Automated external fraud prevention in the public sector

What is keeping public organisations from applying IT for controlling fraud in society in a fully automated way?

Master thesis

P.S. Bolscher

29-8-2014

Contact information

Author

Name:	P.S. (Peter) Bolscher
Address:	Bornsestraat 13, 7627 NS, Bornerbroek, The Netherlands
Study:	Business Information Technology, University of Twente, Enschede
Student number:	s1008935
E-mail:	bolscher.peter@kpmg.nl

First supervisor

Name:	Dr. Ir. A.A.M. (Ton) Spil
Function:	Assistant Professor in Industrial Engineering and Business Information Systems
Faculty:	School of Management and Governance (SMG)
Phone:	+31-53-4893497
E-mail:	a.a.m.spil@utwente.nl

Second supervisor

Name:	Dr. Ir. M.J. (Marten) van Sinderen
Function:	Associate Professor in Information Systems
Faculty:	Electrical Engineering, Mathematics and Computer Science (EEMCS)
Phone:	+31-53-4893677
E-mail:	m.j.vansinderen@ewi.utwente.nl

External supervisor

Name:	Henk Hendriks
Function:	Senior Manager at KPMG, Risk Consulting IT Advisory De Meern
Phone:	+31-50-5222158
E-mail:	hendriks.henk@kpmg.nl

External organisation

Name:	KPMG N.V.
Business unit name:	Risk Consulting IT Advisory De Meern
Office address:	Zuiderzeelaan 33, 8017 JV, Zwolle

Preface

This thesis is the final result of my graduation at the University of Twente for the study Business Information Technology (MSc). I started in the beginning of February 2014 with this graduation project at KPMG, and it has been an interesting experience for me.

The initial start was excellent, with a warm welcome from all KPMG colleagues, who immediately helped me to fit in and assisted in scoping the subject of the thesis. Unfortunately, only three weeks after I started, I broke my leg in a football match. During the miserable weeks I spent at home, I received much support from my KPMG colleagues, my supervisors, my friends and family, my fellow team members and many others. This meant a lot for me during that time and also helped me to regain my spirit. Special thanks go to all persons that supported me during that period.

After I was able to walk again, I continued the project at full speed, which resulted in finishing this thesis with a happy ending. To achieve this, I had much help and support for which I would like to thank a number of persons.

First of all, I would like to thank my supervisor from KPMG, Henk Hendriks, for his useful comments about the thesis and all his time and guidance during the project. Regarding the latter, I also thank all other KPMG colleagues who helped me with this, and for providing a great work atmosphere.

Secondly, I would like to thank my supervisors from the University of Twente, Dr. Ir. Ton Spil and Dr. Ir. Marten van Sinderen, for their helpful advices and comments about the thesis and the graduation project in general. Their help led to great insights and improvements to this thesis.

Thirdly, I would like to thank the experts from the four public sector organisations for their time and sharing of knowledge, both during and after the interviews I performed with them.

Finally, I would like to thank my friends and family in general, for helping me throughout my studying life, and making it fun. Especially my family members always supported me during my education, and helped me to reach where I stand today.

Peter Bolscher

Zwolle, August 2014

Management Summary

Fraud incidents in the public sector gained much attention in recent years, and governments are increasingly realising that the mitigation of fraud risks must be improved. Especially some embarrassing cases of external fraud showed that current solutions for the prevention and detection of fraud incidents are not sufficient.

Both vertical (between governmental and non-governmental parties) and horizontal (between non-governmental parties) external fraud can be considered, and governments have a responsibility to prevent and detect them, which we all combined under the term external fraud prevention. Improving controls in internal control processes can lead to highly effective solutions, and we decided to further study this. Looking at the Dutch government, automated IT controls are becoming more attractive for external fraud prevention, which is why we focussed on them in this thesis.

However, some problems became apparent. First, existing research about applying automated IT controls for external fraud prevention in the public sector was lacking. Several scholars have argued that differences between the public and private sector cause that proven approaches from the private sector cannot be easily transferred for usage in the public sector. Therefore, we studied which specific public sector characteristics influence the applicability of automated IT controls for external fraud prevention, and in which way they do so. Secondly, it was unknown if current standards and frameworks for developing automated IT controls could be used in the public sector for external fraud prevention, or if they needed to be tailored. Therefore, we studied if current, widely-used standards and frameworks for the development of automated IT controls should be tailored to incorporate the influence of such characteristics in the public sector. When this would be the case, we would design guidelines that describe how they should be tailored.

In order to solve these problems, we first summarised knowledge from literature that explained how the risk of external fraud can be mitigated by automated IT controls. The concept of internal control played an important role here, since automated IT controls can be part of it, and several standards and frameworks were discussed that could later be used to assess if they need tailoring, as mentioned previously. After that, a literature review was conducted to identify what public sector characteristics are, and we accordingly proposed which of these could potentially influence the applicability of automated IT controls for external fraud prevention.

An observational case study was subsequently performed, in which interviews with experts of four Dutch public organisations were conducted, to observe in practice which of the identified public sector characteristics actually influence how automated IT controls can be applied for external fraud prevention. The guidelines could then be designed based on these findings.

During the case study, support was found for five influential categories of public sector characteristics. In Table 1, we present the observed effects they have on the applicability of automated IT controls for external fraud prevention. Next to this, most of the categories were mainly supported by one dominant influential factor, which we will also mention. But first, we will shortly describe these categories.

- *Environment*; the environment and network that public organisations are situated in, including the actors, and relations with and between them.
- *Goals & Values;* goals and values that are specific to public organisations, because they serve the public interest.
- *Political control & Bureaucracy;* public organisations are subjected to political authority and specific legislations, and this could include bureaucratic procedures.
- *Resources & Capabilities;* the specific resources that are available to public organisations, which are different from those available to private organisations, and the capabilities to use them.
- *Uniqueness of Tasks & Position;* public organisations perform unique tasks or hold unique positions for the execution of their tasks, which private organisations do not have.

Table 1. The influential categories of public sector characteristics, and their corresponding effect and dominant factor

Category	Effect	Dominant factor
Environment	Negative	Influence of pressure groups
Goals & Values	Very negative	Public value of carefulness
Political control & Bureaucracy	Negative	Legal constraints of privacy
Resources & Capabilities	Very positive	Possibilities for high data sharing
Uniqueness of Tasks & Position	Positive	Unique powers for controlling purposes

An additional, very negatively influencing category was found that could not yet be assigned to a sector. This category is Failing Technology/Manual Necessity, which we can best describe by mentioning the three dominant factors from this category: 1) inability to create reliable risk profiles, 2) inability to extract data automatically, and 3) necessity of a 'human eye' in control processes. These factors all pose constraints on the ability to apply automated IT controls for external fraud prevention. Together with the public value of carefulness, we argue that these characteristics are the most dominant factors for constraining the possibilities for automated external fraud prevention in general.

After that, we judged that current standards and frameworks need tailoring for three of these five categories, that were not sufficiently incorporated in them: Goals & Values, Resources & Capabilities, and Uniqueness of Tasks & Position. Specific guidelines were designed that described what has to be added to such standards and frameworks in general. Finally, we presented recommendations about the possibilities for applying automated IT controls for external fraud prevention, and automated external fraud prevention in general.

The theoretical contributions of this thesis are the following. The influential categories of public sector characteristics add to the understanding that public sector characteristics can actually have influence on how IT solutions can be applied. Scientifically based evidence is thus provided for the extensive debate

on the differences between public and private sectors. Furthermore, we studied an extended role of automated IT controls within the internal control concept, but had to conclude that it is not suitable to fully prevent external fraud.

Practical contributions were also identified. Public organisations and KPMG can use the gained knowledge to assess which essential characteristics cannot be overlooked when determining how to develop appropriate automated controls for external fraud prevention. When using current standards and frameworks for this developmental process, this thesis adds guidelines that tailor these standards and frameworks to be certain of the inclusion of these essential characteristics. Also, the general recommendations assist in recognising current opportunities and constraints for automated external fraud prevention in the public sector.

Further research is necessary for, among others, providing more evidence about the results, and to gain more certainty about the actual effectiveness of automated IT controls for external fraud prevention in the public sector.

Table of contents

Part III

Part IV

Part I

Part I is the introductory part of this thesis. This part first explains what the background of this thesis is, to get a first impression of the context and subjects at hand. Subsequently, we go in more detail about specific problems that become apparent within that context. These problems describe both a theoretical and practical problem, for which we aim to find answers and solutions. This ensures that the thesis is relevant to theory and practice.

After we describe these problems in the problem statement, we determine the research goals, on which the research questions of this thesis are accordingly based. The answering of these questions should lead to a theoretical knowledge gap being filled, and a practical problem being solved. Then, we discuss how the research questions will be answered by setting up the methodology. Before we execute these research plans starting from Part II and onwards, we explain the theoretical and practical relevance of the research, and highlight the structure of this thesis.

1 Introduction

This chapter provides an introduction to this research. First, we describe the background of this research, after which the main problem is identified for which we want to find a solution. Next, we define the research goals and the research questions of this research. After that, the methodology and the relevance of this thesis are discussed. Finally, the structure of this thesis is explained.

1.1 Background

Risk Management has increasingly gained attention of both researchers and practitioners during the last decade [1]. Continuously identifying and handling risks, especially mitigating threats, have become important activities for many (top) managers and executives. This way, the occurrence of certain threats can be properly prepared or even prevented, and opportunities can be addressed. Furthermore, researchers increasingly suggest to perform Risk Management activities on an organisational-wide level, which is apparent in upcoming concepts as Enterprise Risk Management (ERM) [7] and Governance, Risk & Compliance (GRC) [65], taking Risk Management to the board room.

The Dutch government is also becoming aware of the importance of having proper organisational-wide Risk Management, which can contribute to reducing the risks of errors and fraud. Due to recent media attention for fraud incidents, which showed that its annual costs are millions and sometimes even billions of Euros [64], the Dutch government has increased attention for mitigating this risk [75]. Such fraud incidents are not only caused internally by employees, but also externally by Dutch organisations, citizens or even foreigners. For example, there was a case in which Bulgarians committed fraud with Dutch governmental allowances [75].

The problem of fraud with public resources, committed by external parties, is also apparent in other countries. According to the AIC 2008-09 survey on fraud [8], governmental losses due to entitlement fraud in Australia were 489 million dollars ($A), and public sector losses in the United Kingdom were 17.6 billion pounds (£), from which 15.2 billion due to tax fraud and 1.1 billion related to fraud with benefits. Although the survey was some years ago, it still shows how big the impact of externally committed fraud can be to public sector organisations.

The previously discussed fraud incidents are all examples of vertical fraud, which is fraud committed by non-governmental parties to a government. Horizontal fraud is fraud committed between non-governmental parties, which does not affect a government directly. An example of this is when an untraceable person is intentionally assigned as the owner of a company with debts, and leaves behind private creditors who are unable to receive their payments when the company is made bankrupt. Governments can also have the responsibility to prevent such kinds of horizontal fraud. Therefore, both vertical and horizontal fraud can be considered as external fraud to public sector organisations.

We define external fraud in this thesis as a deliberate deception in order to gain an advantage in an unlawful way [39], committed by non-governmental parties, while a governmental party has the responsibility to prevent or stop its occurrence. Both governments and society are thus affected by several kinds of external fraud that are being committed. For the prevention and detection of external

fraud, certain internal controls that should mitigate the external fraud risks have already been installed within governmental organisations.

However, there is still much to be done when it comes to preventing the occurrence of external fraud in advance or detecting it in an early stadium. Known cases of external fraud that were committed for a long time, with individual cases going up to 600,000 pounds (£) of damage [10], call for improved proactive prevention and detection of external fraud. This is strengthened by the rather disappointing fact that in 60% of discovered cases of fraud in the UK, it tends to be discovered by tip-offs or by accident [38]. Although a survey from the AIC reported a very high percentage (90%) of discoveries by internal controls, audits or investigations [8], a more recent PWC survey [63] found a very similar percentage (59%) for discovery by tip-offs or by accident as mentioned before. Since there is more evidence for a huge dependency on tip-offs and accidental discoveries, this shows the weakness of current prevention and detection mechanisms. A KPMG survey partly acknowledges this weakness, since 47% of respondents from different organisations indicated that poor internal controls or the overriding of internal controls was the most important factor that contributed to their largest fraud incident [45].

The Dutch government is already trying to prevent some kinds of external fraud by tightening laws [75], but this only solves a part of the problem. Improving the internal control process on external fraud, by improving controls, is another possibility that can be highly effective [57]. IT could be used to automate parts of mainly manual control processes, which might lead to improved and quicker controlling on such fraud. Implementing more IT controls in the internal control systems of the government could therefore be a solution.

According to Flowerday & von Solms [28], IT controls provide general and technical controls over the policies, processes, systems and people that comprise an IT infrastructure, and supports governance and business management. In addition, IT controls form a part of an internal control system and allow organisations to adapt to risks, by automating business and controlling the IT accordingly. The authors also stress that risk indicators point to a need for controls, which emphasizes that Risk Management can provide the basis for IT controls.

Implementing more IT controls, and especially automated IT controls, is becoming more attractive for the Dutch government for several reasons. First, since the government is struggling to find resources to control on all kinds of external fraud manually by employees, automating parts of control processes can lead to increased prevention and improved detection of fraud with possibly even less resources. Second, the potential of automated IT controls has grown since the government has been centralising essential data about citizens and organisations in accessible databanks, making it easier to automatically collect data for controlling purposes.

1.2 Problem statement

IT controls are increasingly being used and gained more attention in the last decade, mainly due to changing legislation such as the Sarbanes-Oxley Act, making IT governance an even more important concept [1]. IT controls are part of the more general concept of IT governance, on which a large amount of research is focused.

According to Liu & Ridley [49], little literature has been published on IT governance in the public sector. A conclusion from the little literature that has been published on this topic, is that "IT governance in the public sector is different to that in the private sector due to characteristic differences between the two sectors", and that it is more complex in the public sector. Some examples of differences apparent in the public sector compared to the private sector that the authors mention, are shown in Table 2.

Table 2. Differences apparent in the public sector compared to the private sector, according to Liu & Ridley [49]

Differences	Examples apparent in the public sector
Differences in environmental factors	• Less market exposure • More legal and formal constraints
Differences in organisation-environment transactions	• More mandatory powers • Wider scope of concern
Differences in internal structures and processes	• More complex criteria • More frequent rollover of top managers

In addition, specific public sector characteristics can be 1) a bureaucracy in which legislation and policies are changed regularly, and 2) a complex network of interdependent organisations with a variety of stakeholders [13]. This all indicates that there are very clear differences between these two sectors. In addition, Sethibe et al. [71] argue that a 'one-size-fits-all' approach for IT governance is not appropriate when studying the public and private sector, and that failure to address the differences between the two sectors will be a mistake.

Because IT controls are part of the more general concept of IT governance, this implies that there is also little literature on IT controls in the public sector. Furthermore, the conclusions about IT governance might also hold for IT controls. Although the usage of some IT controls will be very similar for both the private and the public sector, many differences can be expected due to specific public sector characteristics. Research about IT controls in the public sector is limited, but necessary, especially when considering that automated IT controls are becoming more interesting for the Dutch government for external fraud prevention. We will use the term 'external fraud prevention' for both the prevention and detection of external fraud in the public sector.

Research on IT controls in the public sector is thus lacking, and it is therefore unknown which characteristics that are specific to the public sector influence the applicability of automated IT controls for external fraud prevention. Furthermore, it is unknown if current standards for developing automated IT controls in the public sector are complete, since these characteristics might indicate that current standards must be tailored because of the unique nature of many external fraud prevention activities in the public sector. Here, applicability comprises the extent to which these controls can be applied in a certain situation, which is dependent on organisational, legal, technical and other constraints, in order to reach their goal. This pertains not only to the technology itself, but also to underlying reasons that may influence if automated IT controls are suitable to apply.

To conclude, proper knowledge about specific public sector characteristics that are influencing the applicability of automated IT controls for external fraud prevention is lacking, and organisations in the

public sector might continue to struggle with implementing them because of that. Preventable external fraud might still occur or is detected in a late stadium because of this lack of knowledge, and it is unknown if current standards for developing automated IT controls, which mainly focus on the private sector, can be used in the public sector for external fraud prevention. The relations between the concepts described here, and the two questions that arise, are depicted in Figure 1.

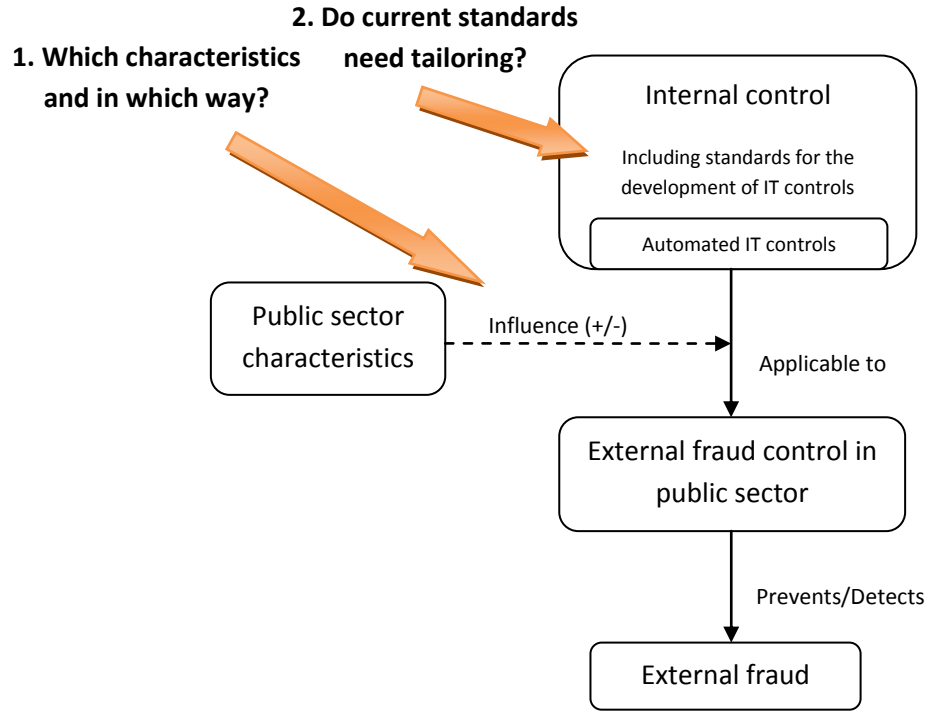

Figure 1. Relations between the different concepts of this thesis and the questions that arise

1.3 Research goals

The goal of this research is twofold, based on the previously described problems.

1 Determine which and in which way characteristics specific to the public sector influence the applicability of automated IT controls for external fraud prevention.

This links two subjects to each other: specific public sector characteristics, and automated IT controls for external fraud prevention. What is the result that we aim for by linking quite a high-level and a low-level concept with each other? External fraud prevention has become more important for the Dutch government, eventually leading to increased possibilities for automated IT controls. However, specific public sector characteristics might influence the way such controls can be applied to the public sector. Research about this potential relation is lacking, and we therefore aim to determine which and in which way such characteristics influence the applicability of automated IT controls.

In Figure 2, we present how the high-level concept of public sector characteristics and the low-level concept of automated IT controls are in this research combined on a mid-level. We do not aim to discuss

detailed IT requirements for the automated IT controls that we will treat in this thesis, but mainly focus on more high-level descriptions of the possibilities of applying such controls.

With respect to automated IT controls, we do not aim to take all kinds of IT controls and study their applicability. Instead, our goal is to discuss specific IT controls that potentially could take over parts of current control processes on external fraud, and accordingly determine if their applicability is influenced by specific public sector characteristics. Therefore, scenarios can be used. We want to find generic characteristics that apply to Dutch public sector organisations, and aim to explain accordingly that the same characteristics will also apply to certain public sector organisations in other countries.

2 Design guidelines for tailoring current standards, for developing automated IT controls for external fraud prevention in the public sector.

These guidelines will be based on the previously mentioned characteristics that we aim to find, and already known standards and frameworks for the development of internal control or IT controls from a Risk Management perspective. This way, we study external fraud from a risk perspective, which assists in identifying and mitigating fraud risks [38], and leads to a need for certain controls [28].

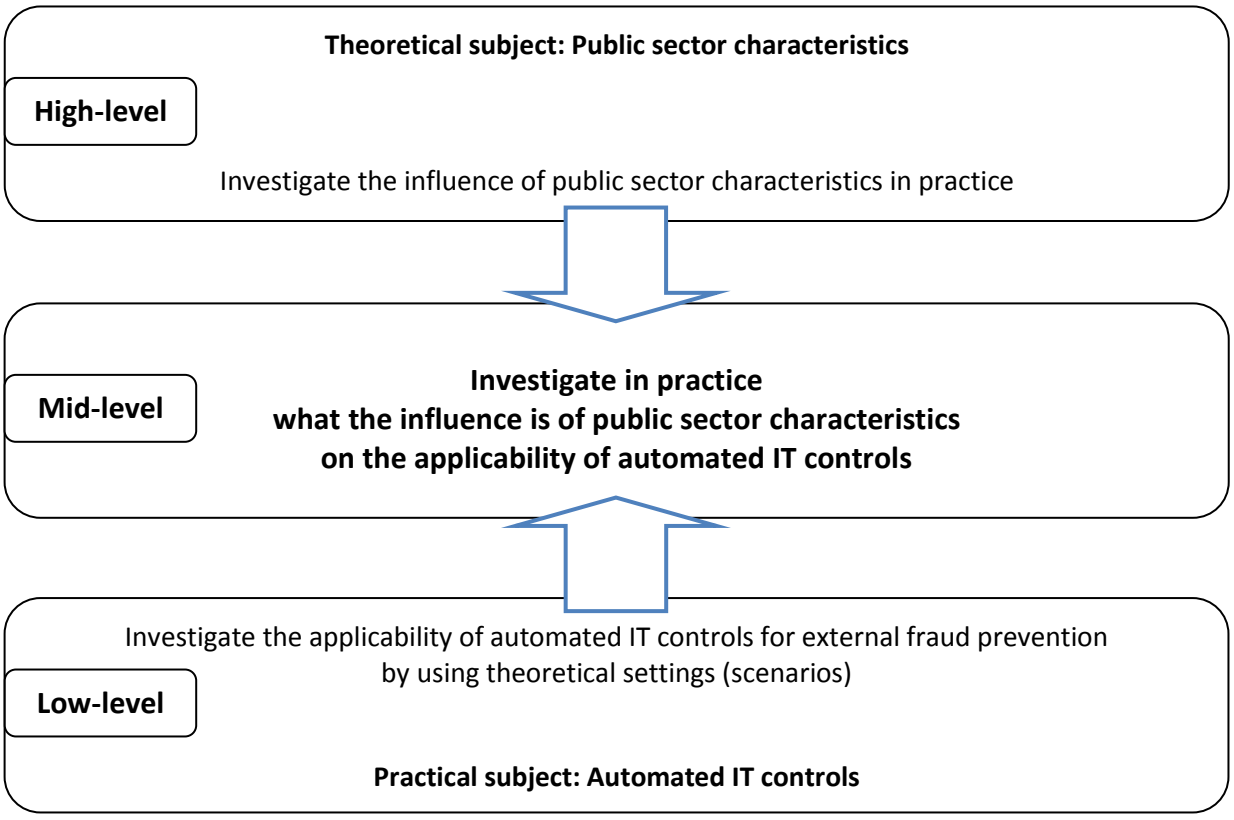

Figure 2. Representation of the concepts on different levels, and how they are combined

1.4 Research questions

Based on the previously stated problems and goals, we pose the following **main research question** *(MQ)*:

> *How must current standards for developing automated IT controls be tailored to include the effect of specific public sector characteristics on the applicability of such automated IT controls, for external fraud prevention in the public sector?*

In order to answer this main research question in a structured way, we pose the following four **sub research questions**:

- *Q1 What is current knowledge about using Risk Management to assess external fraud?*
- *Q2 What are current standards for developing automated IT controls from a Risk Management perspective?*
- *Q3 What is current knowledge about characteristics specific to the public sector?*
- *Q4 Which and in which way do public sector characteristics influence the applicability of automated IT controls for external fraud prevention?*

The purpose of the first three sub research questions is to gain current knowledge and background information in order to answer the last sub research questions and the main research question, from which new knowledge and new guidelines are expected.

