been clearly defined and communicated, progress is constantly monitored, improvements are made when needed and, when needed, financial resources have been made available
2.3Training and education	The organization provides (mandatory) IAM training for the riskiest profiles within the company	Organization provides (mandatory) IAM training several times a year
2.4 Ambition	IAM strategy and roadmap has been clearly defined, communicated and is consistent across all business units but implementation may not be specified for some business units, enterprise level function exists to approve IAM strategy, policy, waivers, and exceptions	IAM strategy and roadmap has been clearly defined and communicated, IAM is a joint responsibility of all business units (including IT) and is aligned with general corporate business objectives and IAM Authority, architecture review board or similar approval authority approves IAM implementation plans and technology adoption
3. Environmental		
3.1 Competitive pressure	The organization is aware and cares what its competitors are doing and compliance procedures are documented	The organization is constantly monitoring their surroundings and compliance processes are automated where possible
3.2 Trading partner support	The software supplier provides support for the IAM software	The software supplier provides support and continuously monitors their IAM software
3.3 External Threats	The organisation is aware of external threats and have systems in place to manage and detect any risks	The organisation is aware of external threats and are continuously reacting on the perceived threats
4. Perceived usefulness		
4.1 Ease of use (employee)	Employees understand the use of the IAM system, the risks involved and try to mitigate them, but there is little support from the organisation	Employees understand the use of the IAM system, the risks involved and try to mitigate them, and the organisation is supporting them
4.2 Usefulness (firm)	IAM processes and procedures have been defined, validated, documented, and made available to affected parties, the processes provide adequate coverage for all the aspects of the IAM framework	IAM processes and procedures are reviewed and updated periodically or as a result of significant change to the business (e.g., regulatory changes, mergers, new business initiatives, etc.), processes are actively maintained as requirements or technologies change and key process metrics are captured and analyzed to determine the effectiveness, appropriateness, and feasibility of IAM processes
5. Adoption intention		
5.1 Willingness to innovate	The organisation knows about new technologies that could improve their IAM system and has an open attitude towards IAM improvements/innovation, but is not actively searching for new technologies that could improve their IAM system	The organisation knows about new technologies that could improve their IAM system, has an open attitude towards IAM improvements/innovation and is actively searching for new technologies that could improve their IAM system

Table C.2: Definitions of the variables per maturity level 2/3

	Optimizing
1. Technological	
1.1 Relative advantage	The organisation is autonomously monitoring their IAM system and has indicated few disadvantages over other IAM systems
1.2 Compatibility	The organisation autonomously monitors their IAM system and is actively searching for innovations of the systems
1.3 Complexity	The IAM system is easy to understand and therefore is efficiently maintained and supervised
2. Organisational	
2.1 Organisational competency (readiness)	IAM strategy is consistently implemented across all business units and is aligned with general corporate business objectives. IAM requirements are clearly defined and included in a verified plan
2.2 Top management	Senior management participates actively in the governance process and financial resources are available
2.3Training and education	Organization provides (mandatory) IAM training several times a year and uses constant monitoring and using phishing security tests
2.4 Ambition	Senior management participates in the governance process and constantly monitors progress on the organisation's defined readmap
3. Environmental	
3.1 Competitive pressure	The organization is actively monitoring competitors, adjusting its own IAM strategy accordingly and regulations are reviewed for impact on IAM compliance
3.2 Trading partner support	The software supplier offers active support and updates the IAM software frequently
3.3 External Threats	The organisation is aware of external threats and actively monitoring/mitigating/improving their IAM system
4. Perceived usefulness	
4.1 Ease of use (employee)	Employees understand the impact of the use of the IAM system and both the organisation and employees are actively involved in the mitigation of risk and system improvements
4.2 Usefulness (firm)	Most IAM processes are systematic and automated, processes allow for risk based decision and enforcement
5. Adoption intention	
5.1 Willingness to innovate	The organisation knows about new technologies that could improve their IAM system, has an open attitude towards IAM improvements/innovation, is actively searching for new technologies that could improve their IAM system and continuously trying to implement them

Table C.3: Definitions of the variables per maturity level 3/3