First, we want to examine how Risk Management can be used to assess external fraud (Q1). This way, external fraud is considered as a risk, and according to Flowerday & von Solms [28], such risk indicators can point to a need for controls.

Therefore, we then want to collect knowledge from existing approaches that describe how automated IT controls can be developed from a Risk Management perspective (Q2). After answering these two questions, we should know how external fraud can be assessed by using a Risk Management approach, and how automated IT controls can be developed from that. The purpose is to attain the most relevant knowledge about these topics, not to give an exhaustive literature review.

Thirdly, we identify characteristics that are specific to the public sector (Q3). In essence, literature about this topic must be reviewed to gain current knowledge about these characteristics. The characteristics serve as the potential influential factors we are looking for when answering the next research question.

The purpose of the fourth sub research question is to identify which characteristics specific to the public sector influence the way automated IT controls can be applied for external fraud prevention, and in which way they influence this (Q4). New knowledge is generated here, since research about this potential relationship is non-existent. In turn, this knowledge can be used for answering the main research question.

The aim of the main research question is to design generic guidelines for tailoring current standards for the development of automated IT controls, used for preventing external fraud in the public sector (MQ). Gained knowledge from all previously discussed sub research questions is used here. Answering this

question must lead to guidelines that tailor current standards for the development in different public sector organisations, for different kinds of external fraud. This should extend existing good practices, instead of replacing it.

1.5 Methodology

In this section, we discuss the methodology of how the research questions will be answered. Because we eventually want to design an artefact, a design science methodology is chosen, partly following Peffers et al. [60]. But before we come to the design activity, we need to start with answering the first three research questions, which are knowledge questions, in order to:

- fully understand the problem,
- present current knowledge, and
- describe objectives of the solution [60].

The first two research questions (Q1, Q2) will be answered by qualitatively examining literature, and existing standards and frameworks, to come up with a summary of relevant knowledge about the topics.

The third research question (Q3) will be answered by performing a systematic literature review, based on Wolfswinkel et al. [77], in order to collect a high-quality sample of currently known public sector characteristics. In addition, hypotheses are proposed that describe the expected influence of such characteristics on the applicability of automated IT controls for external fraud prevention. Both the hypotheses and characteristics serve as input for answering the next question.

The fourth research question (Q4) is another knowledge question. The answer to this question, however, leads to the generation of new theoretical knowledge, and provides direct input to the subsequent design activity. It will be answered by doing an analysis in the form of an observational case study, while using scenarios. A small sample of Dutch public sector organisations will be selected, and experts within those organisations will be interviewed, in order to test the previously proposed hypotheses. The approach for the interviews is further explained in chapter 5.

We use descriptions of Hevner et al. [32] to explain how we use the two methods of observational case study and scenarios. Following the authors' descriptions and translating it to this research, scenarios will be useful to demonstrate the utility of automated IT controls, while the observational case study will be used for an in-depth study of which characteristics will influence the applicability of such controls. In other words, we will use scenarios to initially describe how automated IT controls could be possibly used for external fraud prevention. After that, we 'observe' from the interviews which real-life characteristics influence their applicability, if we wanted to apply the scenarios. This way, the expected influence of characteristics as proposed in the hypotheses, can be tested.

In practice, we do the following. Some cases of external fraud within certain Dutch public sector organisations are investigated, for which specific automated IT controls are suggested that possibly can take over part of the control process. Interviews with experts within those organisations are performed to evaluate the actual possibilities of automated IT controls, and which characteristics influence the

applicability of these controls. The knowledge that is collected from the previous research questions is used as input to the interviews.

From the observational case study, we extract which and in which way public sector characteristics influence the applicability of automated IT controls in the Dutch public sector for external fraud prevention. By conducting the case study this way, we aim to:

1 explain the influencing characteristics for a small sample of Dutch governmental organisations, and
2 reason that there are public sector organisations with similar characteristics in other countries, and that the same characteristics will also apply to these organisations, resulting in a generic answer to the question.

Finally, we come to the design activity, which provides the answer to the main research question (MQ). Using Hevner et al. [32], we do this by designing a method, because methods "provide guidance on how to solve problems". We choose to tailor existing best practices for the development of IT controls, instead of 'reinventing the wheel' by designing a completely new method, because sufficient research and developments from practice have already led to widely accepted standards and frameworks for developing IT controls in general. Therefore, we will present textual descriptions of guidelines that tailor such current standards, which leads to the 'method' that provides guidance on how to solve the problem at hand.

Due to constraints to this research, only a part of a proper design science research process, partly in light with the descriptions of Peffers et al. [60], can be performed. At the stage of answering the main research question, problem identification and objectives of the solution will already be described. The design and development phase is thus limited to tailoring current best practices with textual descriptions. This means that additional research is necessary for further demonstration, evaluation and communication of the guidelines that tailor current standards.

Recommendations can then be provided in which it becomes clear how the gained knowledge and insights from this research can be used. Also, some general recommendations can be given that do not directly pertain to the research goals, but were extracted from the research activities.

1.6 Relevance

In this section, we discuss the practical and theoretical relevance of this research. This concerns the relevance of the results for use in practice and the relevant addition of knowledge to the field of study.

First, this research has practical relevance for the Dutch public sector by examining constructs in public organisations that are sensitive to external fraud, and proposing scenarios in which automated IT controls can improve control processes. This can lead to more insights for increasingly automating control processes, which aims to improve external fraud prevention.

Next to this, there is practical relevance for KPMG. KPMG can advise public organisations about their internal control, of which automated IT controls are becoming increasingly important. With more and more attention for external fraud prevention in the public sector, it is interesting to determine if the

reach of such controls can be expanded to also automatically control on that. This includes an investigation of controlling on legitimacy, and which factors influence the degree to which automated IT controls can be applied to control that. This could lead to an extended role of IT controls in internal control, which can also extend the role of external auditors from an organisation like KPMG. In addition, general recommendations could provide more knowledge about external fraud prevention in general, which KPMG can use in advising public organisations about that.

The guidelines that are designed can be used accordingly to tailor current standards for developing automated IT controls for external fraud prevention in the public sector. This might lead to an appropriate approach for the public sector that can be used when advising about the potential extended role of internal control.

Secondly, regarding scientific relevance, this research summarises current knowledge on how automated IT controls can be developed from a Risk Management approach for external fraud prevention, and what specific public sector characteristics are.

These two subjects are then combined to study the potential effects that specific public sector characteristics can have on the applicability of automated IT controls. Research about these potential effects is non-existent, which means that this research can provide new insights to the research field.

When guidelines are set up, this could also provide implicit evidence that differences between the public and private sectors cannot be overlooked, in case general IT standards that mainly focus on the private sector are directly applied to the public sector. This research could then call for more research that focuses on the potential need for tailoring other IT standards due to specific public sector characteristics.

1.7 Thesis structure

This section describes the structure of this thesis, which concerns the main activities that are performed in order to answer the research questions and how the thesis is structured accordingly.

The theoretical background is presented in Part II, consisting of chapters 2, 3 and 4. In chapter 2, essential concepts are further defined and the scope is determined. The approach of the literature study in chapters 3 and 4 will shortly be discussed by explaining the goal and the strategy that is used to come up with results. Findings will be discussed and conclusions can be drawn in the same chapters, resulting in a theoretical background.

Part III describes the practical part of this thesis, presented in chapters 5 and 6. The observational case study is presented in chapter 5. First, an explanation of the approach is given, which includes descriptions of the chosen governmental agencies and scenarios for improved control processes by automated IT controls. In addition, the method of data collection is explained, which will be interviews with employees of governmental agencies. The results from observations will then be presented and findings can be extracted, leading to the influential characteristics we are looking for.

In chapter 6, results from the previous chapters are used to develop the generic method in the form of guidelines. This means that current knowledge from literature and new insights from the case study are used to determine if current standards for developing automated IT controls should be tailored for external fraud prevention. This chapter starts with explaining the approach that is used to design the guidelines, after which they are described.

Part IV consists of chapters 7, 8 and 9. Chapter 7 consists of recommendations about automated external fraud prevention, based on all the findings from previous chapters. Chapter 8 presents a discussion about the results, the limitations of this research, and the suggestions for further research. In chapter 9, final conclusions are drawn.

Part II

Part II presents the theoretical part of this thesis. The result of this part is a theoretical background that can be used to conduct a solid case study that is grounded on that theory, which eventually should lead to answering the most important research questions of this thesis. Current knowledge from literature and practice is used here. Part II also further explains how the essential concepts can be brought together.

This part first contains an overview and further explanation of essential concepts in this thesis. After that, a summary of knowledge is given on using automated IT controls for external fraud prevention, and how they can be developed. Subsequently, a systematic literature review is performed to extract specific public sector characteristics. We will already evaluate how these might influence the applicability of automated IT controls. At the end, it also becomes clear which hypotheses must be tested during the case study that is described in Part III.

2 Defining and scoping concepts

Before we engage in a theoretical discussion, we first want to separately define and scope the main concepts of this thesis to further explain what we exactly mean by them. Additionally, we discuss how we will use them subsequently.

2.1 Automated IT controls

We already shortly discussed what IT controls are, and will now define the term again by quoting Flowerday & von Solms [28]: "IT controls support governance and business management as well as provide general and technical controls over policies, processes, systems and people that comprise IT infrastructures. These include the processes that provide assurances for information and assist in mitigating the associated risks". We have to further elaborate what IT controls consist of and how we use the term automated IT controls.

IT controls are part of the more general concept of internal control. Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance [25]. The occurrence of external fraud mainly threatens public sector organisations in realising objectives related to operations, and more notably, objectives of compliance. Therefore, internal control can be used to take internal measures for external fraud prevention. The five interrelated components of internal control are depicted in Figure 3, according to INTOSAI [34]. Although there are several standards and frameworks that treat internal control a bit differently, this is a very common view.

The following brief descriptions were extracted from the same source:

- **Control Environment:** Providing the structure and climate for internal control, setting strategy and objectives.
- **Risk Assessment:** Identifying and analysing relevant risks to the achievement of objectives, and developing risk responses.
- **Control Activities:** Mitigating risks through preventive or detective activities, and corrective actions. This includes automated IT controls.
- **Information and Communication:** Effective information and communication is vital to run and control the operations.
- **Monitoring:** Ensure that internal control remains tuned to changing objectives, environment, resources and risks.

Related to internal control is the principle of three-lines-of-defence [58], which we here use to describe the separation of the roles, responsibilities and accountabilities of internal control. This concept is also depicted in Figure 4. The first line of defence comprises the day-to-day operations, where the actual controls must be established and executed. The second line of defence comprises oversight functions that define policies and provide assurance that controls are installed. The third line of defence includes internal and external audit for independent assurance provision. In the end, the CEO of an organisation has overall responsibility for effective internal control.

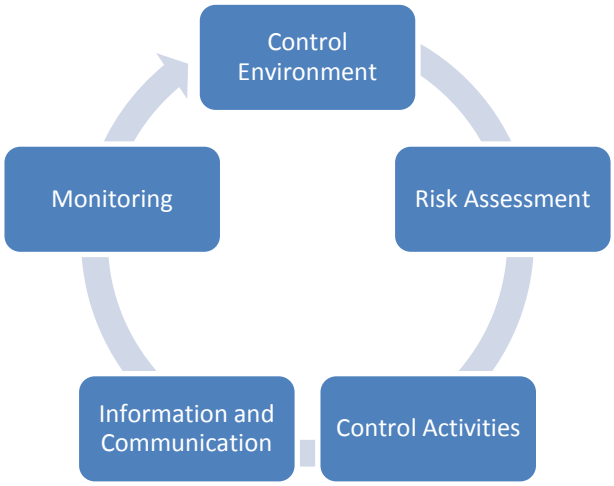

Figure 3. The five interrelated components of internal control, according to INTOSAI [34]

The actual controlling on external fraud occurrences is preferably for a great part situated in the first line of defence, in the day-to-day operations, but having such controls installed does not provide complete assurance. The three-lines-of-defence principle assures not only that appropriate controls are being implemented and executed, but also that these are monitored and evaluated, while tasks and responsibilities are divided among three different levels. IT controls can then be installed and executed in the first line of defence, while being monitored and audited by respectively the second and third line of defence.

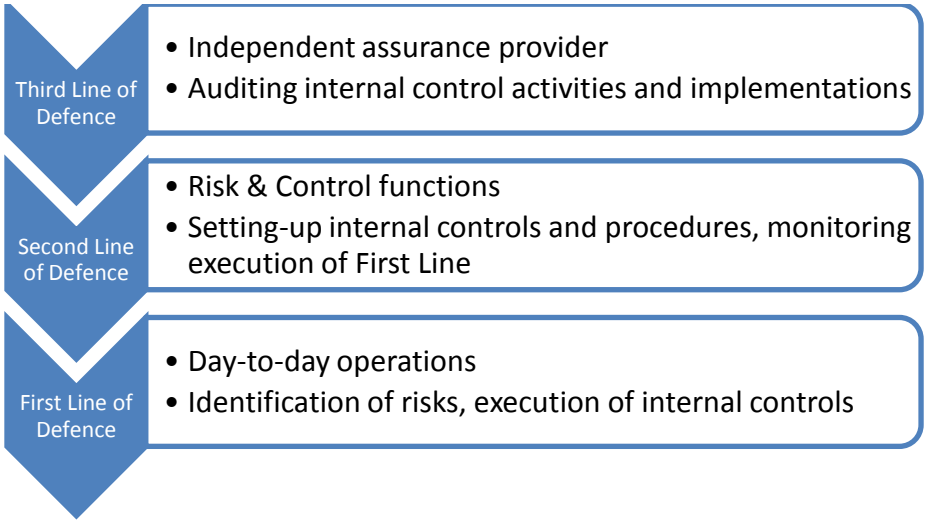

Figure 4. Three-lines-of-defence concept

The term 'IT controls' is mainly used to only describe those internal controls that assure the proper operation of IT systems and the correct processing of data within those IT systems [34]. With appropriate controls in place, certain fraud occurrences can be prevented or detected.

Some examples of IT controls that can assist in that, are the following:

- Validity checks, which ensure only valid data is input or processed;
- Authorisation, which ensures only approved users have access to certain application systems;
- Input controls, which ensure data integrity of input from external sources;
- Forensic controls, which ensure data is scientifically and mathematically correct based on inputs and outputs.

However, public sector organisations deal with preventing external fraud that needs further investigation of data and transactions, especially the input. Most importantly, this concerns legitimacy. Public sector organisations continuously have to control the legitimacy of rights and actions of organisations and individuals in society. To give examples, this pertains to the legitimacy of requests for governmental support (e.g. do you have the right to receive benefits?) and the legitimacy of corporate operations (e.g. are you correctly abiding to tax laws?). Legitimacy is thus concerned with correctly abiding to laws, regulations and other procedures.

This exceeds the original scope of IT controls. Originally, IT controls are concerned with assuring the proper operation of IT systems and the correct processing of data within these IT systems. Here, we also aim to check if correctly processing that data leads to the illegitimate gaining of an advantage by an external party, which is external fraud. This means that you also want to control the external implications of processing data in IT systems, instead of mainly controlling internal implications. Next to the internal objectives of compliance, controlling compliance to laws and regulations by external parties is added. For preventing external fraud in the public sector, this might need controls that link data from different external sources, and use risk profiles for identifying external fraud risks.

Although this is not generally included in the concept of IT controls, we include this to our understanding of IT controls in this research. One reason for this is that we want to use only one term throughout the research, which enhances clarity. A second reason is related to the problem of many current external fraud prevention activities, which are not fast and reactive. Ideally, external fraud prevention is proactive and fast, and IT controls is a concept that entails both. Through automating the control process with IT controls, potential external fraud threats can be immediately mitigated at the moment they might occur, or can be immediately detected when sufficient information is available. Because of these reasons, we make an exception here to include the controlling of the external implications of processing data and transactions to our understanding of IT controls. The following definition, mainly based on Flowerday & von Solms [28], will be used in this research:

> *IT controls support governance and business management, as well as provide general and technical controls over IT infrastructures. These include the processes that provide assurance for information and legitimate consequences, and assist in mitigating associated internal and external risks.*

We must now further define how we interpret automated IT controls. We continue with explaining what we call ‘automated’ IT controls in this research compared to the general term IT controls.

When talking about controls, a distinction can be made between the following controls:

- Manual controls are controls that are performed manually by people [41];
- IT-dependent, or semi-automated controls, combine manual activities with automated procedures and information processing [41];
- Automated controls are completely implemented by machines, such as automatically matching invoices against orders [41]; there are 2 kinds of automated controls:
    - IT general controls "support the functioning of programmed application controls and are the policies and procedures that ensure the continued operation of computer information systems, such as backup, recovery, and business continuity" [28];
    - Application controls "pertain to the individual business processes, application systems or programmed procedures in application software", and ensure complete and accurate information processing [28].

We already discussed earlier that we focus on automated IT controls in this research, and why we do so. Clearly, manual controls are not automated, so those are not incorporated in the scope of this research. We include those IT-dependent controls, where the manual part is heavily dependent on the automated part and thus a significant part of the control process is automated. An example of this can be the automated accessing of data residing on external sources, for which explicit manual approval must be given. So automated IT controls are all automated controls and previously mentioned IT-dependent controls. Other potentially necessary manual actions are not considered in this research, since we aim for fully automating control processes, which minimises the necessity of manual actions.

For this research, we study the applicability of automated IT controls to prevent and detect external fraud. Controls that are able to do this, must be specifically developed to the characteristics of a certain kind of fraud. Application controls are suitable for this. IT general controls are less interesting to consider, because such controls only aim to ensure the continued operation of an information system and to support the application controls. Such controls will be very similar for different systems, in both the public and private sectors. Therefore, we will not intensively look at how IT general controls must be developed during this research.

We now explain the different functionalities of IT controls. IT controls can be preventive, detective and corrective:

- Preventive controls prevent unwanted things from happening [28];
- Detective controls discover problems after they arise [70];
- Corrective controls return the condition back to the expected state [28];

We incorporate all three functionalities, but we expect that the possibilities for corrective controls are worst, due to specific public sector activities. Take for example the controlling of public resources; there might be specific exceptions for legitimately receiving allowances or benefits from public resources, which will always need human judgement. Corrective controls that automatically alter situations with real-life effects, might not be desirable in such cases, and detective controls might then be better.

For simplicity reasons, we will only refer to the term ‘automated IT controls’ to what we discussed in this section.

2.2 Public sector

We also previously mentioned the reasons why we focus on the public sector. External fraud is still occurring on a significant scale in this sector and this causes a lot of damage to society and governments, which includes fraud with public resources. In the Netherlands, fraud with social security benefits alone already added up to an estimate of 153 million Euros [64]. Furthermore, there has not been any research in which it is studied which characteristics influence the applicability of automated IT controls for external fraud prevention in the public sector, and if special guidelines must be designed in the public sector to develop such controls.

Now we have to determine which parts of the public sector will be included in this research. As already mentioned, we perform the case study at public sector organisations in the Netherlands. Although public sector characteristics can differ significantly between countries, we aim to have generic results that can be applied to many countries. An investigation of the possibilities to generalise the influential characteristics to other countries than the Netherlands, is performed during the case study.

Within the Dutch public sector, a first distinction can be made between governmental agencies and semi-governmental agencies, of which the latter is excluded. We will only look at organisations that are fully owned by the Dutch government, or fully operate under the supervision of the government or publicly chosen representatives. A second distinction can then be made between the centralised governments, such as ministries, and decentralised governments, such as municipalities. We will focus on centralised governments, because it is interesting to look at large organisations that deal with many transactions and nation-wide control processes. It is in these organisations that an improvement in the prevention of external fraud can potentially have a great impact and that is why we focus on these centralised organisations. However, we do not exclude decentralised governments, since responsibilities for controlling on external fraud may be transferred to these organisations. Nevertheless, we are not including local-level public sector characteristics, since these can hardly be generalised to the public sector in general, is what we assume. In addition, we assume to get a better generic result when we study such large organisations compared to small organisations that might be very specialised.

Next, we focus on the organisations that have a mandate for supervising compliance to legislation or controlling on incorrect execution of legislation in practice. Special attention is given to main processes in which requests for financial support, such as benefits or allowances, are handled. This way, implementing automated IT controls has great potential, because these organisations actually distribute public resources to those who have the right to receive it by law, but also to those that commit fraud with it. This form of vertical fraud is causing much direct damage, and governments usually have many resources in-house and much authority to control on it. We will also study horizontal fraud cases, to also incorporate findings from this kind of external fraud, which possibly introduces other constraints on the ability to control on external fraud with automated IT controls.

Although we aim to develop a generic result for the public sector in general, we especially take certain centralised governments that heavily deal with external fraud into account, due to the expected higher importance of the result in these organisations. An effect of this can be that the applicability might differ in different kind of public sector organisations, such as small or specialised ones, and organisations dealing with exceptional cases of external fraud. The applicability in smaller organisations with less responsibilities, in which only few transactions occur, must be investigated in further research. It is outside the scope of this research to discuss such small cases or exceptions.

2.3 External fraud in the public sector

External fraud in the public sector can always occur. A former Dutch Secretary of State of the Ministry of Finance recently concluded that the system of allowances within the 'Belastingdienst', the Dutch federal tax agency, can never be made 100% free of fraud [75]. Some individuals will always search for, and will find, weaknesses in systems so that fraud can be committed. Due to differences between all kinds of fraud, and the fact that not all of them can be prevented or detected by IT controls, we have to determine our scope here.

We only include external fraud that can be prevented or detected by using IT resources that are already available to the government or could become available. This is a requirement for IT controls to be useful, since such controls cannot prevent external fraud that needs investigation of other resources than those available in IT systems. This especially excludes certain kinds of horizontal fraud, such as insurance fraud, and these kinds typically do not directly damage the government. With already available IT resources, we also mean data that might not be directly owned by a governmental party, but is regularly obtained on a legal basis. An example of this, is collecting data from a privatised water company about the use of water in a household, to check how much persons might be actually living in that household, for controlling the legitimacy of their allowance or benefit.

We exclude external fraud concerning suppliers and other third parties that deliver supplies or services to the government, such as invoice fraud. The prevention of these kinds of fraud can be performed similarly for both the private and the public sector, and already known solutions from the private sector can be used for this. To be more precise, we only include external fraud that relates to specific governmental activities, or where the government has a specific responsibility of preventing and detecting it.

Furthermore, remaining kinds of external fraud could all be included, but we will give special attention to external fraud with complicated control processes. From these investigations, we expect the impact of IT controls to be most significant, and also expect to discover many different influential characteristics.

2.4 Automated IT controls tackling external fraud

We now discuss how automated IT controls can actually be used in practice for external fraud prevention. We use the scope and definitions from the previous sections to present an example that fits into the context of this research. This can be used to gain a more detailed understanding of how we see

automated IT controls and what their possibilities are, and why they can be preferred above manual controlling in many cases.

We examine external fraud prevention of fraud with benefits for low income households. In several countries, unemployed citizens can request these benefits when their household has a continuous low income, only few assets, and they need the benefits to pay for a modest household. In the Netherlands this is also known as the 'bijstandsuitkering'. We will now highlight an example of how automated IT controls could hypothetically automate parts of a control process in the Netherlands.

2.4.1 Example of possibilities of automated IT controls

For a citizen called John to receive a benefit, he has to send a request to the municipality where he lives. The municipality receives the request and decides if John has the right to receive the benefit. John may receive the benefit if he meets the legal requirements. The basic requirements, together with the way these can be checked, are presented in Table 3.

Table 3. Basic requirements for receiving a 'bijstandsuitkering', and how to check them

Requirement	How to check the requirement (among others)
You must be legitimately living in the Netherlands	Check legal status in DKD[1]
You must be 18 years or older	Check the age in DKD[1]
You (and your partner together) do not have enough income or assets to make a living	Check living status, income numbers, worth of assets in DKD[1]
You do not have the right to receive other benefits	Check in Polisadministratie[2], check personal situation
You are not kept in custody	Check with DJI[3]
Your assets are worth less than the predetermined value applying to your situation	Check worth of assets in DKD[1], check personal situation
You are cooperating in activities that the municipality offers you in order to find a job	Check internal system, check internally with employees

1: DKD stands for 'Digitaal KlantDossier', a databank with personal data, and data about work and income of citizens
2: Polisadministratie is used to check if a person has the right to receive a benefit
3: DJI stands for 'Dienst Justitiële Inrichtingen', which is the organisation responsible for the execution of custodial punishments and other measures

Many of these compulsory checks could be automatically performed directly at the moment when the request of John is transferred to the system of his municipality. Automated IT controls can steer the automated checking of these requirements by requesting the necessary information about John from external sources. When implemented, connections with for example the DKD ('Digitaal KlantDossier', with personal data, and data about work and income of citizens) are set up, or with 'basisregistraties'. These are the main databanks in which the Dutch government centralised essential information about citizens, land registers, etc., to be used for proper execution of governmental activities. An example of a 'basisregistratie' is the BRV, in which information about all vehicles registered in the Netherlands is stored.

In this case, automated IT controls not only check if the input from John's request is valid and complete, but also examine the available information about John to check if he meets the requirements for receiving the benefit. Automated IT controls then assure that no single unlawful request for benefits is assigned in the systems of a municipality. This could also be reached manually by employees, but it would take much more time to control the requests that way, which in some countries might result in the inevitable payment of advances while a part of corresponding requests are unlawful. This usually happens when such requests are controlled very late, after which the citizen has to pay everything back, but has problems doing so because he already spent it. This causes problems for both citizens and municipalities.

The previously described process works preventive, when the request must be judged. In case the benefit is actually assigned to John, and he starts receiving the benefit periodically, detection must be included. The goal of detection is to check if John still meets the requirements, or if changes occur in his situation (e.g. higher income) that might cause him to lose his benefit, which can be external fraud in case he deliberately does not communicate it to the municipality. Automated IT controls can be installed at other organisations to assure that it is automatically communicated when, for example, John's income has become higher. This way, it is assured that changes in the situation of persons are automatically checked, and human intervention might only be needed in case of some drastic changes. Huge time-savings in control processes can be made, and more importantly, external fraud is detected much earlier, which can decrease the amount of outstanding debts.

Of course, it is possible that John does some 'moonlighting', which he does to generate more income without paying taxes. With the extra income, John would not have the right to receive the benefit any longer, so he does not notice governmental parties. With or without automated controlling, this kind of external fraud is hard to tackle, and it will always remain an issue. Automated IT controls cannot solve everything, but they can still help in identifying which benefit receivers are possibly concealing essential information from the government. For example, when a new, expensive car is bought by John from his 'moonlighting' money, this might be automatically detected by automated IT controls when the car is registered on his name in the BRV 'basisregistratie'. After detecting this, manual actions can be taken to control where he got the money from to buy such an expensive car. Although this can also be done completely manually by employees, the control process becomes much more faster, effective and efficient.

2.4.2 Discussion

This example highlights only one instance where automated IT controls could potentially be preferred to manual controlling. However, we also noticed that external fraud cannot always be prevented or detected by such controls, due to the complex nature of certain kinds of external fraud and the limited possibilities for external fraud prevention in the first place.

There are also examples in which automated IT controls can change the control processes, instead of just replacing what was previously done manually. This is especially the case were such controls can steer data analyses and increased coupling of data, and accordingly prevent and detect external fraud based on matching with risk profiles. Increasingly using and analysing data from multiple sources, and

recognising patterns from them that can indicate fraudulent behavior, is an ongoing development in external fraud prevention. Public sector organisations can benefit from this development, but until now, this has mainly be used reactively, instead of proactively. As mentioned before, there is not much research about how automated IT controls can be used for proactively doing this in the public sector, and that is why we further study this.

3 From external fraud to automated IT controls

This chapter presents current knowledge on how automated IT controls can be used for external fraud prevention, based on a Risk Management approach. We first examine how a Risk Management approach can be used for managing the risk of external fraud. Next, we search for current approaches that explain how automated IT controls can be developed using the previously described Risk Management approach.

We qualitatively search for literature in this chapter to come up with a theoretical background on these topics. It is not our goal to give an extensive review of the existing literature here, but to summarise current knowledge that we can also use for answering subsequent research questions. Therefore, we aim to search for existing literature studies on these topics, widely accepted insights from practice, and articles that are highly cited or are published in high impact factor journals.

3.1 Risk Management approach for external fraud

In this section, we shortly explain what Risk Management is and then further elaborate on how the concept can be used for assessing external fraud.

We first want to explain what we define as 'risk' and 'Risk Management'. The literature study by Mensink [53] gives some useful directions for this. According to his review, multiple definitions exist of both concepts. Definitions of risk also vary with respect to the potential effects, whether they are only negative or also positive.

COSO presented the following definition of risk: risk is "the possibility that an event will occur and adversely affect the achievement of objectives" [25]. Two elements of this definition of risk, a possibility and an effect, can also be seen as the likelihood of occurrence (probability) and the potential consequences (impact), which represents a more classical view [23]. The definition implies that both negative and positive effects can arise from such an event, which are also described as, respectively, threats and opportunities. According to Benaroch et al. [11], research nowadays more and more recognises this view that risk can also have positive effects. Although external fraud is mainly considered as a threat in the context of this research, we will not exclude the positive effects from our understanding of risk.

What is then considered as Risk Management? Using Hubbard [33], it can be defined as the identification, assessment, and prioritisation of risks followed by coordinated and economical application of resources to minimise, monitor and control the probability and/or impact of unfortunate events or to maximise the realisation of opportunities. The ISO describes it somewhat shorter as the coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives [36]. In addition, a Risk Management process "describes a set of systematic activities to support the proactive identification and mitigation of risks within a specific environment", according to Barateiro & Borbinha [9].

External fraud can clearly be considered as a risk within the environment of public sector organisations, because the occurrence of fraudulent events affects the achievement of public sector organisations'

objectives, which include fairness [19] and lawfulness [73]. Combining the previously stated definitions, Risk Management can then be applied to systematically identify and monitor the risks of external fraud, and to mitigate them accordingly by applying resources to control the probability and/or impact of potential fraudulent activities. By doing this systematically, public sector organisations can continuously defend themselves and others against individuals or groups that are always trying to find new ways of committing fraud.

As mentioned earlier, we propose that one of the resources to control external fraud is ought to be automated IT controls. How automated IT controls can be developed from a Risk Management approach, and which current approaches exist, is explained in the next section.

3.2 IT controls based on Risk Management

Implementing an internal control system is an element of Risk Management that is intended to counteract inherent risks, according to Flowerday & von Solms [28]. They continue by stressing that IT controls form part of the overall system of internal controls, which indicates that developing internal controls, including automated IT controls, is inherently related to a Risk Management approach. The authors also state that several well-known internal control frameworks or guidelines exist to help organisations in setting up an internal control framework, such as COSO, COBIT, ISO/IEC 17799, and ITIL. These standards can guide organisations in translating risks to controls.

So using such standards can realise the development of controls from a Risk Management approach. Some standards only steer to the development on a high-level, while others may assist in the actual realisation of automated IT controls. Here, we mainly take a high-level view. With the internal control standards we will discuss, IT controls are mostly used for IT audit or general IT governance purposes. These standards, however, do not necessarily involve specific control processes on external fraud in the public sector.

Nevertheless, it is still possible that the need for IT controls for such specific risks arise, as long as these risks are taken in consideration when applying the standards. We make the assumption that these standards do not provide prescriptions for developing specific IT controls for such specific risks, but they may still provide useful approaches or elements that can be used to translate the associated external fraud risks in objectives, needs or activities for control. Therefore, we discuss for several standards what they consist of, how they translate risks to control, and what they can add for the development of IT controls for external fraud prevention.

We will now shortly discuss several of these well-known and mostly-used standards that comprise current approaches, which we will use for further studying. After that, other related concepts and tools concerning internal control with the use of IT are discussed, and conclusions are drawn.

3.2.1 COSO

The COSO *Internal Control – Integrated Framework* [25] describes a direct relationship between objectives, integrated components of internal control, and the organisational structure.

The objectives, which are what an entity strives to achieve, can be divided in three categories: Operations Objectives, Reporting Objectives and Compliance Objectives.

More interestingly here are the five integrated components of internal control:

- *Control Environment*, which is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organisation;
- *Risk Assessment*, which involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives;
- *Control Activities*, which are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out;
- *Information and Communication*; Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives, while Communication is the continual, iterative process of providing, sharing, and obtaining necessary information;
- *Monitoring Activities* comprise the ongoing or separate evaluations to ascertain whether each component of internal control, including controls to effect the principles within each component, is present and functioning.

The relationship between the objectives and components is shown in Figure 5. In addition, seventeen principles represent the fundamental concepts associated with each component, from which the following are interesting in the context of this research. By doing a risk assessment, organisations must consider the potential for fraud in assessing risks to the achievement of objectives. After that, control activities are performed, in which organisations select and develop the controls that contribute to the mitigation of those risks to acceptable levels.

Figure 5. Relationships of Objectives and Components from the COSO Internal Control – Integrated Framework [25]

This means that controls are developed according to the risk assessment. The COSO framework, however, does not go in further detail about how these controls must be actually developed. In this respect, the COSO framework should be considered as an overall evaluation framework for internal control [62]. We therefore stress that using COSO alone is not suitable to develop IT controls in detail, but it is a good starting point for identifying risks of external fraud and translating it to appropriate control activities. A first judgement can then be given about the possibility of using automated IT controls for those control activities.

This is also what the INTOSAI framework does, which tailors the COSO framework [34]. It gives special attention to certain public sector elements, without really stating how IT controls must accordingly be developed in detail. This framework can also be studied to see if guidelines are necessary to further tailor this framework.

3.2.2 COBIT

COBIT (Control Objectives for Information and related Technology) is all about IT governance. It "helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use" [35]. Furthermore, it sets out a set of controls over IT and organises them around a logical framework of IT-related processes, according to De Haes et al. [26]. The authors also describe that COBIT is built around five core principles:

- *Meeting stakeholder needs,* which implies that COBIT provides all of the required processes and other enablers to support business value creation and risk management through use of IT.
- *Covering the enterprise end-to-end,* which states that COBIT covers all functions and processes within organisations, and does not solely focus on the 'IT function'.
- *Applying a single, integrated framework*, which states that COBIT aligns at a high level with other relevant standards and frameworks, so that it can serve as an overarching framework for governance and management of organisational IT.
- *Enabling a holistic approach,* which explains that efficient and effective implementation of governance and management of organisational IT requires a holistic approach.
- *Separating governance from management.* Here, governance is ensuring the achievement of organisational objectives by evaluating stakeholder needs, setting direction, and monitoring performance, compliance and progress against plans. Based on these governance activities, management is planning, building, running, and monitoring activities (a translation of the Plan, Do, Check, Act cycle) in alignment with the direction set by the governance body.

The generic COBIT principles and 'enablers', which are the factors that influence whether the governance and management over enterprise IT will work [26] and are shown in Figure 6, are useful for public sector organisations [35]. The framework has become the main standard and is globally accepted in the public sector for IT governance and IT audit [4]. However, we are not studying standard IT governance and IT audit here. We therefore still question the use of COBIT for developing controls in specific public sector control processes such as controlling external fraud, and we stress that its usefulness is uncertain for these purposes.

COBIT thus provides a comprehensive framework for the alignment of IT and business objectives and is very large in scope. According to Al Omari et al. [4], it is not uncommon that public sector organisations 'cherry pick' controls from the framework when implementing the entire framework is too large a task. The authors therefore created an optimised sub-set of COBIT control objectives for public sector organisations in Queensland (Australia), which consists of the most important control objectives perceived by organisations in that sector. Such a sub-set could also be made to give special attention for external fraud prevention, but it is outside the scope of this research to further elaborate on that.

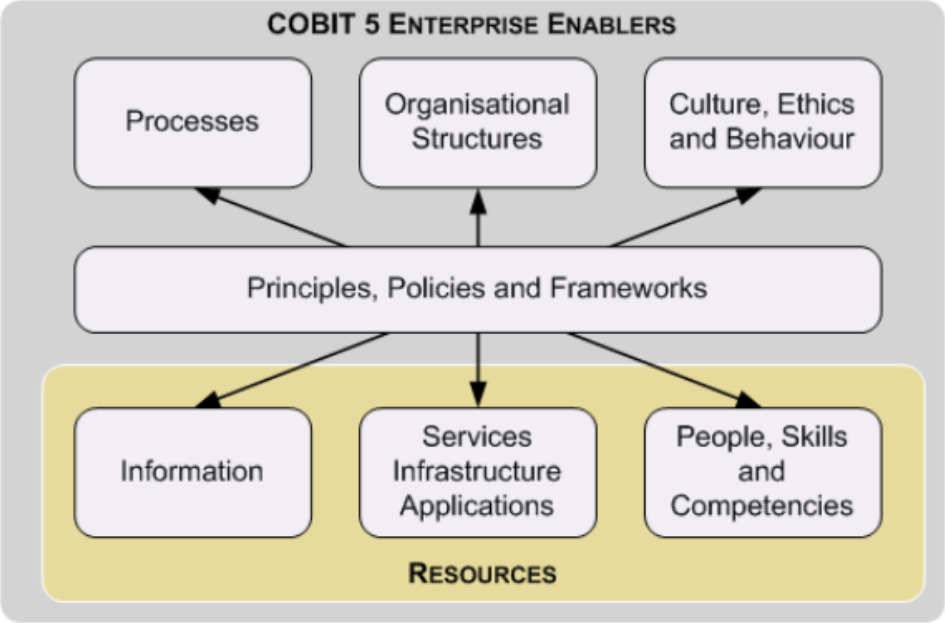

Figure 6. COBIT 5 Enablers from the COBIT 5 Framework [35]

Question remains how IT controls are developed accordingly. COBIT describes over 300 detailed controls covering a range of IT management and governance [4]. Based on the control objectives, appropriate controls can be chosen from the wide range of controls that are defined in the framework. The development of IT controls from COBIT seems to be dependent on this 'checklist' of controls. COBIT thus provides more guidance to actual controls than COSO, and it describes more specifically how such controls should be implemented, which can also include IT controls.

3.2.3 ITIL

ITIL (IT Infrastructure Library) is a framework that describes best practices for the governance of IT, and the management and control of IT services [72]. IT services are concerned with facilitating business needs with IT. In addition, ITIL principles focus on the continual measurement and improvement of the quality of IT services delivered, from both a business and a customer perspective.

ITIL consists of five publications that describe the stages of the service life cycle [72]:

- *Service Strategy*, concerned with understanding organisational objectives and customer needs;
- *Service Design,* in which the service strategy is turned into a plan for delivering business objectives;
- *Service Transition,* concerned with developing and improving capabilities for introducing new services, based on the service strategy and service design;
- *Service Operation,* in which agreed levels of service must be delivered, and to manage the resources that support delivery of these services;
- *Continual Service Improvement,* concerned with the continual evaluation and improvement of the quality of services.

ITIL's main target is to describe how IT services must be deployed and how they are properly managed and improved. When controlling on external fraud by IT can be seen as an IT service, developing IT controls for that purpose can be included. IT controls are then developed from an IT service perspective, in which a service design should describe how IT controls realise the objectives of the control process on external fraud, and thus how these controls must be developed. This way, a design of the 'service' that IT controls must provide can be given and this is another way to develop IT controls.

3.2.4 Related concepts and tools

In addition to these standards, other concepts exist which involve optimising control. Next to this, we discuss certain well-known tools that exist for the realisation of IT controls.

Continuous Auditing & Continuous Monitoring, CA/CM in short, is a concept that deserves attention. It consists of two separate, but related concepts, with respect to auditing (CA) and monitoring (CM). We use the definitions of KPMG [44] here. CA is "the collection of audit evidence and indicators by either the external auditor or the internal auditor in IT systems, processes, transactions and controls on a frequent or continuous basis throughout a period". CM is "a feedback mechanism used by management to ensure that controls operate as designed and that transactions are processed as described", which can form "an important component of the internal control structure".

In the context of this research, especially the CM part is interesting. Implementing automated monitoring controls that continuously control on potential fraud cases is an active form of detection that can lead to faster discovery of external fraud compared to many current practices. Especially large public organisations that deal with many transactions and extensive control processes can benefit from this. Automated IT controls can be implemented to systematically steer such monitoring, and ensure proactive external fraud prevention.

CA/CM can in turn be part of the wider concept of GRC, which stands for Governance, Risk & Compliance. Racz et al. [65] define it as "an integrated, holistic approach to corporate governance, risk and compliance ensuring that an organisation acts in accordance with its self-imposed rules, its risk appetite and external regulations through the alignment of strategy, processes, technology and people, thereby leveraging synergies and driving performance". The essential idea is to integrate the organisational-wide efforts for managing risks, monitoring and evaluating control, and compliance to rules.

GRC provides a very broad approach for setting-up control needs based on organisational-wide risks and compliance requirements. Automated IT controls could be developed according to those control needs. Awareness of this topic has led to an increasing number of GRC implementations that can assist in this process, predominantly with the use of well-known tools, such as BWise GRC or SAP GRC.

The concepts and tools described here provide popular views that currently gain very much attention in practice for improving internal control. However, public sector organisations are more reluctant to follow these developments than their private counterparts, as was the case with GRC adoption investigated in US federal agencies [30]. Less attention for research on the applicability and usefulness of these concepts and tools in the public sector can be a reason for this. Due to constraints to this research, we do not go in further detail. However, we want to stress that these concepts deserve more attention of the research field for usage in the public sector.

3.3 Summary and discussion

We identified how controlling external fraud can be done based on a Risk Management approach. In short, risks of external fraud are identified and assessed, after which control activities are set up to mitigate the risks. Based on these control activities, appropriate automated IT controls can be developed.

Well-known frameworks from practice are helpful for this. COSO is a framework that is best for a more high-level evaluation of internal control, focussing on governance. COBIT and ITIL can be used to dig deeper into the need for developing certain controls in IT operations, where ITIL has special attention for IT service management. It might be assumed that more attention for automated IT controls can be given through COBIT and ITIL, but this is not explicitly done. For a more clear comparison of what these frameworks offer, we refer to Figure 7.

The previously discussed frameworks and related concepts traditionally focus on use in the private sector, on which most research also focuses. There is only little scientific evidence about applying such frameworks and concepts to the public sector. It is uncertain if such frameworks can be simply transferred to the public sector, and therefore, it is also uncertain if developing IT controls can be done the same way as for the private sector.

To conclude, we studied current approaches for developing IT controls for two reasons. First, it provides insights into the possibilities of automated IT controls, which can be used for the scenarios in the case study, to discuss the potential usage of IT controls to automate and improve current control processes. Secondly, the current standards describe how IT controls can be developed. This is used to assess if guidelines have to be designed in case current standards have to be tailored to take into account the possible influences of specific public sector characteristics. However, it is also possible that the standards do not have to be tailored at all.

To find out, we will search for possible influential public sector characteristics in the next chapter. After these are known, it can be determined in practice if they affect how automated IT controls, which were discussed here, can be applied for external fraud prevention.

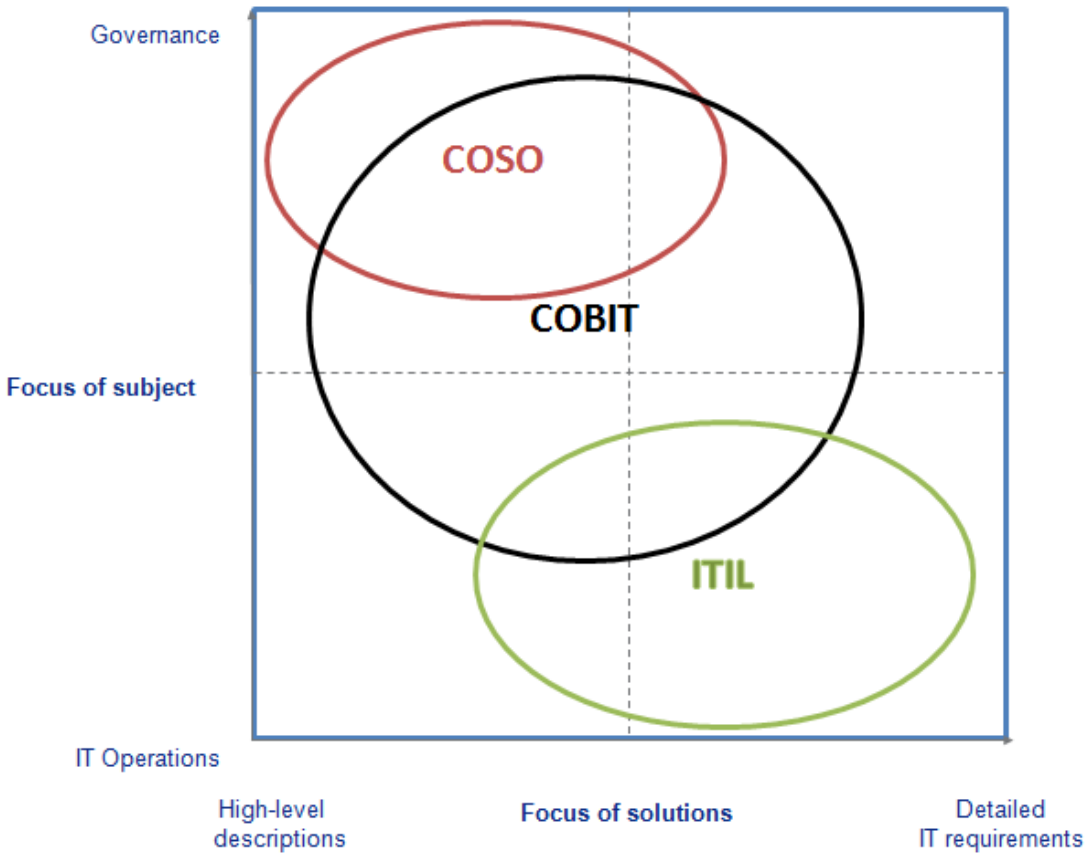

Figure 7. Simplified representation of the fields of focus of COSO, COBIT and ITIL (partly based on [26] and [37])

4 Influential public sector characteristics

This chapter presents a literature review to create a theoretical background on specific public sector characteristics. We use the approach of Wolfswinkel et al. [77] for systematically reviewing literature to do this, which will be further discussed in the next sections.

Subsequently, we will use logic reasoning to determine which of the extracted characteristics could possibly influence the applicability of automated IT controls for external fraud prevention in the public sector. In addition, we propose hypotheses that also describe in which way the characteristics could influence that applicability. These hypotheses can then be tested during the case study.

In other words, the public sector characteristics that we will find from literature (theory), will be incorporated in the case study to determine in practice if they influence the way automated IT controls can be applied. In this chapter, we take the high-level theory of public sector characteristics and the low-level knowledge about IT controls together, and aim to bring them together on a level in between. We do this by first examining the literature, and discuss the potential influence they have on automated IT controls after that.

4.1 Literature review approach

First, we describe how we searched. Criteria for the inclusion or exclusion of articles were set, an appropriate field of research was identified to search in, academic sources were chosen and search terms were formulated. Then, the actual search was performed, after which we selected articles based on the previously defined criteria. We only performed two full iterations of the selection stage, meaning that checking backward citations was performed just twice. We did this because we did not select very strict criteria, due to the wide range of different characteristics that was ought to be found. Therefore, we expected to already have a complete view of public sector characteristics after two iterations.

Next, the texts that were chosen were analysed using open coding, axial coding and selective coding. During these steps, different categories of public sector characteristics were identified and relations between the main categories had to be found, in order to develop a single reasoning about the topic. By representing and structuring the gained knowledge from the previous step, findings and insights about the topic became clear.

4.2 Public management literature

After the second full iteration was completed, and newly found references were refined, we eventually came up with 38 references. The next task is to extract and categorise the relevant public sector characteristics from the 38 references and discover relations between them, which is done by analysing. But first, a short discussion on the literature related to our subject is given.

Characteristics that are specific for the public sector can mainly be found when it is compared to the private sector. Literature reviews on the differences between public and private organisations have been performed several times in history, including those by Rainey et al. [67], Perry & Rainey [61], and Boyne [13]. From these literature reviews, it becomes clear that there is a substantial debate about this topic. Emerging concepts, such as New Public Management (NPM), triggered debates on unresolved

issues during the past few decades [52], both in research and practice. The view of the distinctive characteristics of the public sector has both numerous proponents and critics.

Numerous scholars have proposed differences between the two sectors ever since. Among these scholars and their publications are, in chronological order, Rainey et al. [67], Bozeman & Bretschneider [15], Kickert [42], and Cong & Pandya [24], spanning several decades of research. The proponents argue that it is doubtful whether private sector management can easily be transposed to the public sector, due to fundamental differences between the two sectors [42]. Many of them also quote that private and public management are only "fundamentally alike in all unimportant aspects" [3].

Critiques on these identifications point at the mainly theoretical foundations of those findings, whereas empirical evidence would be much stronger. Compared to theoretical contributions, the amount of empirical evidence on this topic is relatively low. When Boyne [13] discussed public and private management, he concluded that the existing empirical evidence does not provide clear support for the view that they are fundamentally dissimilar, nor can it be concluded that there are no differences at all. According to the author, there may still be differences that have not been identified in the literature yet, but "there are few solid empirical grounds for rejecting the application of successful private practices to public organizations" [13].

This immediately raises the question if there actually should be different developmental guidelines in the public sector for IT controls for external fraud prevention. Why would successful private practices for developing IT controls not be applicable to the public sector? Evidence of significant differences on particular elements of both sectors, such as in human resource management policies and practices [14], and the lack of knowledge on successful management strategies in the private sector that can be drawn upon the public sector [13], still suggests that public sector characteristics cannot yet be overlooked.

To summarise, successful private practices might be applicable, but it is just as likely that they have to be tailored for use in the public sector, caused by specific public sector characteristics. Therefore, we still study those characteristics, which could possibly be influential on the applicability of automated IT controls for external fraud prevention. But we also bear in my mind that it is possible that no evidence will be found for the need for specific guidelines for the public sector.

The previously mentioned debate on this topic resulted in a significant amount of research that covers the study of many different public sector characteristics. We extracted these characteristics from the literature and analysed them, following the analysing phase described by Wolfswinkel et al. [77]. This analysing phase resulted in the recognition of high-level categories in which the characteristics could be divided, which resulted in eight main categories. These main categories are presented in Table 4. A complete overview of the mapping of references and corresponding categories that were found from this process, is presented in Appendix A. Although some scholars argue the lack of evidence for some of these characteristics, we still included them for reasons of completeness.

Table 4. Main categories of public sector characteristics

Environment	Goals & Values
Political control & Bureaucracy	Resources & Capabilities
Performance & Evaluation	HRM & Personnel
Organisation & Structure	Uniqueness of Tasks & Position

4.3 Detailed results

We now discuss in more detail what each category entails and which characteristics of the public sector are apparent. Simultaneously, we check for each characteristic how plausible it is that the characteristic might influence the applicability of IT controls for external fraud prevention. Characteristics with a very low plausibility are then excluded from further studying.

The remaining public sector characteristics are then used to propose hypotheses that can be tested during the case study. Building hypotheses helps us to question which potential relations we want to examine. We limit ourselves to presenting hypotheses about the categories of the identified public sector characteristics, instead of discussing an extensive list of detailed hypotheses that treats each of the identified characteristics separately. Of course, these characteristics will be incorporated in the case study, but we expect that results are better understandable and can better be generalised when the hypotheses concern the more high-level categories.

4.3.1 Environment

This category describes characteristics that pertain to the specific environment (or network) public sector organisations are situated in, including the actors in its surrounding, the relations with and between them, and the corresponding effects. This category was widely discussed, and the characteristics that are drawn below were convincingly supported by numerous references.

The environment of public sector organisations is characteristic mainly due to the ownership and the corresponding interests of these organisations. They are collectively owned and controlled by members of political communities [13], and they serve the public interest [67], especially were market failure occurs [15]. This leads to an environment with a great variety of stakeholders, each placing demands and constraints on public managers that are likely to be conflicting [13]. In addition, public organisations are easily influenced by external events [13]. Furthermore, public organisations face less competitive pressures [13], partly because they have many dominant and monopolistic positions with services they provide. Therefore, a non-economic rationality is apparent in the environment [19].

Public sector organisations have to deal with greater accountability and public scrutiny, and a bigger role of press and media to the substance and timing of their decisions [3]. They are not accountable to shareholders, as in the private sector, but to a wide variety of stakeholders in their environment.

To conclude, the characteristics that were found in this category from the literature, are:

- G1 Great variety of stakeholders, placing demands and constraints that are likely to be conflicting;
- G2 Little competitive pressures, and non-economic rationality;
- G3 'Open systems' that are easily influenced by external events;
- G4 High public scrutiny and accountability to multiple stakeholders.

Now we determine which ones are plausible to influence the applicability of automated IT controls. We argue that the absence of competitive pressures, and the presence of a non-economic rationality, will not influence the applicability of IT controls. The same yields for the fact that public sector organisations are easily influenced by external events, and face high public scrutiny and accountability. These three environmental characteristics (G2, G3, G4) will not influence the applicability, because they do not pose constraints on IT controls in particular, or how they can be used and reach their targets.

This leaves us with only one characteristic (G1), which we argue is significant and is expected to have a negative influence. External fraud prevention can involve many different stakeholders and high interests with respect to corresponding control processes, and public organisations might therefore prefer to address these demands very carefully. Especially when constraining demands are strong, this can cause that doing the controlling systematically and automatically might not be preferable. In this way, environmental influences can cause pressures that need custom control processes with special, manual attention. Therefore, the following hypothesis is presented:

H1: Environmental factors negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.

4.3.2 Goals & Values

As discussed in the previous section, public sector organisations mainly serve a specific interest: the public interest. This leads to specific goals and values that are characteristic to the public sector. This category was also heavily supported, and the characteristics presented below have support from multiple references.

Serving the public interest leads to public sector goals that are more externally set and transcend single-organisational interests [15]. Public sector organisations thus have a wider scope of concern [3]. Next to this, they face multiple goals, many of which are complex [2], intangible or in conflict with one another [21]. This often involves ethical values that cannot be easily measured [22], such as defence readiness and public safety [66], or other public values, such as transparency and correctness [51].

Research in which evidence was found for higher goal clarity in the public sector shows quite the contrary of what scholars earlier proposed about the vagueness and measurability of goals [47]. We propose that goal clarity and intangibility are not completely in conflict, and for reasons of completeness, we include them both to our characteristics. Since there is considerable conflict about measurability, we exclude it from further studying.

To conclude, the characteristics that were found in this category from the literature, are:

G5 Many externally set goals that transcend single-organisational interests, leading to a wide scope of concern;
G6 Multiple goals, many of which can be:
- Complex,
- Intangible,
- Conflicting;
G7 Numerous ethical and public values.

We argue that all three of these characteristics are plausible to influence the applicability of automated IT controls, and it is expected that this influence will be negative. A problem for public organisations is namely that goals and values pertaining to controlling external fraud can be intangible [61], or ethical. This causes that no 'hard' measurements exist, which makes automatically controlling such cases very hard. Furthermore, a typical public sector opinion is that increased controlling on individuals is itself not ethical, since privacy of citizens would then be in danger. This opinion stresses that governments must not be able to install 'Big Brother' control systems, and this can make that the increasing use of automated controlling, including automated IT controls, is brought to a halt.

The following hypothesis is presented accordingly:

H2: Goals & Values negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.

4.3.3 Political control & Bureaucracy

What we shortly mentioned previously, is that public sector organisations are collectively owned and controlled by political communities [13]. This indicates that these organisations are subjected to political authority, which is implemented by means of legal and constitutional structures [15]. That these structures and their effects are also specific public sector characteristics, will now be elaborated.

Organisations that are facing political control are likely to face multiple sources of authority that are potentially conflicting [13]. Furthermore, political control and legislations lead to many legal and political constraints [22]. An element of political control is the way how politics works. For example, re-elections are typical for politics, which might result in instability when programs and policies are changed regularly [13]. Due to re-elections, public managers have shorter time horizons [3], in which there is more focus on quick results, which in turn are possibly catalysed by a so-called 'crisis agenda' [15].

When there are frequent leadership and program changes, this can cause discontinuities in basic data element definitions in IT, and also disrupt the long-range planning that is necessary for information resource management [21]. Moreover, a change in stakeholders of an IS project can have an effect on IS success , for example when a government with an opposing view on policies is elected during project stages [27].

Next to this, bureaucracy (or formalisation) is a legal constraint. Robertson & Seneviratne [69] reviewed from literature that formalised, 'bureaucratic' elements of organisations are identified as "the likely barriers to successful public sector organizational development".

To conclude, the characteristics that were found in this category from the literature, are:

G8 Political authority, potentially from multiple conflicting sources, implemented by means of legal and constitutional structures;
G9 Many political and legal constraints, including bureaucracy;
G10 Instability, resulting in:
- Short-range planning and focus on quick results,
- Discontinuities and disruptions in IT, and a bad effect on IS success.

Multiple references support the characteristics presented here, except for the following part: discontinuities and disruptions in IT, and a bad effect on IS success. The two parts of that sentence are each supported by only one reference, but were considered to be important in the context of this research, which is the reason why we included it.

Now we determine which ones are plausible to influence the applicability of automated IT controls. We argue that it is not the political authority of public sector organisations itself that poses constraints on the applicability of IT controls, but that the political and legal constraints stemming from legislations and policies can. Therefore, G8 is excluded. While including the other two, we expect the influence to be negative for the following reasons.

Where a control process is dependent on complex procedures and legislation, including many exceptions and special cases, it becomes complex itself. Control processes might even become too complex for automated IT controls to appropriately control in the first place. Also, political instability and continually changing legislations, which can be caused by changing political landscapes after elections, can cause that it becomes inefficient when automated IT controls in complex control processes must be adjusted every now and then. This effect of politics can additionally cause discontinuities and disruptions in IT [21], which might also have a negative effect on the applicability of automated IT controls.

H3: Political controls & Bureaucracy negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.

4.3.4 Resources & Capabilities

The resources and capabilities available to public sector organisations can be different from those available to private sector organisations. Compared to other categories, however, this category has the least support of references. The characteristics that are presented below are each supported by only one, two or three references, but these were considered to be important in the context of this research.

Alford [2] discussed that public sector managers use more diverse resources and utilise a wider array of productive capabilities than private sector managers. Not only is public money (largely funded by

taxation [13]) a specific public sector resource, so is public power. Capabilities are organisational capabilities, such as labour and materials, to be deployed for optimising public 'production'.

However, public managers have less control over the inputs and mix of organisational resources than do private managers [19]. This can be explained by the fragmented authority of public managers over the resources they require [2]. Next to this, data sharing beyond the organisation has become important in the public sector, for example by matching records from different public agencies [15]. This could lead to information richness, but since information requirements are inherently more difficult and unstable in the public sector due to specific goals and values [21], it can be hard to actually reach those goals with the information at hand. Furthermore, public sector agencies do not have the financial flexibility for quick changes in IS projects, mainly due to predetermined budgets [27].

To conclude, the characteristics that were found in this category from the literature, are:

- G11 Wide array of resources and capabilities to utilise;
- G12 Less control over the inputs and mix of organisational resources than in the private sector;
- G13 High data sharing beyond organisational boundaries;
- G14 Difficult and unstable information requirements;
- G15 Little financial flexibility for quick changes in IS projects.

We argue that all of these characteristics are plausible to influence the applicability of automated IT controls. However, the way they influence that applicability might differ, since some could pose constraints, while others could create opportunities. It is hard to say if the characteristics of this category will eventually influence the applicability significantly positive or negative. Therefore, the following hypothesis is proposed:

H4: Resources & Capabilities neutrally influence the applicability of automated IT controls for external fraud prevention in the public sector.

4.3.5 Performance & Evaluation

We now discuss overall performance in the public sector and the evaluation techniques that are applied. This was significantly discussed in the literature we found, with multiple references that support each subsequently discussed characteristic.

It has often been argued that public sector organisations perform less productive and efficient [43], and different causes are mentioned. Possible causes include cautiousness and the rate of turnover of top leaders [3], common ownership [13], a missing strong link between work input and reward [15], and little market exposure [21]. Another widely-accepted cause is 'red tape', which has to do with many procedural delays that can exist in the public sector [18].

Next to that, performance targets are inherently unclear [13], which might be yet another cause. Partly as an effect of that, less performance measuring is done in the public sector [3]. The fact that policy success is a measure of accomplishment in the public organisations [19], speaks for itself. In addition, quality can be difficult to define or measure in the public sector [19], which adds to the complex task of

performance evaluation [78]. Moreover, an important evaluation technique in the private sector is fiscal control, whereas public 'social good' questions can cause that such a business-like evaluation technique cannot be easily transferred to the public sector.

To conclude, the characteristics that were found in this category from the literature, are:

G16 Low productivity and efficiency;
G17 Performance targets are inherently unclear;
G18 Performance measuring is done less in the public sector;
G19 Performance evaluation is complex due to indefinable or immeasurable targets.

Now we determine which ones are plausible to influence the applicability of automated IT controls. We argue that two Performance & Evaluation characteristics have very low plausibility in influencing the applicability of IT controls. Low productivity and efficiency do not influence the way IT controls work, and neither does the fact that performance measuring is done less in the public sector. We therefore exclude G16 and G18. We assume that performance targets may influence the applicability, since the benefits of IT controls may be unclear when such targets are unclear or complex. However, it is not expected to be of significant influence. Therefore the following hypothesis is presented:

H5: Performance & Evaluation negatively influences the applicability of automated IT controls for external fraud prevention in the public sector, but this is expected to be not significant.

4.3.6 HRM & Personnel

HRM (Human Resource Management) principles are found to be different in public sector organisations compared to private organisations. Personnel is about specific characteristics that deal with employee mind-sets and attitudes towards their work. Multiple references that support the characteristics of this category provide empirical evidence, which shows considerable support for these characteristics.

A traditional style of HRM (paternal, standardized and collectivized) is more apparent in the public sector, partly because public sector organisations usually are model employers. This includes giving extensive trainings, promotion of equal opportunities, and concern for the welfare of employees [14].

Compared to the private sector, public sector personnel have different perceptions regarding their work. Several scholars acknowledge that public sector personnel feel less committed to their organisation [13], feel less presence of policies for rewarding based on (individual) performance [14], feel less incentives for efficient work, and feel less authority and hierarchy [3]. Empirical evidence was found for differences between the two sectors in job satisfaction and commitment, motivation, perceptions of rewards, structure, decision patterns, and performance [16]. To summarise, it is stated that public sector personnel are less satisfied, feel less motivated and rewarded, have less decision-making autonomy, and perform less.

Furthermore, public sector (top) managers have a more political role, feel less authority over subordinates, and have greater reluctance to delegate [21]. A public service ethos is also recognised

among public sector managers, which includes less materialistic behaviour and a stronger desire to serve the public.

To conclude, the characteristics that were found in this category from the literature, are:

- G20 Traditional style of HRM and model employer;
- G21 Public sector personnel are less satisfied, motivated, and rewarded, have less decision-making autonomy, and perform less compared to the private sector;
- G22 Public sector (top) managers have a public service ethos, have a political role, have less authority over subordinates, and are more reluctant to delegate.

Now we determine which ones are plausible to influence the applicability of automated IT controls. We exclude all HRM & Personnel characteristics (G20, G21, G22), since the way HRM is designed and how public personnel is perceiving their work, does not influence the aspects of automated IT controls. We assume that automated IT controls are applicable with every kind of HRM style and personnel constraints, since there is no (or almost not any) human intervention when IT controls are to be executed automatically. Only if there would be significant resistance against IT controls among personnel, this could be influential, but that was not identified as a specific public sector characteristic. No hypothesis about this category is proposed that will be tested in the case study.

4.3.7 Organisation & Structure

Differences in organisational and structural factors are apparent between the public and private sectors [42]. The three characteristics discussed below do not have that much specific support, but multiple references provide findings that complement each other, which is the reason why these characteristics are still considered to be significant.

First, there is a greater organisational interdependence in the public sector [18], with a system of complex hierarchies incorporated [19]. Secondly, public sector organisations tend to have a more compartmentalised, or ‘silo’, structure [24].

Organisational structures only change little in the public sector, due to the required organisational stability, according to Yan [78]. Morales [55] found that structural change in public sector organisations occurs despite high external regulatory pressures and perhaps because of them. The author points out the strong impact of regulatory dependency of the public sector as covariate of change. When we take the findings of these two authors together, we can say that there is little change of organisational structures in public sector organisations, but when there is, it is presumably due to the regulatory dependency of such organisations.

To conclude, the characteristics that were found in this category from the literature, are:

- G23 Significant organisational interdependence;
- G24 Compartmentalised, or ‘silo’, organisational structure;
- G25 Little changes in organisational structures, which are mostly steered by regulatory changes.

We argue that all three of these characteristics are plausible to influence the applicability of automated IT controls, and that they pose more constraints than opportunities. The interdependence of public sector organisations [18] can lead to limitations for such controls, in case the responsibilities of control processes are divided among such interdependent organisations, or if an organisation has to rely on specific input or activities from other organisations. It is not always possible to fully apply automated IT controls in that case.

Also, compartmentalised structures of public sector organisations can lead to failure of identifying organisational-wide risks of certain kinds of external fraud. Developing automated IT controls within compartmentalised structures based on such compartmentalised risks, can lead to less efficient and less effective external fraud prevention by such controls compared to taking an organisational-wide view. Although we stated at the beginning of this thesis that the Dutch government is already becoming aware of taking an organisational-wide view, we incorporate it for reasons of completeness, also because this might still be the case in other countries.

Therefore, the following hypothesis is presented accordingly:

H6: Organisation & Structure negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.

4.3.8 Uniqueness of Tasks & Position

Many public sector organisations perform unique tasks or hold unique positions that private sector organisations never will or can. Although not that many references support this category, all three characteristics that are identified have multiple references that support it and they are therefore considered to be significant.

Compared to the private sector, public sector organisations face more multidimensional tasks [40] and different types of problems [19]. Furthermore, governments use unique sanctions and coercive powers which are unavoidable or mandatory for the execution of specific government activities [3]. This way, governments act as monopolies that can ensure the participation and compliance from the public through coercion [22]. Next to this, as mentioned earlier, public sector organisations are collectively owned and have a specific legal status, and legitimacy [16].

To conclude, the characteristics that were found in this category from the literature, are:

- G26 More multidimensional tasks and different problems compared to the private sector;
- G27 Usage of unique sanctions and coercive powers for the execution of specific activities;
- G28 Collective ownership and specific legal status.

Now we determine which ones are plausible to influence the applicability of automated IT controls. We argue that the ownership and status of public sector organisations itself has no effect on the applicability of IT controls, but that coercive powers that might stem from that can. This leads to the exclusion of G28. The remaining two characteristics could have both positive or negative influence on the applicability.

We expect here that public sector organisations not only have unique tasks and positions that create opportunities, but also unique external fraud problems, some of which cannot be executed automatically and pose constraints. An example of the latter is when detection based on risk profiles is not effective, due to a unique and complex composition of indicators that is necessary to identify an external fraud case.

The last hypothesis then becomes:

H7: Uniqueness of Tasks & Position neutrally influences the applicability of automated IT controls for external fraud prevention in the public sector.

4.4 Limitations and conclusions

Since we excluded 10 public sector characteristics with low plausibility for influencing the applicability of automated IT controls, this leaves us with 18 characteristics. These are divided among seven categories, which in turn led to seven hypotheses that will be tested during the case study. The seven categories with corresponding characteristics, which will be incorporated in the case study, are shown in Table 5. The seven hypotheses are shown in Table 6.

Some limitations of our literature review must be addressed. First of all, we did not have the resources to gain access to all the references we wanted to look at. Therefore, a number of references was not added to this review, which could possibly lead to some public sector characteristics not being included in this research.

Secondly, the quality and impact scores of the references could possibly be higher. We did not specifically search for references that are published in high impact journals, which would imply higher quality. The selected references are averagely cited by around 177 other references according to Google Scholar, with scores fluctuating between 0 and 705. This average is not really low for this quality indicator, but not that high either. Most references (32) were found in journals that exclusively focus on public administration or (public) management. Also, there are many older references in relation to more recent ones, which indicates a higher chance of outdated information.

Thirdly, most references pertain research applied to a limited number of countries, which mostly concerns traditional developed countries, such as the US and the UK. This might indicate that public sector characteristics from differing countries are not included. We assume here that IT controls for the purpose of external fraud prevention will probably not be that much applied in less developed countries, so the inclusion of research that mainly focuses on developed countries is quite logical at this point in time. Still, a sample of more diverse countries could be possible. Furthermore, we stress that we focused on taking general public sector characteristics into account, that might also apply to such less developed countries.

Fourthly, no evidence from the literature was used when discarding ten of the found characteristics in the discussion of the results in the previous section. Logical reasoning was used, but this indicates that the eventual list of public sector characteristics might be affected by some subjectivity, instead of the preferred objectivity based on scientific evidence. Also, a category might be more representative if it

accounted for a large number of characteristics. However, we still argue that the list is correct and that the choices were appropriate.

To conclude, we found the main public sector characteristics that might influence the applicability of automated IT controls for external fraud prevention in the public sector. These characteristics are divided among categories, for which we posed hypotheses that suggest how the categories are expected to influence the applicability of automated IT controls. In essence, we can only actually identify such relations between the two subjects by studying it in practice. Therefore, the seven categories and characteristics are included in the case study, next to the gained knowledge about automated IT controls from chapter 3, in order to test the hypotheses about the potential relations between them.

Table 5. Eventual list of categories with corresponding public sector characteristics

Public sector characteristics		
Categories	**Nr.**	**Characteristics**
Environment	C1	Great variety of stakeholders, placing demands and constraints that are likely to be conflicting
Goals & Values	C2	Many externally set goals that transcend single-organisational interests, leading to a wide scope of concern
	C3	Multiple goals, many of which can be: complex, intangible, or conflicting
	C4	Numerous ethical and public values
Political control & Bureaucracy	C5	Many political and legal constraints, including bureaucracy
	C6	Instability, resulting in: short-range planning and focus on quick results; discontinuities and disruptions in IT, and a bad effect on IS success.
Resources & Capabilities	C7	Wide array of resources and capabilities to utilise
	C8	Less control over the inputs and mix of organisational resources than in the private sector
	C9	High data sharing beyond organisational boundaries
	C10	Difficult and unstable information requirements
	C11	Little financial flexibility for quick changes in IS projects
Performance & Evaluation	C12	Performance targets are inherently unclear
	C13	Performance evaluation is complex due to indefinable or immeasurable targets
Organisation & Structure	C14	Significant organisational interdependence
	C15	Compartmentalised, or 'silo', organisational structure
	C16	Little changes in organisational structures, which are mostly steered by regulatory changes
Uniqueness of Tasks & Position	C17	More multidimensional tasks and different problems compared to the private sector
	C18	Usage of unique sanctions and coercive powers for the execution of specific activities

Table 6. Hypotheses about the potential relations between categories of public sector characteristics and the applicability of automated IT controls for external fraud prevention in the public sector

Nr.	Hypotheses
H1	*Environmental factors negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H2	*Goals & Values negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H3	*Political control & Bureaucracy negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.*
H4	*Resources & Capabilities neutrally influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H5	*Performance & Evaluation negatively influences the applicability of automated IT controls for external fraud prevention in the public sector, but this is not expected to be significant.*
H6	*Organisation & Structure negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.*
H7	*Uniqueness of Tasks & Position neutrally influences the applicability of automated IT controls for external fraud prevention in the public sector.*

Furthermore, the guidelines that we want to design will be based on the identified public sector characteristics. These characteristics might cause that the current frameworks for developing IT controls have to be extended by the to-be designed guidelines. This links the identified public sector characteristics also to the process of developing automated IT controls, since the guidelines will describe how such developmental processes are affected by certain characteristics. These guidelines will be designed after the case study.

Until now, we used current knowledge from literature in order to gain a better understanding of the two subjects of this thesis, and to come up with the previously mentioned hypotheses that describe potential relations between them. The next step is to generate new knowledge, which is done by performing the case study, as described in the next chapter. The hypotheses are tested and this leads to new knowledge about the actual relations, and might also lead to new insights about automated external fraud prevention in general.

Part III

Part III presents the practical part of this thesis. The theoretical background is now used in the case study, in which we want to extract findings from practice. Interviews will be performed to come up with these findings, after which the results will be analysed. After that, a part of the scientific design activity is performed, by designing the guidelines that we mentioned earlier. By performing these activities, the two most important research questions will be answered, including the main research question. More general discussions and conclusions are then presented in Part IV.

5 Case study

We perform an observational case study to get insights from practice about which public sector characteristics actually influence the applicability of IT controls for external fraud prevention, and in which way they do so. By testing the previously mentioned hypotheses, we can extract such relations. In this chapter, we discuss how we organised this case study, and subsequently discuss the results.

5.1 Case study content

We conduct interviews with representatives from Dutch public sector organisations to extract the influential factors we discussed before. By conducting interviews, we can test the previously described hypotheses about the influential categories and corresponding public sector characteristics. While doing this, we aim to identify if the factors that are discussed by the interviewees relate to the 18 specific public sector characteristics mentioned in Table 5, so we can judge the influence of the categories to which those characteristics belong.

Objectivity is very important here, in order to not explicitly steer to answers that might be most interesting for this research. Therefore, we set up an interview framework, which will be first discussed. After that, the interviews are conducted, and results are filtered from them accordingly. The last section of this chapter presents a discussion about the results, and concluding remarks about the case study.

Conducting interviews is the most commonly used method of qualitative research, and especially useful for exploring complicated phenomena that require elaborate descriptions of meaning [74]. To assure that exploring such phenomena is done properly with respect to completeness and to prevent bias, an interview framework is set up. This framework is presented in Appendix B.

For each interview, we came up with brief descriptions of scenarios of potential improvements to specific control processes, or how an ideal control process could look like for the corresponding organisation. We do this for two reasons: 1) to discuss the possibilities of increasingly using automated IT controls for external fraud prevention, and 2) to identify the influential public sector characteristics with current automated solutions, but also those that are influential when potential automated improvements would be made. During the interviews, additional scenarios can be added promptly while discussing possibilities with the experts. In the next section, these additional scenarios will be simultaneously discussed with the scenarios that were made upfront, which are shown in Appendix C.

As previously mentioned, these interviews are conducted with employees of a small sample of public sector organisations in the Netherlands. We selected organisations that deal with external fraud and are potentially able to address the prevention of it with automated IT controls. For reasons of confidentiality, we cannot describe the organisations and the scenarios in detail, but the eventual results are not influenced because of this.

We were able to perform interviews within four public sector organisations. In each of these four organisations, one expert with the appropriate understanding of the context was available. Control processes on external fraud, and organisational characteristics, vary to a significant degree between the selected organisations. This makes our sample of organisations more representative and ensures that

our results are less one-sided, although we do not study organisations from other countries. The employees that are interviewed, are those having managerial responsibilities with respect to control processes for preventing fraud or errors, internal control and/or IT control.

The results of the interviews are discussed in the next section.

5.2 Interview results

We now describe what was discussed during the interviews. We discuss an organisation, the investigated control process(es) within that organisation, and how automated IT control could improve those processes. For reasons of confidentiality, characteristics of the organisations and the current control processes might be discussed very high-level and simplified. The expert opinion of the interviewees is then discussed, after which we extract which and in which way factors influence the applicability of such automated IT controls.

We use a five-point scale to indicate in which way and how significant an identified factor influences the applicability of automated IT controls; we will now call this the effect of that identified factor. Since we expect that it is hard to attach clear values of measurement to all identified factors, we have to include some 'soft' values here. We will use the scale that is presented in Table 7.

Here, a positive effect means that the characteristic is shaping possibilities for automated IT controls to be applied for external fraud prevention in the public sector. A negative effect means that a characteristic is posing constraints on the ability to apply automated IT controls for the same purpose. So both positive and negative effects have significant influence on the applicability of automated IT controls, and both are important to consider.

Table 7. Five-point scale for indicating the effect of an identified factor

Effect	Name	Description
--	Very negative	Important negative effect
-	Negative	Medium negative effect
+/-	Neutral	Slightly positive or negative, but not significant
+	Positive	Medium positive effect
++	Very positive	Important positive effect

For reasons of completeness, we not only included identified public sector characteristics as factors, but also included observed factors that could not directly be related to such characteristics, but were mentioned by the experts. For each organisation, we observed the influential factors and identified if they relate to characteristics from our categories of public sector characteristics. Separate tables with the observed results from each interview can be found in the next four sections.

5.2.1 Organisation A

Organisation A is a large, centralised governmental agency that acts on a nation-wide level. Although it faces direct supervision from a Ministry, it operates independently, with its own budget and board of directors. The control process that was discussed within this organisation, is related to the distribution

of a specific kind of public resources to a large group of people. Those persons can make a request for this and receive the public resources if they fulfil certain requirements. A part of them receives more of these resources than others, because of certain differences in personal circumstances. This simplified process of when a person makes a request and is assigned certain public resources, is depicted in Figure 8. It has to be continuously checked if the persons that receive extra public resources, still legitimately receive this, or if they are lying about their personal circumstances and are committing fraud.

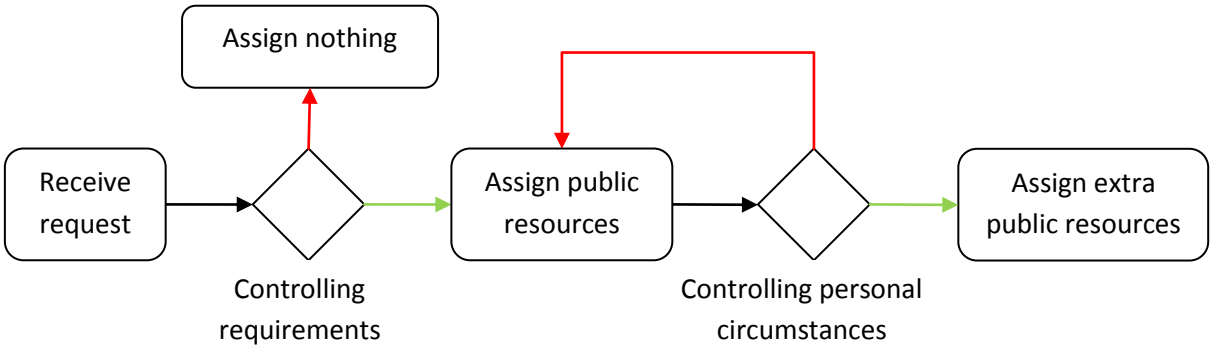

Figure 8. Simplified representation of the decision process for handling a request for public resources in organisation A. (A red arrow indicates a negative decision after which the process ends, a green arrow indicates a positive decision)

The current control process is mainly detective (reactive), partly because of the need for continuous controlling. This continuous control process is quite sophisticated already. Automated data-analyses, performed with data from multiple sources , are executed periodically (monthly). This way, potential offenders are extracted using a risk profile, after which some manual actions are necessary to see if someone is actually committing fraud. One specific manual action is performed by a third party. This current process is already quite efficient, because of all identified potential offenders that are checked in practice, a large part is also actually committing fraud. Measures can be taken against them subsequently.

This current control process could be improved by implementing more automated IT controls. Two possible scenarios were discussed for this: 1) more automated controls before assigning the extra public resources in the first place, and 2) automated controls that replace some of the manual actions that are performed after data-analysis, which could eliminate a lot of manual work. These possibilities were proposed during the interview, and the opinion of the expert was asked about these possibilities. Since sophisticated data-analyses are already performed automatically, there is no possibility to improve this part of the process with more IT controls, according to the expert.

With respect to implementing more automated IT controls before assigning the extra public resources in the first place, this would mean such controls increase the automated assessment of a request for extra public resources. According to the expert, it is not possible to reject a request based on the execution of some IT controls, since the law requires that the specific manual action by a third party must be performed before a person can be indicated as fraudster. In other words, the organisation has to wait for the manual action by a third party before it can legally stop the payment of extra public resources to

a person that should not receive it. Clearly, there are some legal constraints here for increasingly using automated IT controls.

Therefore, more IT controls for increased automated assessment of a request can only be used to assess the risk of fraud in advance. The only advantage that could be reached compared to the current control process is that a potential offender is identified somewhat earlier and the manual action by the third party could be steered earlier. The expert was clear in stating that in practice, this would probably not make a big difference.

The second way in which automated IT controls could improve the control process, is to automate some of the manual actions that are still performed after the data-analyses. The expert stated that the process cannot be completely automated for two reasons. First, the manual action by the third party will always remain a manual action in practice. Secondly, extraordinary personal circumstances may be very hard to detect automatically. It is always necessary to have a 'human eye' look at the circumstances before someone is perceived as a potential offender, according to the expert. This implies that the risk profile is not 100% trustworthy in judging about fraudsters. Knowledge of extraordinary circumstances and how to interpret specific relations between data is something that cannot be completely automated.

In addition, the organisation has an extra responsibility of carefulness, which is a specific public sector value. Carefulness is even defined in the law, to assure that governmental agencies take each individual decision well prepared, with proper research of facts and interests, in accordance with procedures, while correctly treating each civilian. A popular political view is that this requirement needs human intervention, which limits the possibilities of automated IT controls.

Furthermore, the expert stated that not all data from external sources can be extracted automatically, due to technical constraints. In other words, they already have access to the resource, but have to extract it manually. Although this is quite related to Resources & Capabilities, there was no directly related characteristic, and we therefore identified it as not relating to a category of public sector characteristics. A further discussion of this factor will be given in upcoming sections.

Other factors that influence the applicability of automated IT controls in the control process were identified and discussed during the interview. The results are presented below in Table 8 and Table 9.

Table 8. The identified factors for organisation A that relate to the categories of public sector characteristics

Category	Identified factor	Related characteristic	Effect
Goals & Values	Carefulness	C4	--
Political control & Bureaucracy	Privacy	C5	-
	Legitimacy	C5	+/-
Resources & Capabilities	High data sharing possibilities	C9	++
Uniqueness of Tasks & Position	Unique powers for controlling	C18	+

Table 9. The identified factors for organisation A that do not relate to the categories of public sector characteristics

Identified factor	Effect
'Human eye' necessary for interpretation	--
No technical possibility of sharing all data automatically	--
Dependency on possibilities of reliable risk profile(s)	-

We also asked the expert about the approach that is followed for developing internal control and IT controls. The expert stated that the organisation uses a Risk Management approach, and that they developed their own approach for translating identified risks in (IT) control needs.

5.2.2 Organisation B

Organisation B is a large municipality (150,000-200,000 citizens), which faces supervision of its own city council for the execution of the tasks that are decentralised to local governments. The control process that was discussed during the interview is related to the distribution of public resources among certain citizens of the municipality. These public resources are benefits that every municipality in the Netherlands can distribute. Citizens can have the legal right to receive these benefits. A person can make a request for the benefits, after which his personal circumstances are checked. When certain requirements are fulfilled, a person can receive these benefits, but continuous controlling of his personal circumstances is necessary to determine if that person is still legitimately receiving it. Especially when changes occur in personal circumstances, this should be checked to see if these changes should have an effect on receiving the benefits. If a person deliberately conceals information in order to unlawfully receive benefits, that person commits fraud.

According to the expert, the current control process in this municipality is quite standard in many municipalities. The current control process is both preventive and detective, but also mainly manual, so possibilities for automated IT controls could be high. When a request is filed, an initial manual check on data is performed. When this check does not immediately rejects the request, an appointment is made where an employee and the requester will talk about the personal circumstances. The requester must hand in certain documents that confirm his circumstances. After this, it can be decided that the request is rejected, or that the person can receive benefits and also how much. While receiving benefits, the circumstances of the person are periodically controlled by manually checking with data from another public organisation, which is a centralised agency that collects relevant and updated data about persons. During the several stages of this control process, risk profiles are used to assess the risk of fraud.

This current control process might be improved by implementing more automated IT controls in the following ways: 1) automating the initial check on data, 2) replacing (parts of) checks from the appointment by automated checks, and 3) automating the periodically controlling of personal circumstances. These scenarios were all discussed with the expert.

The initial check on data by automated IT controls could mean that no human intervention is necessary, by automatically checking the most simple requirements for which data is already available to the municipality. Examples are checking if the person is 18 years of age or older, and if the income of the person does not exceed a predetermined threshold. According to the expert, it is possible to automate this initial check, but since this does not present a complete image of the situation, an appointment is always necessary to fully determine the current personal circumstances. Nevertheless, we can conclude that the available data and technical possibilities are sufficient to use automated IT controls for the initial check.

It is somewhat harder to fully replace certain checks from the appointment and have the same reliability as with manual checks. For example, it is possible to automatically check if a person has some registered properties, but to determine the value of them is somewhat harder to do automatically. In general, certain checks can definitely be automated, but more information might be necessary, which is also discussed during the appointment. Next to this, the expert claims that extraordinary circumstances occur, which calls for the inclusion of looking at each situation with a 'human eye'. This must ensure the public value of doing things correctly for each case. According to the expert, it is also a cultural problem that most employees think that manual controlling is the natural way for doing it correctly for each case.

Furthermore, the expert stated that politics also play a very important role in the preservation of the appointment. The expert explained that fully automating the checks could become feasible in the public sector, "but not in the political sector". The previously discussed term of carefulness is very much related to this, which negatively influences the applicability of automated IT controls.

Next to this, pressure groups can be of influence. Pressure groups generally represent a group of people or organisations with certain values or interests, mostly based on a shared political, religious, moral, or commercial position. An example of a pressure group is a so-called 'privacy watchdog', which protects privacy of civilians. Pressure groups pose constraints on the extent to which citizens are being 'watched', which therefore has a negative effect. Further explanations about this are provided later in this chapter.

Finally, automating the periodically controlling of personal circumstances is partly possible, but there are always manual actions that should be performed in practice to ascertain the situation. The expert agreed that when certain data is changed, an automated check could be performed to see if the benefit is still legitimately received or should be stopped. The high availability of data is a positive influential factor here. However, this cannot always guarantee a complete image, which indicates that manual checks are sometimes preferred. Quite to the contrary of what we are discussing here, the municipality would most ideally also check data from private organisations. One example is the privatised water company, which could provide data about water usage to determine the risk that someone is not living alone, but could possibly have a bigger household than mentioned. Automated solutions for this are forbidden due to privacy laws, which limits the high availability of data to some extent.

Furthermore, other factors that influence the applicability of automated IT controls in the control process were identified and discussed. The results are presented in Table 10 and Table 11.

We also asked the expert about the approach that is followed for developing internal control and IT controls. The expert stated that the organisation uses a Risk Management approach and a common standard that is used by similar organisations for similar control purposes. Based on this standard, procedures are developed mainly for the processes, not specifically for IT control. In a similar way, IT controls are taken care of, which are audited by an external party.

Table 10. The identified factors for organisation B that relate to the categories of public sector characteristics

Category	Identified factor	Related characteristic	Effect
Environment	Pressure groups	C1	-
Goals & Values	Carefulness	C4	--
	Doing things correctly for each case	C4	-
Political control & Bureaucracy	Privacy	C5	-
Resources & Capabilities	High data sharing possibilities	C9	++
	Little financial flexibility	C11	+/-
Performance & Evaluation	Performance targets unclear	C12	-

Table 11. The identified factors for organisation B that do not relate to the categories of public sector characteristics

Identified factor	Effect
'Human eye' necessary for interpretation	--
Dependency on possibilities of reliable risk profile(s)	-

5.2.3 Organisation C

Organisation C is a centralised agency that operates independently and faces direct supervision of a Ministry. One of its responsibilities is signalling potentially fraudulent activities performed in organisations, which includes both vertical and horizontal fraud.

The current control process consists of a very sophisticated data-analysis system, in which data from multiple external resources is analysed against risk profiles that are periodically updated. This results in system signals, after which manual controlling with even more data is performed by an employee to ascertain if corresponding law enforcers should be contacted about the risk of fraudulent activities.

Whereas the previous two cases showed more clear possibilities for essential improvements by using automated IT controls, such possibilities are harder to identify in this case. Overall, it is hard to improve the current 'control' (or signalling) system in such a way that much more external fraud is prevented or detected, or that it is detected much earlier. With respect to the current system that is already very automated and quite preventive, we only study 1) if there are possibilities to create current system signals even earlier, and 2) if the manual part of the control process can be replaced by automated IT

controls. This case is thus mainly interesting for our main goal of extracting factors that influence the applicability of automated IT controls, and not that much for improvement scenarios.

The expert indicated that when system signals should be created even earlier, there should be automated IT controls at the external sources that should be triggered when specific changes are made to data that is input to the risk profile, or when new entities are created. However, this would mean that a part of the signalling function would move to the organisations that are managing the external sources, but there is no legal ground for that. The signalling function is legally assigned to just one organisation, so there should be changes in the law to do the signalling even earlier, but the expert stated that this is not likely in the foreseeable future.

We then discussed the possibilities of replacing the manual part of the process by automated IT controls. The expert stated that this would be preferred eventually, but that it is hard to do so. First of all, data from some external sources cannot be extracted automatically. One reason for this can be that such external parties do not have centralised or suitable databanks to be an automated data supplier, which leads to the inability of extracting data automatically. This is a significant influential factor here. Even more important, according to the expert, is the that the eventual risk identification of external fraud should be manually performed with a 'human eye', since it is impossible to automate all human knowledge of possible situations.

Furthermore, the previously mentioned factor of carefulness is also applying to this organisation, and also in a negative way. On the other hand, the unique powers that are lawfully assigned to organisation C positively influences the potential of extracting a lot of data automatically. Related to this is that data sharing between public organisations is relatively high, which certainly accounts for organisation C.

All factors that were identified that influence the applicability of automated IT controls in the control process are presented below in Table 12 and Table 13.

Table 12. The identified factors for organisation C that relate to the categories of public sector characteristics

Category	Identified factor	Related characteristic	Effect
Environment	Pressure groups	C1	-
Goals & Values	Carefulness	C4	--
Political control & Bureaucracy	Difficult laws	C5	-
	Instability	C6	+/-
Resources & Capabilities	High data sharing possibilities	C9	++
	Little financial flexibility	C11	-
Uniqueness of Tasks & Position	Lawfully assigned unique powers	C18	++

Table 13. The identified factors for organisation C that do not relate to the categories of public sector characteristics

Identified factor	Effect
'Human eye' necessary for interpretation	--
No technical possibility of sharing all data automatically	--
Dependency on possibilities of reliable risk profile(s)	-

We also asked the expert about the approach that is followed for developing internal control and IT controls. The expert stated that the organisation uses a Risk Management approach that is steered by the Ministry, but also incorporated in the IT control standard that is used. This IT control standard is specifically designed for public organisations in the Netherlands and focuses on information security and related control concepts, which are tailored for these organisations.

5.2.4 Organisation D

Organisation D is a centralised agency that operates independently and faces supervision from a Ministry. It is assigned with specific tasks, which mainly involves the distribution of a specific kind of public resources. Two different stakeholders are involved with receiving these public resources. Stakeholder X is the actual receiver of the public resources, for which X has to deliver services to stakeholder Y. Stakeholder Y has to fulfil certain requirements before the public resources are assigned to X, from which Y then can receive the services. Figure 9 represents a simplified representation of this process, in case the public resources are assigned. Organisation D has to control both stakeholders X and Y, and the control process consists of checking data about both stakeholders, and controlling the legitimate assigning of public resources, both before and after the public resources are actually distributed.

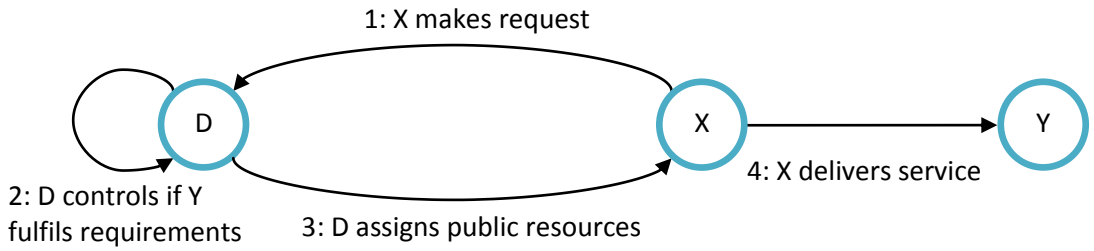

Figure 9. Simplified representation of the stakeholders and activities in the process of assigning public resources from organisation D to stakeholder X

Organisation D is currently working on a transition to a new system, in which the control process will be improved. We took the old system as a starting point, discussed the changes that will be made in the new system, and also discussed more possibilities for even further improving the control process with automated IT controls. We now present the results by combining the discussions about the changes that

will already be made in the new system with the scenarios that were proposed for an ideal control process.

When a request is filed, certain requirements can be automatically checked with data from external sources. This can lead to the automated assigning of the public resources, or a necessary manual check in case the available data is not sufficient. According to the expert, this will be a sufficient preventive check, in which the possibilities of automated IT controls are maximally used. As was the case in previous cases, organisation D subsequently faces necessary manual checks that can absolutely not be replaced by automated IT controls. This is, again, caused by the necessity of a 'human eye' to look at complex situations.

However, the expert stated that automated IT controls could assist in steering how the manual checks are performed. If a reliable risk profile could be set up, automated IT controls could assist in indicating if there are cases with a high risk of unjustified distribution of public resources. These could then be manually checked, which can lead to a much more effective and efficient control process. The expert claims that it must be technically possible, but it is unknown if a reliable risk profile can be made that can effectively steer the necessary manual part.

In another part of the control process, organisation D controls certain amounts that are filed by one of the stakeholders. According to the expert, automated IT controls are very suitable for preventively checking if that stakeholder does not file higher amounts than he is supposed to file. With the necessary data already available in-house, the inclusion of this in the new system must be possible. Overall, this means that this organisation faces less influence of privacy issues for applying automated IT controls in this part of the control process. To the contrary, privacy issues certainly have influence in other parts.

In general, organisation D can extract data from external sources, but for some of the external parties yields the same as we discussed for organisation C: some of the external parties do not have an organisation that is suitable for being an automated data supplier. The expert mentioned that slow political decision processes might also lead to the inability of incorporating more automated extraction of external data in an IT project, but this does eventually not influence automated IT controls itself.

All factors that were identified that influence the applicability of automated IT controls in the control process are presented below in Table 14 and Table 15.

Table 14. The identified factors for organisation D that relate to the categories of public sector characteristics

Category	Identified factor	Related characteristic	Effect
Goals & Values	Carefulness	C4	--
Political control & Bureaucracy	Privacy	C5	-
Resources & Capabilities	High data sharing possibilities	C9	++
	Little financial flexibility	C11	+/-

Table 15. The identified factors for organisation D that do not relate to the categories of public sector characteristics

Identified factor	Effect
'Human eye' necessary for interpretation	--
No technical possibility of sharing all data automatically	--
Dependency on possibilities of reliable risk profile(s)	-

We also asked the expert about the approach that is followed for developing internal control and IT controls. The expert stated that the organisation uses a Risk Management approach that is based on a standard for internal control that is used in public organisations. The need for controls will become apparent from that, after which (IT) controls are developed.

5.3 Case study results

We now evaluate which identified factors were found during the interviews, and in which way and how strongly they appear to influence the applicability of automated IT controls. Table 16 presents an overview of the scores for the categories from each organisation separately. Both positive and negative effects are important to consider here, because they, respectively, shape possibilities or pose constraints on the applicability of automated IT controls.

We start with discussing the categories of public sector characteristics that were identified from the literature, from which hypotheses were set up. After that, we discuss other characteristics that were found from the interviews, but which do not pertain to the specific public sector characteristics.

Table 16. Overview of all scores for the categories of public sector characteristics, for each organisation separately

Categories	Organisation			
	A	B	C	D
Environment		(--)	(-)	
Goals & Values	(--)	(--), (-)	(--)	(--)
Political control & Bureaucracy	(-), (+/-)	(-)	(+/-), (-)	(-)
Resources & Capabilities	(++)	(++), (+/-)	(++), (-)	(++), (+/-)
Performance & Evaluation		(-)		
Organisation & Structure				
Uniqueness of Tasks & Position	(+)		(++)	

5.3.1 Environment

Two of the organisations (B and C) face environmental influences for applying automated IT controls. Especially certain pressure groups that reside in these organisations' environment are important. 'Privacy watchdogs' are one of them, and they usually want to influence public opinions and/or policies by using various forms of advocacy. Since public sector organisations are able to share much more

personal data with each other than private sector organisations, these pressure groups will put much more pressure on such public sector organisations.

The experts from organisations B and C mentioned that such pressure groups can use forms of advocacy to influence how control processes within these organisations must be organised. Both experts indicated that pressure groups that relate to protecting citizens' privacy play the most important role here. These groups usually want to prevent that governments can use much data sources and compare data automatically, in order to prevent that a 'Big Brother' government is created, in which privacy of citizens is minimised. By using advocacy, these groups can have significant influence on how much data about citizens can be ethically checked by certain public organisations automatically, which in turn influences to which degree automated IT controls can be applied in control processes of public sector organisations. It does, however, not prevent that such controls can actually be used, so we indicate the effect as negative.

5.3.2 Goals & Values

All four experts indicated that characteristics from this category are influential factors. The most important factor is carefulness. This could also be interpreted as a legal constraint, since it is defined in the law and public organisations should abide it. We mainly interpret it as a public sector value, which is the reason it was defined in the law in the first place.

Automated IT controls cannot be applied in case the value of carefulness causes that such controls are deemed to be not careful enough. In other words, when there is doubt that making a certain decision automatically would not fully satisfy the carefulness demands, that decision should better be made manually, instead of an automated solution such as automated IT controls. All experts judged the effect of this factor as being very negative and we therefore conclude the same.

Furthermore, one expert mentioned that in his organisation, they want to do "things correctly for each case". This is interpreted as both a goal and a value. It is somehow related to the value of carefulness, with a small difference. The difference is that carefulness pertains to the process of decision-making for a case, while "doing things correctly for each case" is more related to the decision itself, and the corresponding actual result. The decision and the result should always be correct with respect to the current information at hand. Of course, this cannot always be fulfilled. Nevertheless, it can influence the degree to which automated IT controls can be applied in public organisations. Since there is only one organisation in which this was identified, we judge this factor as not significant and will discard it.

The eventual effect of this category is very negative, due to the very strong influence of the carefulness principle.

5.3.3 Political control & Bureaucracy

All four experts indicated that characteristics from this category are influential factors. Several factors were mentioned, of which privacy was mentioned by three out of four experts.

Privacy issues were mentioned before as the main driver for certain pressure groups. In this category, privacy pertains to the legal and political constraints of privacy, which are caused by the law and

politicians respectively. Privacy is already a constraint in control processes in general, but we only want to extract factors that are specific to automated IT controls. In which way is there a difference that makes privacy a specific influential factor for automated IT controls, instead of an influential factor for control processes in general?

When looking at the privacy law in the Netherlands [76], there are some differences between processing personal data manually and processing personal data (partly) automatically. One difference is that the automated processing of personal data always has to be reported to the national, independent authority that protects privacy ('CBP'), whereas this must not always be reported in case of manual processing. Furthermore, the logic behind the automated processing has to be explained in case a 'stakeholder' has the right to ask for this. Also, it is forbidden to make certain decisions when they are solely based on the automated processing of personal data in order to get an image of the personality of the corresponding person.

With respect to applicability of automated IT controls in the context of this research, these differences in the law are not very important factors as to why the experts mentioned privacy. Political decision-making is more important, since politicians are usually very careful with deciding about automated coupling of data sources and approving 'black boxes' for enhanced data analyses on personal data of many civilians. Although here counts that it is still technically possible, political decision-making caused by privacy issues certainly influences if automated IT controls can be applied. The previously mentioned effect of pressure groups might also influence how politicians make decisions, but since we did not observe such a relationship, we assume that this is not the case here. The three identified scores on privacy together therefore lead to a negative effect.

Some other factors were also identified (legitimacy, difficulty of laws, political instability), but since each of these were only identified by only one expert, we conclude their effect is not significant. The eventual effect, however, remains negative.

5.3.4 Resources & Capabilities

All four experts indicated that characteristics from this category are influential factors. Two factors can be identified as significant, which are high data sharing possibilities and little financial flexibility.

High data sharing possibilities between public organisations is an important positive factor for the applicability of automated IT controls, which was equally judged by all four experts. Recent developments of centralising huge amounts of data in a limited amount of databanks leads to increased possibilities to extract data automatically. All experts stated that their organisation was assigned with the capability to use such external sources. It is clear that this has a very positive effect.

Three out of four organisations also identified that little financial flexibility, with special attention for IT projects, has a an effect. These organisations face tight budget planning and do not have the flexibility for fast attainment of resources in case new options for automated solutions are identified, or project costs are going to exceed limits. Of course, accurate business cases and project planning can partly prevent this, but manual checks might still be preferred above automated checks because of that, and this might prevent the level of automated controls that is used in IT systems in public organisations.

However, the identified effect in two of the organisations is not significant. Therefore, we have to conclude that the effect is not strong enough for further studying.

The eventual effect then becomes very positive.

5.3.5 Performance & Evaluation

Only the expert of organisation B mentioned that due to unclear performance targets, that organisation is more reluctant to apply automated IT controls. The expert stated that it is hard to set targets with clear values of measurement, which can lead to difficulties in setting hard criteria for automated controls. Since only one expert mentioned this factor, we have to conclude that this category has no significant effect.

5.3.6 Organisation & Structure

None of the experts identified factors in this category. We therefore conclude that this category probably has no effect on the applicability of automated IT controls.

5.3.7 Uniqueness of Tasks & Position

Experts of two organisations (A and C) indicated that a factor in this category is an influential factor. Both mentioned the unique power that is assigned to their organisation for controlling purposes.

Both organisations are lawfully assigned with specific powers to design a control process in an extensive way. The two experts stated that possibilities for automated IT controls are higher since their organisations has such unique powers. Since two out of four mentioned this, and one of them indicated that it is very important, we conclude that this has a positive effect overall.

5.3.8 Other influential factors

Some other influential factors were identified that do not directly relate to the categories of public sector characteristics. However, it is still possible that these factors are public sector characteristics, but further research is necessary to assess this. We take a neutral view here and only refer to them as influential factors. For reasons of completeness, these identified factors are added to our study, in case they were perceived significant by the experts.

First, all experts agreed on the fact that a ‘human eye’ is necessary for good interpretation of certain situations. In addition, this has an important negative effect on the applicability of automated IT controls according to each expert. Although it is somewhat related to the need for manual controlling in case the public value of carefulness holds, there is an essential difference. Both call for manual controlling, but a ‘human eye’ is necessary to see extraordinary circumstances and to interpret specific relations between data that is almost impossible to do completely automated. This ‘human eye’ criteria could very well also be necessary in certain private sector control processes. We claim that this is currently unknown, partly because the term is quite vague and a little bit prone to subjectivity. What we do know, is that all experts are clear about the need for a ‘human eye’ in difficult control processes at some point, and this will always be necessary in the foreseeable future. Therefore, we conclude that it has a very negative effect.

Secondly, and very much related to the previously discussed factor, is that there is a dependency on the possibilities of creating reliable risk profiles. All experts stated that for automated external fraud prevention to be effective, reliable risk profiles are essential. Of course, this is also the case for manual controlling, but a collection of risk indicators can then also be judged somewhat subjectively, based on experience and instinct. For automated controlling with a risk profile, it must be possible to calculate the chances of fraud according to 'hard' criteria. In other words, you must be able to trust on historical data, from which you can select a collection of risk indicators that can reliably determine the risk of fraud, while being based on objective and measurable values.

The problem is that setting up such a reliable risk profile is not always possible, for example when there are no effective and decisive criteria that you can use to accuse someone of fraud. All experts mentioned that they are struggling to find the best 'recipe' for risk profiles that can be automatically checked. Since a good 'recipe' is necessary to be able to completely control automatically, dependency on the possibilities of reliable risk profiles is negatively influencing how automated IT controls can be applied. We conclude by stating that it has a negative effect.

Finally, there is not always a technical possibility of sharing all data automatically, by which we mean that some data is already manually attainable, but cannot be extracted automatically. One reason that was mentioned by an expert is that external parties are not organised properly and do not have a centralised databank that can be used for automated data extraction. A second important reason is that some public organisations are very reluctant in rapidly sharing data; they provide it eventually, but they do not simply provide data immediately when it is asked for by other public organisations. Although the official possibilities for high data sharing are present, this reluctance in actually sharing data rapidly is causing that explicit manual procedures must sometimes be followed in order to get the data, which limits the rapid possibility of sharing data automatically. Both reasons have direct implications for the possibilities of automated IT controls, so the effect of this is very negative, which was also indicated by three experts.

For ease of representation, we take these other influential factors together in one category, which we will call Failing Technology/Manual Necessity. The eventual effect of this category is very negative.

5.3.9 Conclusions

We first summarise the eventual results, by presenting Table 17. The eventual effect of each category, as described in previous sections, are shown.

Table 17. The identified, significant effects of all influential categories

Category	Effect
Environment	-
Goals & Values	--
Political control & Bureaucracy	-
Resources & Capabilities	++
Uniqueness of Tasks & Position	+
Failing Technology/Manual Necessity	--

Now we can make concluding statements about the hypotheses. Table 18 shows all hypotheses once again. The hypotheses H1, H2 and H3 can all be confirmed, since the expected negative influences of the corresponding categories were also observed in the case study, with the strongest negative effect observed for H2. The main factors behind the negative effects of these categories are, respectively, pressure groups, carefulness, and privacy. These three main factors cause that their corresponding categories pose constraints on the ability to apply automated IT controls for external fraud prevention.

Table 18. Hypotheses about the potential relations between categories of public sector characteristics and the applicability of automated IT controls for external fraud prevention in the public sector

Nr.	Hypotheses
H1	*Environmental factors negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H2	*Goals & Values negatively influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H3	*Political control & Bureaucracy negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.*
H4	*Resources & Capabilities neutrally influence the applicability of automated IT controls for external fraud prevention in the public sector.*
H5	*Performance & Evaluation negatively influences the applicability of automated IT controls for external fraud prevention in the public sector, but this is not expected to be significant.*
H6	*Organisation & Structure negatively influences the applicability of automated IT controls for external fraud prevention in the public sector.*
H7	*Uniqueness of Tasks & Position neutrally influences the applicability of automated IT controls for external fraud prevention in the public sector.*

The hypotheses H4 and H7 must be rejected, since the evidence shows support for a positive relationship, instead of the expected neutral one. This means that we underestimated the effect of the corresponding categories, which apparently shape possibilities for automated IT controls to be applied. With respect to Resources & Capabilities (H4), support for a very positive relationship is apparent, due to the main factor of official possibilities for high data sharing. The unique powers that can be assigned to public organisations for controlling on external fraud is causing the positive relationship for the category Uniqueness of Tasks & Position (H7).

There is not enough support for hypotheses H5 and H6, which are therefore rejected. These categories and their corresponding characteristics do not significantly shape possibilities, nor pose constraints, on the applicability of automated IT controls for external fraud prevention. This means that the expected relationships that were derived from findings in the literature were, in the context of this research, not observed in practice.

In addition, the new category of Failing Technology/Manual Necessity provides some additional insights. Although the corresponding characteristics cannot be identified as public sector characteristics, they pose major constraints on the ability to use automated IT controls for external fraud prevention. In addition, we stress that these will also influence automated external fraud prevention in general, but

more research is necessary to be certain of that. All three identified characteristics are important issues here, which concerns reliable risk profiles, extracting data from external parties in an automated way, and the necessity of a 'human eye' in the control process.

5.4 Case study discussion

Now the results of the case study are presented, we have to discuss the most important findings, how we can use them, and the limitations of these case study.

5.4.1 Evaluation of results

The results show that there are indeed specific public sector characteristics that influence the applicability of automated IT controls for external fraud prevention. Support was found for five of the seven categories that were included in the case study. Most of these five significant categories of public sector characteristics are mainly supported by only one strong corresponding characteristic from that category. It could be argued that the category should then be discarded and only the characteristic should be taken for further studying, but for reasons of clarity, we stick with the name of the category. However, to ensure the appropriate further studying, we will take into account the dominant effect of one characteristic in a category. These dominant public sector characteristics within the categories are the following:

- Influence of pressure groups
- Public value of carefulness
- Legal constraints of privacy
- Possibilities for high data sharing
- Unique powers for controlling purposes

The following additional, strongly influencing factors were found, which we assigned to a new category:

- Inability to create reliable risk profiles
- Inability to extract data automatically
- Necessity of a 'human eye' in control processes

The additional important category (Failing Technology/Manual Necessity) that was found, does not directly relate to the public sector characteristics. Since that category turned out to be very influential according to the experts, it cannot be overlooked. The category also imposes some incongruence in the results with respect to data sharing. Within the category of Resources & Capabilities, high data sharing possibilities very positively influence the applicability of automated IT controls in the sense that much data is available and centralised. To the contrary, the Failing Technology/Manual Necessity category claims that there are several examples in which automated data sharing between public organisations is technically not possible or not yet possible, which very negatively influences that applicability. This causes that Resources & Capabilities can only positively influence the applicability of automated IT controls in case the Failing Technology/Manual Necessity category does not already negatively influence it with respect to technical possibilities of data sharing. There is a dependency between these categories that should not be neglected.

However, we focus on the influence of specific public sector characteristics in this research, so we do not further study this category in the next chapter. In others words, we cannot make conclusions about this additional category with respect to differences between the public and private sector. Further research must be performed to determine if this category and its characteristics are specific to the public sector, and if standards should be tailored to incorporate it. Nevertheless, we will take this category into account when we state recommendations about applying automated IT controls for external fraud prevention, and automated external fraud prevention in general.

Now we examined the results, we question ourselves: what do these results add? The ability to apply automated IT controls, for automated external fraud prevention, is dependent on the identified influential categories and the corresponding characteristics, which can shape possibilities or pose constraints for that ability. This knowledge can be used to determine the degree to which automated IT controls are applicable for external fraud prevention in public organisations. The results provide the first scientifically based evidence for the influential relationships between the two subjects that are combined in this thesis; automated IT controls for external fraud prevention, and specific public sector characteristics.

We also stress that the identified characteristics are influential for automated external fraud prevention in general, which can help in determining the degree to which external fraud can be tackled automatically by other IT solutions; however, evidence must be provided to be certain of this. Therefore, we add the following new proposition to theory that needs to be tested:

P1 *The ability to apply automated external fraud prevention in the public sector, is dependent on the influence of the following factors:*
- *a Influence of pressure groups*
- *b Public value of carefulness*
- *c Legal constraints of privacy*
- *d Possibilities for high data sharing*
- *e Unique powers for controlling purposes*
- *f Inability to create reliable risk profiles*
- *g Inability to extract data automatically*
- *h Necessity of a 'human eye' in control processes*

As mentioned before, we found that specific public sector characteristics exist that have an influence on the ability to apply automated IT controls. This adds evidence to the view that differences between the public and private sector should not be overlooked [71]. This strengthens our second research goal, in which we proposed that due to differences between the two sectors, standards from the private sector for developing automated IT controls might need to be tailored to incorporate such influential public sector characteristics. This will be further studied in the next chapter.

5.4.2 Limitations

Some limitations of this case study are quite evidently related to the sample. Of course, one may question if our sample of four public sector organisations actually provides enough evidence to be able

to make the concluding statements we discussed in the previous section. One reason for the small sample is the absence of willingness of some organisations. Despite this limitation, we still argue that we found very representative results from the interviews.

The four organisations that were selected in the case study, certainly differ in structure and activities. However, some similarities can also be found, of which some detailed checks in control processes provide an example of a similarity. Of course, a larger sample that contains more interviews within more organisations could potentially lead to better results. Also, more empirical results are necessary to gain proper acceptance. Nevertheless, we argue that the amount of four organisations is sufficient to make the concluding statements, since similar findings were found among these different organisations, which indicates that coincidence is ruled out significantly.

We mentioned earlier that the scope of the case study is limited to large public sector organisations in the Netherlands that face external fraud problems, from which specific public sector control processes must be installed. Further research is necessary to determine if the results also hold for smaller public sector organisations and organisations in which less specific control processes reside to counter external fraud.

In addition, it is hard to determine if the results can be generalised to the public sector in other countries. It can be assumed that countries that are similar to the Netherlands with respect to political systems and political culture, social security systems, state and use of technology, and other national criteria, will also face the same influential factors. To give an example, Denmark could be an example of a country quite similar to the Netherlands. On the other side, countries with very different characteristics might not be facing the same factors. However, hardly any well-founded theoretical comparison can be made to be fully certain that the results in the specific context of this research can be generalised to other countries. Therefore, it is clear that further research in other countries is necessary to see if results can be generalised to the public sector in general, or specific other countries. For now, we can only make concluding statements about public organisations in the Netherlands.

6 Guidelines

Now all sub research questions are answered in previous chapters, we want to answer the main research question in this chapter. We do this by taking the gained knowledge from previous chapters and combine it in order to present guidelines for developing automated IT controls for external fraud prevention in the public sector. We mainly determine if current standards are sufficient or must be tailored for the influential categories of public sector characteristics that were found in the case study.

As mentioned before, the design science research process by Peffers et al. [60] is partly followed. Identification of the problem is already explained in previous sections. The objective of the solution is to assure that current standards and frameworks that are widely used, are tailored to include the effect that influential public sector characteristics can have on the applicability of automated IT controls. Otherwise, public organisations and organisations that audit or advise about internal control might overlook these essential elements when developing or auditing appropriate measures against the risk factor of external fraud.

The design and development activity is performed in the next sections. When the identified categories of public sector characteristics are not sufficiently covered by current standards and frameworks that are mainly focused on the private sector, we judge how they can be tailored to incorporate those categories. While doing this, the eventual guidelines are set up.

For reasons of completeness, we also incorporate standards and frameworks that are specifically designed for the public sector, to see if the identified influential characteristics are already incorporated by them. This includes standards that were mentioned by the experts during the interviews. Some conditions for including them is that such standards or frameworks must be high-level and can be generically applied to different public organisations. Next to COSO [25], COBIT [35] and ITIL [72], we also add INTOSAI [34] and BIR (Baseline Informatiebeveiliging Rijksdienst) [54]. BIR is mainly focused on information security in Dutch public organisations, but it includes some specific IT control subjects, such as access controls and assurance of proper processing of data. These five will be referred to as standards in the next sections.

6.1 'Gaps' in current standards and frameworks

Based on the results from the case study and the knowledge about automated IT controls and current standards for developing them, we study if there are 'gaps' in these current standards. What we mean by this, is that we look to current standards and assess if the influential categories are sufficiently addressed by them, or if they need to be tailored to these categories. We now discuss each of these influential categories separately.

6.1.1 Environment

This category mainly deals with how to handle pressures from external parties that want to prevent increased (personal) controlling. Environmental influences, however, should not prevent that the best possible solution is initially sought. After investigating potential solutions, it can be determined if those solutions are appropriate and will not cause environmental agitation, which you want to prevent. It is

during this stage that it might be suitable to involve the viewpoints of external parties in the decision process.

The standards take into account some external interests, but this has little to do with a possible resistance against the solution itself. Environmental influences on how the control process should be designed, is therefore not included in the standards. Is it then necessary for developing automated IT controls to tailor the standards for this? We argue that this is not necessary, because the designers of appropriate control activities should focus on finding the best solution within the predetermined possibilities that laws, regulations and procedures provide. Of course, they may already take into account that certain legitimate solutions can still cause resistance with external parties, but in the end, it is the responsibility of politicians to decide whether the wishes of external parties should be granted. Therefore, standards do not have to take explicit consideration for this, and they do not need tailoring for this category.

6.1.2 Goals & Values

The specific goals and values of public sector organisations should be accounted for when designing a control process. We already mentioned that such goals and values can have significant influence on the degree to which automated IT controls can be applied. It might be expected that standards take into account that such specific goals and values can exist that partly determine how a control process must be designed. However, only COSO and INTOSAI mention this. COSO mentions a control principle which states that an organisation should demonstrate “a commitment to integrity and ethical values” [25]. INTOSAI is based on COSO and goes even further by stating that “the ethical aspect of operations” is included in internal control, and that citizens should always “receive impartial treatment on the basis of legality and justice” [34]. What the effect of it is on the development of IT controls, remains unclear.

We argue that for developing automated IT controls for external fraud prevention, goals and values should be incorporated in all standards. By investigating which goals and values apply to a certain control process, it becomes clear to which degree that process can be automated by IT controls, while being in accordance with those goals and values. Not only should this be looked at for internal control in general, but also for the potential of automated IT controls specifically.

6.1.3 Political control & Bureaucracy

In the public sector, political influences and legal constraints are almost everywhere. Regulatory and legal issues, including bureaucracy, must always be taken into account in control processes, especially in public organisations. We can say that COSO, INTOSAI, COBIT, and BIR have explicitly incorporated it, mostly discussed as compliance to laws and regulations. Although ITIL does not mention it specifically, we can still say that attention is given for it and that it needs no further studying.

The related subject of political control is not incorporated in the standards. However, during the case study, the separate effect of political control was not considered to be important. Therefore, we stress that standards do not need to be tailored for political control either.

6.1.4 Resources & Capabilities

Resources & Capabilities positively influences the applicability of automated IT controls. It is now questioned if standards should incorporate it explicitly in order to fully identify its potential benefits. To be more specific, high data sharing possibilities are the main driver here, and pertain to both resources (the data and technology) and capabilities (permission to share).

BIR explicitly mentions that exchange of data must be controlled. Since BIR is mainly concerned with information security, it sees this as a risk, instead of an opportunity. COBIT states that organisations must identify the major IT resources to be leveraged, of which information is part. This indicates that high data sharing possibilities can also be seen as a major IT resource that can be leveraged as an opportunity. Other standards also incorporate an investigation of resources and capabilities, but overall, we argue that the standards mainly involve those within the own organisational boundaries.

In public organisations, resources and capabilities must be included that pertain to external parties, which means the own organisational boundaries are crossed. There is room for investigating this in the current standards, but we stress that increased attention should be given to this to be fully certain of the potential opportunities. Therefore, we stress that a more external focus should be added to this category in the standards.

6.1.5 Uniqueness of Tasks & Position

This category pertains to the tasks and position that public organisations have, which mostly indicates that these organisations are one-of-a-kind. The activities and powers of an organisation can greatly determine the degree of controlling ability, which for public organisations has a positive effect.

The investigation of the unique tasks and position that can be assigned to a public organisation, seems a pretty logical step in the design of a control process. With ITIL, specific tasks could be translated to services. This way, unique elements of a public organisation its tasks can be properly dealt with. The other standards also include attention for tasks, processes or operations, and we argue that unique tasks can therefore sufficiently be addressed by the current standards.

With unique position, this is a bit different. As with the previous category, the standards lack a sufficient external focus, which causes that the possibilities with a unique position might be overlooked when designing a control process. This might have a direct effect on how automated IT controls will be used. Therefore, the possible unique position of a public organisation should be incorporated in the standards.

This means that a guideline will not have to mention unique tasks; only the unique position.

6.2 Guidelines for filling ‘gaps’

Since we identified some ‘gaps’ in the previous section, we argue that these must be filled. This concerns specific public sector Goals & Values, a lacking external focus with respect to Resources & Capabilities, and insufficient focus on unique positions of public organisations.

The comments from the previous sections are therefore translated in guidelines for the development of automated IT controls in control processes for external fraud prevention. These guidelines can tailor

current standards that for usage in the public sector for that purpose. Constraints to this research cause that we can only state very high-level guidelines. Guidelines that state in more detail how actual solutions for the 'gaps' can be found, must be developed in further research. In this research, we limit ourselves to statements about the identification of the 'gaps' and that these must be addressed.

As recommended earlier, specific public sector Goals & Values can influence the degree to which automated IT controls can be applied. During the investigation of solutions for risk mitigation, this should be addressed. Especially ethical and public values, which might even be (partly) defined in the law, should be investigated. These values can be applying for the public sector internationally, but also specifically for organisations under supervision of a certain Ministry, or even specific for one organisation. Therefore, the following guideline should be added:

> *Specific goals and values, especially public and ethical ones, from existing on an international-wide level to specific organisational ones, must be investigated to check if these influence the degree to which automated IT controls can be applied.*

Resources & Capabilities that exist outside the organisational boundaries, but can be used in the control process, deserve more attention. Without a complete image of this, possibilities for improved controlling with automated IT controls might be missed. An expansion of the focus is therefore important. This leads to the following guideline:

> *External resources, and corresponding capabilities to use them, must be investigated to identify the maximum level of control, and the degree to which automated IT controls can make use of them.*

The Uniqueness of Tasks & Position of public sector organisations can determine how far the powers for controlling that are assigned to that organisation reach. This position therefore influences not only how much can be controlled, but also how much can be controlled automatically. An expansion of the focus is necessary because of that, and the following guideline addresses this:

> *The unique position of an organisation compared to the external parties in its network, including the powers that are assigned to it, must be investigated to identify how far it can take its control processes, and how extensive automated IT controls can be applied in them.*

These three guidelines should be incorporated in standards when developing automated IT controls for external fraud prevention in the public sector. By using them, both constraints and opportunities of automated IT controls are better addressed. This also assists in identifying the degree to which automated IT controls can be used.

Part IV

Part IV presents the final remarks in this thesis about the research that was performed. First, we pose recommendations about automated external fraud prevention, based on all the findings from previous chapters. Then, a discussion is presented on the findings of this research. After that, we discuss some general limitations of this research that were not yet discussed in previous sections. For reasons of completeness, a summary of previously mentioned limitations is also provided. Suggestions for further research are subsequently discussed.

Finally, we present the general conclusions of this thesis. A summary of the activities and findings is presented, together with the eventual outcomes of this research. This summarises the research problem and research questions, the way they were answered, and what the outcomes and their relevance are.

7 Recommendations

We now discuss recommendations about using automated IT controls for external fraud prevention, and about automated external fraud prevention in the public sector in general.

We start with the initial problem of using the internal focused concept of IT controls, part of internal control, for external fraud prevention in the public sector. We aimed to propose possibilities for using automated IT controls for this, while this is currently not seen as the most useful solution to identify and prevent external fraud in the public sector. The predominant thought is that it should mainly be used for the original concept of internal control of IT systems, and not to check on, for example, legitimacy of requests for public resources. Although the experts that were interviewed were unanimously in stating that it cannot be used to completely prevent external fraud, the potential to use automated IT controls for increased automation of control processes and early detection of the risks of external fraud, were acknowledged.

It can thus be helpful to broaden the scope of IT controls from a mainly internal focus, to also include a more external focus regarding external fraud prevention. Therefore, we recommend that a good investigation is performed within public organisations to examine how the originally internal concept of automated IT controls can be focussed more externally to improve the external fraud prevention activities of such organisations.

However, as we observed before, the actual applicability of automated IT controls for external fraud prevention is very dependent on certain factors. When automated IT controls are aimed to be developed with such an external focus, we strongly recommend that the influential categories of public sector characteristics are taken into account. In addition, the newly observed category of Failing Technology/Manual Necessity is also an important one to consider.

What already became clear from the previous section, is that the standards that are currently used for developing automated IT controls do not need to be changed drastically. Some categories of influential public sector characteristics can already be taken into account when these standards are used, but we still had to design three guidelines to assure that all influential factors are investigated. We recommend that these guidelines are added to such standards for developing automated IT controls for external fraud prevention. The advantage of doing this, is that proven methods for developing automated IT controls are still used, while being tailored for some specific public sector characteristics.

We now question ourselves: what are the consequences in practice? Although the previous statements about applying automated IT controls for external fraud prevention may have sound quite positive, it is not expected that they can be used as the main solution in practice. Despite their potential to increase automation of control processes, current constraining factors seem too strong. Some of the most dominant influential factors that were mentioned in section 5.4.1, are the main reason for this. They cause that it is very hard to fully control on legitimacy in an automated way, while preserving the reliability of current control processes. We will now discuss the four most constraining factors: 1) the public value of carefulness, 2) the inability to extract data automatically, 3) the inability to create reliable risk profiles, and 4) the necessity of a ‘human’ eye in control processes.

As mentioned earlier in this thesis, a popular political views is that the public value of carefulness needs manual intervention in control processes, which limits the possibilities for automated controlling. Moreover, it causes that not a single control process related to real-life consequences will be made fully automated. Only two scenarios can change this: 1) the political view, together with its definition in law, suddenly changes, or 2) automated controlling becomes (almost) even careful as human judgements. Since we do not want to engage in a discussion about how a public value must be politically perceived, we focus on the latter. Before that scenario becomes realistic, the next three important constraining factors must first be addressed.

The inability to extract data automatically is caused by external parties that are not properly organised to be a data supplier, and by a reluctance to actually share data rapidly. This indicates that there are structural issues and cultural issues within public organisations. We recommend that these must be resolved in order to increase the ability of applying automated IT controls, but also for automated external fraud prevention in general. Clearly, knowledge about information requirements of different public organisations can be used to steer which organisations must be properly structured. Next to this, clear agreements on instantly sharing data with other parties, together with culture changes, must be made to realise the official possibilities of high data sharing between public organisations. Additional research must be performed to study appropriate solutions for this in more detail.

The inability to create reliable risk profiles is quite a technical constraint. This inability can be caused by the absence of enough diverse data from which fraudulent patterns should be recognised, or more importantly, by the inability to create a profile that reliably grasps the patterns of fraudulent activities solely from data. If it is not possible to design a risk profile to which automated IT controls, or even other IT solutions in general, can reliably assign when someone is a fraudster, it cannot be used as a solution for controlling automatically. Some of the experts that were interviewed, also indicated that they struggle with designing an appropriate risk profile because of that second constraint. Automated external fraud prevention cannot be applied because of that. There already is an ongoing development in the Dutch public sector to increasingly assess the possibilities of risk profiles, but we argue that more attention is necessary for how it can be used in an automated way. Therefore, we recommend that increased attention must be given for determining how risk profiles can be designed for automated controlling in the public sector, and when someone can be marked as a fraudster in the first place.

The observed necessity of a ‘human eye’ in control processes is partly concerned with having the knowledge of extraordinary circumstances and correctly interpreting specific relations between data, in which intellect and experience play a critical role. In control processes that demand such criteria, having a human being in place can be much more effective and efficient compared to IT. It is unfeasible to take the effort and resources to make appropriate IT solutions for such processes, if it is even possible in the first place. Of course, technology evolves and costs are lowered, which makes it always interesting to search for the outer boundaries of the possibilities. However, in the foreseeable future, automated IT solutions cannot replace it, and a ‘human eye’ remains necessary. When determining the degree to which control processes can be automated, we recommend that these limitations of IT should be considered.

Especially these four factors cause that automated IT controls cannot be used to fully automate external fraud prevention; public organisations might only use to them to automate some manual checks, for which current knowledge is already available in practice. We therefore argue that the results are not convincingly enough for KPMG to extend their current practices of advising about internal controls or auditing them, with a special approach for tackling external fraud in public sector organisations with automated IT controls. A possible extended role for an external auditor like KPMG that we introduced, does also not seem realistic due to the same reasons.

We recommend that KPMG should first focus on other IT solutions that might be more suitable to counter external fraud, although those will also not fully automate it. As mentioned before, we also argue that when other IT solutions are considered, some of the influential factors that were identified in this research might also hold for the applicability of other IT solutions. Of course, more research is necessary to be fully certain of this. However, we recommend that KPMG includes these observed influential factors when auditing or advising about other IT solutions for external fraud prevention.

Since we found that automated IT controls will not become the main solution, we now discuss one of the other potential IT solutions for increasingly automating external fraud prevention. We learned from the interviews with experts that the solution with the greatest potential is extensive data analysing, with the use of predefined risk profiles, although designing such a risk profile can be hard. The related concept of CA/CM, which we mentioned before, could be further studied for use in the public sector.

The potential of extensive data analyses solutions are increasingly acknowledged, and implemented. In short, a large amount of data from large databanks is analysed periodically with a short time span, and cases with high fraud risks are filtered out by using a risk profile, which is based on statistics and mathematical models. After that, these detected high risk cases are investigated in more detail. Despite the current developments in data analysis, its limits will be reached when risk profiles cannot reliably judge about fraudulent activities in an automated way, and this forces that the possibilities of this solution will also, at some point, be brought to a halt.

Nevertheless, KPMG can assist public organisations in applying data analysis solutions, since knowledge about data analysis solutions is already in-house. However, this knowledge mainly concerns application in private sector organisations, and applying it in public organisations for specific external fraud cases could be quite different. In addition, we recommend that the effectiveness of increasingly using automated data analysing should be explored for external fraud prevention in the public sector.

When looking at the future, we argue that when some of the constraining influential factors that were discussed are taken away, a greater role for automated IT controls is likely. The influence that public sector characteristics now have on the applicability of automated IT controls, might definitely change over time. The past decades, we have seen a development in which governments are able to increasingly couple databanks and have the ability to collect much information about citizens for controlling purposes. If this development continues, some of the constraining factors might actually be taken away. We recommend that this development must be monitored, since it might cause that eventually, the possibilities of automated IT controls for external fraud prevention have sufficiently

increased that an extended IT auditing approach for a external auditor like KPMG becomes reality. We have to conclude that this is just a futuristic possibility and that it is not the case at the moment.

To summarise this chapter, our main recommendations are the following:

- Although it will not become the main solution, public organisations should investigate the potential of using automated IT controls for increasingly automating external fraud prevention, while the (public sector) characteristics that influence their applicability must be taken into account.
- When public organisations use standards (e.g. COSO, COBIT, ITIL) for developing automated IT controls for external fraud prevention, the designed guidelines from this research should be included to assure that all influential public sector characteristics are investigated.
- KPMG does not need to extend current practices with a special approach for using automated IT controls for external fraud prevention, since it will not become the main solution for this. Moreover, fully automated external fraud prevention in general is not realistic in the foreseeable future.
- KPMG can advise public organisations about using other IT solutions for increasingly automating external fraud prevention, but should already take into account the influential characteristics found in this research, of which the following four are the most constraining factors:
    - The public value of carefulness
    - The inability to extract data automatically
    - The inability to create reliable risk profiles
    - The necessity of a 'human' eye in control processes

8 Discussion

This section describes a discussion about this research, its limitations, and the recommendations for further research.

8.1 Research discussion

We first discuss how we must judge the contributions of this research. We question ourselves: what did we discover, how can the discoveries be explained, and why are they relevant to theory and practice? The two main contributions that we make, are directly related to the two research goals in section 1.3. Two research questions in particular were devoted to these goals, which are the fourth sub research question (Q4) and the main research question (MQ) presented in section 1.4. Next to this, we summarised current knowledge on how automated IT controls can be developed from a Risk Management approach, and what specific public sector characteristics are. We also presented recommendations about automated external fraud prevention in general.

The first main contribution is related to the fourth sub research question:

> *Which and in which way do public sector characteristics influence the applicability of automated IT controls for external fraud prevention?*

Our findings show that five categories of public sector characteristics influence the applicability of automated IT controls for external fraud prevention. Also, a sixth category was found that could not yet be assigned to a sector. What does this mean? We already stated what positive and negative effects mean in section 5.32. It is important to realise the existence of these effects, since they determine how well automated IT controls can be used for the continuous and extensive problem of external fraud for public sector organisations.

These effects might possibly be already known by some experts in practice, but this research provides the first scientifically based evidence for it. This evidence strengthens the view of several scholars that proposed that the public and private sectors are fundamentally different, of which Allison [3] is an example. With respect to the fields of research, this adds new insights to public management research regarding the influence of public sector characteristics, and also research pertaining to internal control of IT.

Not only is a knowledge gap in the research field filled by these findings, public sector organisations also profit from the findings when they aim to find an appropriate IT solution for preventing external fraud. Now the effects of public sector characteristics on the applicability of automated IT controls are known, public organisations can better assess if such controls are an option. With respect to this, the scenarios that were proposed were also relevant for these organisations, and also assisted in the discovery of the influential characteristics and possibilities for automated controlling in general. We argued that automated IT controls have potential to increasingly automate control processes, but that it will not become the main solution in the foreseeable future. The four most constraining influential factors that cause this were subsequently discussed, and the corresponding recommendations assist in pointing out

the main reasons that could cause that (fully) automated external fraud prevention is not applicable in public organisations.

In addition, the findings have direct practical relevance for KPMG. The previously mentioned effects are known and some possibilities for automated IT controls were studied simultaneously. Based on that, KPMG can assess what essential factors are in auditing on, or advising about automated IT controls for external fraud prevention, and perhaps even automated external fraud prevention in general. Maybe more importantly, the necessity for potential extended auditing and advising roles became clear, of which we conclude that it is low under current circumstances.

The second main contribution is related to the main research question:

> *How must current standards for developing automated IT controls be tailored to include the effect of specific public sector characteristics on the applicability of such automated IT controls, for external fraud prevention in the public sector?*

Our findings show that three of the five influential categories are in general insufficiently addressed by current standards and frameworks that focus on developing internal control and automated IT controls, and we therefore designed guidelines to tailor them. What does this mean? When public organisations apply current standards and frameworks, three influential categories of public sector characteristics might be overlooked when developing internal controls, of which automated IT controls can be part. Since the influential categories have an influence on the applicability of automated IT controls, it is necessary to involve these categories in the early development phase of such internal controls. It is therefore recommended that the corresponding three guidelines that were designed are added to such current standards and frameworks for use in the public sector. This must ensure that public organisations cannot overlook these important issues in the developmental phase of controls for external fraud prevention, which is the most important contribution here.

The added value of these findings to theory is mainly the strengthening of the view that it is doubtful whether private sector management can easily be transported to the public sector, due to differences between them, as described by Kickert [42]. Our findings indicate that standards and frameworks that mainly focus on the private sector, need to be tailored to be used for external fraud prevention in the public sector. Implicitly, this research calls for additional studies that focus on the potential need for tailoring IT standards due to specific public sector characteristics. This is related to the findings of Sethibe et al. [71] that a ‘one-size-fits-all’ approach for IT governance is not appropriate for both sectors.

The practical relevance is also significant, since public sector organisations that apply such internal control or IT control standards can use the designed guidelines in practice. This helps them in doing a complete investigation of all important influential factors for developing appropriate automated IT controls for external fraud prevention.

To a lesser extent, KPMG could use the guidelines when advising or auditing on automated IT controls in the public sector, in case of external fraud prevention. However, we previously discussed that it is not likely that automated IT controls become a main solution for external fraud prevention, which means

that an extended role of an IT auditor that can use the guidelines, is not realistic in the foreseeable future.

8.2 Limitations

There are several limitations to this research that influenced the impact of the results. Some limitations were already discussed in previous sections, and these will only be shortly summarised subsequently.

First, there were some limitations due to constraints to the size and available time for this research. Only a part of a design science research process could be performed for designing the guidelines in this research, and these constraints also cause that the designed guidelines are very high-level, and mainly pertain to the identified 'gaps'. Demonstration, evaluation and communication of the guidelines was not performed. Also, concepts and tools related to automated IT controls could not be further studied.

Secondly, there were some limitations to the literature review. The limited access to resources is one of them, which caused that a number of potential references might be missed. Next to that, the quality and impact scores of the references could possibly be higher, and the chance of outdated information is significant since many old references were found. Also, most references pertain research applied to a limited number of countries, which mostly concerns traditional developed countries such as the US and the UK. A more diverse sample could be possible. Furthermore, no evidence from the literature was used when discarding ten of the found characteristics in the discussion of the search results from the literature review. Logic reasoning was used there, which is weaker compared to evidence from literature. Also, a category of public sector characteristics might be more representative if it accounted for a larger number of characteristics. Some categories only represent a small number of characteristics.

Thirdly, there were some limitations to the case study. Most importantly, the size of the sample of the case study was limited, which was partly caused by the absence of willingness of some organisations, but also due to the size and available time for this research. Although different cases were studied, the four selected organisations showed some similarities, which further weakens the diversity of the sample. A larger and more diversified sample could greatly improve both the evidence for the results, and their generalisability to public sectors in other countries. Some of the categories of public sector characteristics that showed to have a significant effect, were supported by only one strong corresponding characteristic from that category, but we neglected this for reasons of clarity.

8.3 Further research

Partly based on the previously sections, we now state recommendations for further research. Some suggestions were already previously made, but will be summarised here for reasons of completeness.

Clearly, further research can be done to gather more evidence for the results, by taking a larger and more diversified sample. The generalisability of the results must also be further studied, in order to be sure that the results can be generalised to public sectors in other countries. Especially if less constraining influential factors are apparent, this could enhance the possibilities for automated IT controls, and an extended role for an IT auditor or IT advisor. In addition, further research is necessary to determine if the results also hold for smaller public sector organisations and organisations in which

less specific control processes reside to counter external fraud, since these were not included in this research.

One of the six influential categories on the applicability of automated IT controls was not considered to be a specific category of public sector characteristics; this was Failing Technology/Manual Necessity. No evidence was found from the literature review that could indicate this is a category specific to the public sector, but neither can it be stated that it belongs to the private sector. Further research can be performed to assess if Failing Technology/Manual Necessity is specific to the public sector. If that would be the case, it could mean that an additional guideline must be added to the guidelines that were proposed in this research. We purposely state 'proposed' here, since we did not fully evaluate, demonstrate, and communicate the designed guidelines according to the design science research process discussed by Peffers et al [60]. Further research must be done to perform these phases for all the guidelines.

Furthermore, it is interesting to study the actual effectiveness of automated IT controls for external fraud prevention. We only looked at the effects that public sector characteristics have on the applicability of automated IT controls by using scenarios, but another step that has to be taken before such controls are considered appropriate, is to study if they effectively counter external fraud in practice. This includes the actual testing or implementation of automated IT controls in real-life control processes. In addition, it can be determined if controlling on external fraud in public organisations becomes more efficient by using such controls.

The related concepts and tools that were shortly discussed were not further studied. Further research can be performed to see if such related concepts and tools can be effectively used for external fraud prevention in the public sector. Other potential automated IT solutions that were not mentioned in this thesis could also be incorporated.

Further research can also be performed to study a larger number of standards and frameworks than we did in this research. Although we incorporated the most well-known standards and frameworks, others could be checked to see if the guidelines that we proposed are already addressed in them. If this would not be the case, then this strengthens our view that the guidelines should be generally applied in the public sector for the development of internal control or IT controls.

Also, it was recommended that further research is necessary to determine if the influential characteristics that were found also influences the applicability of other IT solutions, such as automated data analysing. These solutions might be more realistic options for external fraud prevention in the public sector, and it is therefore necessary to separately determine the factors that influence the applicability of such solutions.

9 Conclusions

Public sector organisations face external fraud problems regularly. Both citizens and organisations try to gain advantages through unlawful ways, and this still causes a lot of damage to both governments and societies. This thesis provides a first study of automatically tackling these problems in advance by using automated IT controls. However, control processes for preventing external fraud are quite complicated in the public sector, and this could be caused by specific public sector characteristics. Such characteristics might also influence the ability to apply automated controlling on external fraud, but research about this was lacking. Therefore, we studied which specific public sector characteristics influence the applicability of automated IT controls, and in which way they do so. In addition, we studied if current standards and frameworks for developing automated IT controls needed tailoring to incorporate these influences, since many of the standards and frameworks focus on the private sector.

In order to come up with the answers, we made a theoretical background from literature and conducted interviews in a case study. Six influential categories were found from this, of which five categories pertain to specific public sector characteristics, and one category that could not yet be assigned to a sector. This thesis thus adds an understanding of the factors that influence if public organisations can apply automated IT controls for external fraud prevention.

When looking more closely at these results, the influential categories are represented by a limited number of dominant characteristics. Especially the dominant constraining characteristics were interesting to consider, since they limit the ability to apply automated IT controls for external fraud prevention, and we assume this also holds for automated external fraud prevention in general. The four most constraining characteristics are:

- The public value of carefulness
- The inability to extract data automatically
- The inability to create reliable risk profiles
- The necessity of a ‘human’ eye in control processes

After that, we investigated current standards and frameworks, and designed three guidelines to tailor such standards and frameworks in general for incorporating the influential categories of public sector characteristics. The ‘gaps’ that were identified in a selection of standards and frameworks, and for which we designed high-level guidelines, are pertaining to:

- Specific goals and values, especially public and ethical ones
- External resources, and the capabilities to use them
- Unique position (and included powers) of an organisation compared to external parties in its network

Finally, we discussed the issues that relate to the most dominant characteristics in more detail and it must be concluded that these are very hard if not impossible to resolve in the foreseeable future. Fully automated external fraud prevention does not seem realistic because of that, and we pose that automated IT controls can only be used to partly automate simple checks in control processes. Other IT

solutions might be more suitable to increasingly automate current control processes, of which data analysis solutions are perceived to have the greatest potential, which was also the opinion of the four interviewed experts from Dutch public organisations.

Based on the findings in this research, we expect that public organisations will not be directly moved to increasingly apply automated IT controls in their control processes. Furthermore, organisations like KPMG are not expected to currently give special attention for an extended role as an IT auditor or IT advisor in this context. These statements must also be seen as results of this thesis, but what did we further add?

This thesis also makes the following main contributions. Unique scientifically based evidence is found that shows that specific public sector characteristics actually have an influence in practice on how an IT solution, with a focus on automated IT controls, can be applied for external fraud prevention. In practice, public organisations and KPMG can use this knowledge to assess which essential characteristics cannot be overlooked when determining if automated controls are an appropriate solution. When using current standards and frameworks in the developmental process, this thesis adds guidelines that tailor these standards and frameworks to be certain of the inclusion of these essential characteristics. Furthermore, regarding to the topic of public management in literature, this thesis adds evidence to the view that private sector standards cannot be simply transferred for usage in the public sector.

Further research is necessary for, among others, providing more evidence about the results, and to gain more certainty about the actual effectiveness of automated IT controls for external fraud prevention in the public sector.

This thesis aimed to help public organisations in their everlasting battle against external fraud. It is a first attempt to see automated IT controls as the main weapon for this. Simultaneously, the characteristics of the public sector that are helping or constraining the application of this weapon are now known, and we argued that these also hold for other IT solutions. Guidelines were designed that assure that when such weapons are developed, such characteristics are not overlooked. However, there are still concerns for fully relying on automated IT controls as the main weapon, which prevents that it is currently considered as a real ‘game-changer’ in the battle. Nevertheless, an increased understanding is created about applying this weapon, and future developments may cause that this thesis paved the way for winning the battle against external fraud with automated IT controls as the main weapon. For now, public organisations should still consider a broad arsenal.

References

[1] Ahuja, M., Kuhn, R., & Mueller, J. M. (2012). IT Control Weakness and Company Financial Health. *Social Science Research Network.* Available at: http://dx.doi.org/10.2139/ssrn.1304125.

[2] Alford, J. (1993). Towards a new public management model: beyond "managerialism" and its critics. *Australian Journal of Public Administration*, *52*(2), 135-148.

[3] Allison, G. T. (1980). *Public and private management: are they fundamentally alike in all unimportant respects?* (pp. 283-298). John F. Kennedy School of Government, Harvard University.

[4] Al Omari, L., Barnes, P. H., & Pitman, G. (2012). Optimising COBIT 5 for IT governance: examples from the public sector. *Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information Systems Research (2nd. ATISR2012)*. Academy of Taiwan Information Systems Research.

[5] Andersen, K. V. (1999). Reengineering public sector organisations using information technology. *Reinventing government in the information age: International practice in IT-enabled public sector reform*, *1*, 312.

[6] Antonsen, M., & Jørgensen, T. B. (1997). The 'publicness' of public organizations. *Public Administration*, *75*(2), 337-357.

[7] Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659-675.

[8] Australian Institute of Criminology. (2011). *Fraud against the Commonwealth 2008-09 annual report to government.* Retrieved from: http://www.aic.gov.au/publications/current%20series/mr/1-20/14.html.

[9] Barateiro, J., & Borbinha, J. (2011). Integrated management of risk information. *Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on* (pp. 791-798). IEEE.

[10] BBC News Scotland. (2012). *Fraud investigation uncovers £20m public sector fraud and error.* Retrieved from: http://www.bbc.com/news/uk-scotland-18271810. Accessed at: 28-4-2014.

[11] Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: an empirical validation of risk-option relationships. *MIS quarterly*, *30(4),* 827-864.

[12] Biondi, Y. (2012). Should Business and Non-Business Accounting be Different? A Comparative Perspective Applied to the French Central Government Accounting Standards. *International Journal of Public Administration*, *35*(9), 603-619.

[13] Boyne, G. A. (2002). Public and private management: what's the difference?. *Journal of management studies*, *39*(1), 97-122.

[14] Boyne, G. A., Poole, M., & Jenkins, G. (1999). Human resource management in the public and private sectors: an empirical comparison. *Public Administration*, *77*(2), 407-420.

[15] Bozeman, B., & Bretschneider, S. (1986). Public management information systems: Theory and prescription. *Public Administration Review*, *46(Special issue),* 475-487.

[16] Bozeman, B., & Bretschneider, S. (1994). The "publicness puzzle" in organization theory: A test of alternative explanations of differences between public and private organizations. *Journal of public administration research and theory*, *4*(2), 197-224.

[17] Bozeman, B., & Kingsley, G. (1998). Risk culture in public and private organizations. *Public Administration Review, 58(2)*, 109-118.
[18] Bretschneider, S. (1990). Management information systems in public and private organizations: An empirical test. *Public Administration Review*, *50*(5), 536-545.
[19] Brook, D. A. (2002). Administrative Reform in the Federal Government: Understanding the Search for Private Sector Management Models - An Annotated Bibliography. *Public Administration and Management: An Interactive Journal* 7.2.
[20] Careja, R. (2011). Paths to Policy Coherence to Create Market Economies in Central and Eastern Europe. *International Political Science Review, 32*(3), 345-366.
[21] Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key information systems management issues for the public sector. *MIS quarterly, 15(2)*, 171-188.
[22] Chandler, J. A. (1991). Public administration and private management. Is there a difference?. *Public Administration*, *69*(3), 385-391.
[23] Charette, R. N. (1996). The mechanics of managing IT risk. *Journal of Information Technology*, *11*(4), 373-378.
[24] Cong, X., & Pandya, K. V. (2003). Issues of knowledge management in the public sector. *Electronic Journal of Knowledge Management*, *1*(2), 25-33.
[25] COSO. (2013). *Internal Control – Integrated Framework: Executive Summary*. Committee of Sponsoring Organizations of the Treadway Commission. Retrieved from: http://www.coso.org/ic.htm.
[26] De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307-324.
[27] Elpez, I., & Fink, D. (2006). Information Systems Success in the Public Sector: Stakeholders' Perspectives and Emerging Alignment Model. *Issues in Informing Science & Information Technology*, *3*.
[28] Flowerday, S., & Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers & Security*, *24*(8), 604-613.
[29] Gold, K. A. (1982). Managing for success: A comparison of the private and public sectors. *Public Administration Review, 42(6)*, 568-575.
[30] Gowans Miller, A., (2010). The Maturity of GRC in the Public Sector. *AGA CPAG Research Series, Report No. 26, September 2010.*
[31] Gray, A., & Jenkins, B. (1995). From public administration to public management: reassessing a revolution?. *Public administration*, *73*(1), 75-99.
[32] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75-105.
[33] Hubbard, D. W. (2009). *The failure of risk management: why it's broken and how to fix it*. John Wiley and Sons.
[34] INTOSAI. (2004). *INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector.* Retrieved from: http://www.intosai.org/issai-executive-summaries/view/article/intosai-gov-9100-guidelines-for-internal-control-standards-for-the-public-sector.html.

[35] ISACA. (2012). *COBIT 5 Executive Summary.* Retrieved from: http://www.isaca.org/cobit/pages/default.aspx. Accessed at: 2-6-2014.
[36] ISO. (2009). *ISO31000 Risk Management – Principles and guidelines.* International Organization for Standardization.
[37] ITGI. (2006). *CobiT Mapping: Overview of International IT Guidance, 2nd Edition.* IT Governance Institute, United States of America.
[38] Jackson, P. M. (2013). Debate: Fraud risk management in the public sector. *Public Money & Management*, *33*(1), 6-8.
[39] Jans, M., Lybaert, N., & Vanhoof, K. (2010). A framework for internal fraud risk reduction at IT integrating business processes: the IFR² framework. *The International journal of digital accounting research*, *9*, 7.
[40] Jørgensen, T. B., Hansen, H. F., Antonsen, M., & Melander, P. (1998). Public organizations, multiple constituencies, and governance. *Public Administration*, *76*(3), 499-518.
[41] Julisch, K., Suter, C., Woitalla, T., & Zimmermann, O. (2011). Compliance by design – Bridging the chasm between auditors and IT architects. *Computers & Security*, *30*(6), 410-426.
[42] Kickert, W. J. (1997). Public Governance in the Netherlands: An Alternative to Anglo-American 'Managerialism'. *Public administration*, *75*(4), 731-752.
[43] Knott, J. H. (1993). Comparing public and private management: Cooperative effort and principal-agent relationships. *Journal of Public Administration Research and Theory*, *3*(1), 93-119.
[44] KPMG. (2012). *Continuous auditing and continuous monitoring: The current status and the road ahead.* Retrieved from: http://www.kpmg.com/nl/nl/issuesandinsights/articlespublications/pages/continuous-auditing-and-continuous-monitoring-2012.aspx.
[45] KPMG (2013). *A survey of fraud, bribery and corruption in Australia & New Zealand 2012.* Retrieved from: http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/fraud-bribery-corruption-survey-2012.aspx.
[46] Lachman, R. (1985). Public and private sector differences: CEOs' perceptions of their role environments. *Academy of Management Journal*, *28*(3), 671-680.
[47] Lan, Z., & Rainey, H. G. (1992). Goals, rules, and effectiveness in public, private, and hybrid organizations: More evidence on frequent assertions about differences. *Journal of Public Administration Research and Theory*, *2*(1), 5-28.
[48] Levaggi, R. (2007). Tax evasion and the cost of public sector activities. *Public Finance Review*, *35*(5), 572-585.
[49] Liu, Q., & Ridley, G. (2005). IT Control in the Australian public sector: an international comparison. *Proceedings of the 13th European Conference of Information Systems*.
[50] Lynn, L. E., Heinrich, C. J., & Hill, C. J. (2000). Studying governance and public management: Challenges and prospects. *Journal of Public Administration Research and Theory*, *10*(2), 233-262.
[51] Maarse, N., & Janssen, M. (2012). The need to adjust lean to the public sector. *Electronic Government* (pp. 54-65). Springer Berlin Heidelberg.
[52] Meier, K. J., & O'Toole, L. J. (2011). Comparing public and private management: theoretical expectations. *Journal of Public Administration Research and Theory*, *21*(suppl. 3), i283-i299.

[53] Mensink, M. (2011). *Risicomanagement: risicomanagement en risk maturity in de praktijk.* Bachelor of Science thesis at the Faculty of Management and Governance, University of Twente. Retrieved from: http://purl.utwente.nl/essays/61888.

[54] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2012). *Baseline Informatiebeveiliging Rijksdienst – Tactisch Normenkader (TNK).* Retrieved from: www.earonline.nl/images/ear/6/6f/BIR_TNK_1_0_definitief.pdf.

[55] Morales, F. N., Wittek, R., & Heyse, L. (2013). After the reform: Change in Dutch public and private organizations. *Journal of Public Administration Research and Theory*, *23*(3), 735-754.

[56] Murray, M. A. (1975). Comparing public and private management: An exploratory essay. *Public Administration Review, 35(4)*, 364-371.

[57] National Audit Office. (2008). *Tackling external fraud – Good practice guide.* Retrieved from: http://www.nao.org.uk/report/good-practice-in-tackling-external-fraud-2/.

[58] Oyemade, R. (2012). Effective IT Governance Through the Three Lines of Defense, Risk IT and COBIT. *ISACA Journal, 13(1),* p. 24-29.

[59] Parker, L., & Gould, G. (1999). Changing public sector accountability: critiquing new directions. *Accounting forum, 23(2),* pp. 109-135. Blackwell Publishers Ltd.

[60] Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). The design science research process: a model for producing and presenting information systems research. *Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006)* (pp. 83-106).

[61] Perry, J. L., & Rainey, H. G. (1988). The public-private distinction in organization theory: A critique and research strategy. *Academy of management review*, *13*(2), 182-201.

[62] Protiviti. (2013). *The Updated COSO Internal Control Framework – Frequently Asked Questions.* Second Edition. Retrieved from: http://www.protiviti.com/en-US/Pages/The-Updated-COSO-Internal-Control-Framework-FAQ.aspx.

[63] PWC (PriceWaterhouseCoopers). (2011). *Fighting fraud in the public sector: The government and public sector extract from PwC's Global Economic Crime Survey.* Retrieved from: https://www.pwc.com/en_GX/gx/psrc/pdf/fighting_fraud_in_the_public_sector_june2011.pdf.

[64] PWC (PriceWaterhouseCoopers) (2013). *Naar een fraudebeeld Nederland.* Retrieved from: http://www.pwc.nl/nl/publicaties/naar-een-fraudebeeld-van-nederland.jhtml.

[65] Racz, N., Weippl, E., & Seufert, A. (2010). A frame of reference for research of integrated governance, risk and compliance (GRC). *Communications and Multimedia Security* (pp. 106-117). Springer Berlin Heidelberg.

[66] Rainey, H. G. (1989). Public management: Recent research on the political context and managerial roles, structures, and behaviors. *Journal of Management*, *15*(2), 229-250.

[67] Rainey, H. G., Backoff, R. W., & Levine, C. H. (1976). Comparing public and private organizations. *Public Administration Review, 36(2)*, 233-244.

[68] Ring, P. S., & Perry, J. L. (1985). Strategic management in public and private organizations: Implications of distinctive contexts and constraints. *Academy of Management Review*, *10*(2), 276-286.

[69] Robertson, P. J., & Seneviratne, S. J. (1995). Outcomes of Planned Organizational Change in the Public Sector: A Meta-Analytic Comparison. *Public Administration Review*, *55*(6), 547-558.

[70] Romney, M. B., Steinbart, P. J. (2009). *Accounting information systems*, 11th ed. Upper Saddle River, NJ: Prentice Hall.
[71] Sethibe, T., Campbell, J., & McDonald, C. (2007). IT governance in public and private sector organisations: examining the differences and defining future research directions. *18th Australasian Conference on Information Systems* (pp. 833-843). Toowoomba.
[72] TSO. (2012). *An Introductory Overview of ITIL 2011.* Retrieved from: https://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf. Accessed at: 2-6-2014.
[73] Van der Wal, Z., De Graaf, G., & Lasthuizen, K. (2008). What's valued most? Similarities and differences between the organizational values of the public and private sector. *Public administration*, *86*(2), 465-482.
[74] Van Dyke, M. A. (2005). *Toward a theory of just communication: A case study of NATO, multinational public relations, and ethical management of international conflict*. Dissertation at the University of Maryland, College Park.
[75] Weekers, F. (2013). Maatregelen ter bestrijding van fraude met toeslagen. Den Haag: Ministerie van Financiën. Retrieved from: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/10/brief-met-maatregelen-ter-bestrijding-van-fraude-met-toeslagen.html.
[76] Wet bescherming persoonsgegevens (Wbp). (2000). Retrieved from: http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_01-07-2014.
[77] Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45-55.
[78] Yan, L. (2011). Public Human Resources Development and Management under the Background of Knowledge Economy. *Management and Service Science (MASS), 2011 International Conference on* (pp. 1-4). IEEE.

Appendix A Mapping of articles on public sector characteristics

Articles		Categories							
Author(s)	Year of publication	Environment	Goals & Values	Political control & Bureaucracy	Resources & Capabilities	Performance & Evaluation	HRM & Personnel	Organisation & Structure	Uniqueness of Tasks & Position
Alford [2]	1995	X	X	X	X				
Allison [3]	1980	X	X	X		X	X		X
Andersen [5]	1999	X		X					
Antonsen & Jørgensen [6]	1997		X					X	
Biondi [12]	2012				X				
Boyne [13]	2002	X	X			X	X	X	
Boyne et al. [14]	1999			X			X		
Bozeman & Bretschneider [15]	1986	X	X	X	X	X	X	X	
Bozeman & Bretschneider [16]	1994		X	X		X	X	X	
Bozeman & Kingsley [17]	1998			X			X		X
Bretschneider [18]	1990	X			X	X		X	
Brook [19]	2002	X	X		X	X	X	X	X
Careja [20]	2011			X					
Caudle et al. [21]	1991	X	X	X	X	X	X		
Chandler [22]	1991	X	X	X					X
Cong & Pandya [24]	2003	X						X	X
Elpez & Fink [27]	2006	X	X	X	X				
Gold [29]	1982		X						
Gray & Jenkins [31]	1995	X	X	X					X
Jørgensen et al. [40]	1998	X	X	X				X	X
Kickert [42]	1997	X						X	
Knott [43]	1993	X	X	X		X	X	X	X
Lachman [46]	1985	X		X			X	X	X
Lan & Rainey [47]	1992		X						
Levaggi [48]	2007					X			
Lynn et al. [50]	2000			X				X	
Maarse & Janssen [51]	2012	X	X	X			X		
Meier & O'Toole [52]	2011	X				X	X		
Morales et al. [55]	2013			X	X	X		X	
Murray [56]	1975	X	X			X			
Parker & Gould [59]	1999	X		X					X
Perry & Rainey [61]	1988	X	X	X		X			
Rainey [66]	1989	X	X	X		X	X	X	X
Ring & Perry [68]	1985	X	X	X					
Robertson & Seneviratne [69]	1995			X					
Van der Wal [73]	2008		X						
Yan [78]	2011					X	X	X	

Appendix B Interview framework

Goals

The goals we want to achieve by performing interviews, are the following:

- To get an understanding of control processes on external fraud in public sector organisations;
- To discuss the possibilities of (increased) automation of such control processes by implementing automated IT controls;
- To find out which and in which way public sector characteristics influence the applicability of automated IT controls in such control processes.

In the end, the last goal is the most important one, since that corresponds with answering one of the sub research questions. If confidentiality is an issue, written explanations about how the first two goals were achieved do not have to be included in this thesis.

Organisations and interviewees

We perform interviews with employees of Dutch public sector organisations. More specifically, it concerns governmental agencies that deal with obvious risks of external fraud themselves or have the responsibility to control on external fraud that affects organisations or individuals in society.

The interviewees have a managerial role, which should prevent that we interview employees who potentially give biased answers because controlling on external fraud is part of their direct job description. Furthermore, the interviewees must have sufficient knowledge of certain control processes and related possibilities and limitations of IT within their organisation.

Methodology

We want to enhance as much information as possible from the interviewees, who will be interviewed for about one and a half hour. Therefore, much information about the organisation, and corresponding control processes and external fraud occurrences is searched and learned. In advance, the interviewees will only receive a general description of the research that is performed and specific suggestions pertaining to the control processes within their organisation that we like to discuss. We assume that the interviewees are aware of current developments of external fraud prevention and general opportunities of automated IT solutions.

During the interview, special attention is given to the interpretation of concepts. It is important that the same interpretation of concepts is handled, so there cannot be any confusion in the meaning of statements that are done. Therefore, concepts will be shortly discussed when they arise to establish a common understanding of them. The interviews will be done in the native language (Dutch) to further enhance this. Furthermore, we ask open questions and steer to open discussions, to prevent bias and to stimulate interviewees in coming up with appropriate and precise formulations of answers and descriptions.

We also give special attention to the fact that the interviewees might discuss characteristics that influence the applicability of automated IT controls only because they already influence the control process itself. In other words, such characteristics do not specifically limit the possibilities of controlling with automated IT controls, but they limit the actual possibilities of controlling in the first place. Therefore, we will clearly ask for which characteristics influence the applicability of automated IT controls, when the underlying principle of controlling itself is possible.

We take notes during the interviews, but we will also try to audio-record the interviews if permission is granted by the interviewee, since less necessary writing can lead to better quality of both interviewing and reporting. The recordings will be analysed and typed down accordingly.

Structure and questions

The following general elements are included in the interview, which also describes the interview structure:

1) Introduction (greeting, explaining the goals, content and points of attention of the interview)
2) Discussing specific control process on external fraud
3) Discussing possibilities of (increased) automated control through automated IT controls
4) Discussing ideal automated control process
5) Summary and closing

The characteristics that influence the applicability of automated IT controls will be asked when discussing the current automated control, the possibilities of more or completely automated control, and the ideal automated control process. This ensures that we do not only identify the characteristics that hold for current solutions, but also the ones that would be influential when potential automated improvements would be made.

The following questions are asked during the interview, presented in the actual spoken language:

Bespreken van rol en kennis van geïnterviewde

1. Wat zijn uw taken en verantwoordelijkheden m.b.t. interne controle?
2. Wat is uw kennis m.b.t. het toepassen van ICT binnen controleprocessen, en automated IT controls in het bijzonder?

Bespreken van een specifiek controleproces op externe fraude

3. Wat zijn de taken en verantwoordelijkheden van uw organisatie in dit controleproces?
4. Met wie werkt uw organisatie samen om de controle uit te kunnen voeren?
5. Welke andere (externe) partijen zijn er betrokken bij dit controleproces en welke belangen spelen hierbij?
6. Wat is de inrichting van het huidige controleproces?
    a) Wat wordt er gecontroleerd en met welk doel wordt dat gedaan?
    b) Welke stappen/fasen worden gevolgd?
    c) Door wie wordt gecontroleerd?

d) Welke middelen (gegevens e.d.) worden gebruikt?
e) Hoe vaak wordt er gecontroleerd?
f) Hoe is er zekerheid ingebouwd dat de controle correct en volledig uitgevoerd wordt? (worden er frameworks gebruikt?)

7. Wat zijn sterke punten van het huidige controleproces waardoor externe fraude voorkomen wordt?
8. Hoe zou er ondanks dit huidige controleproces nog externe fraude voor kunnen komen?
9. Wat is de geschatte omvang en impact van deze externe fraude?
10. Wat zijn de zwakke punten van het huidige controleproces waardoor deze externe fraude nog voor kan komen?

*** In geval van al toegepaste automatische controle m.b.v. automatische IT controls, doorgaan met 11. In geval van volledige automatische controle, na 11 vervolgens 14 t/m 18 overslaan. ***

*** In geval van beperkte automatische controle, door met 14.***

11. Op welke manier is er gestalte gegeven aan de huidige automatische IT controls?
    a) Gebaseerd op control frameworks? (COBIT, COSO, etc.)
    b) Gebaseerd op risicoanalyse? (Risk Management approach)
    c) Preventieve/Detectieve/Correctieve werking? En waarom?
    d) Welke soort controls zijn het belangrijkst voor externe fraude preventie?
    e) In hoeverre controleren automatische IT controls op legitimiteit?
12. Wordt er gebruik gemaakt van gerelateerde concepten in het huidige controleproces?
13. Welke factoren zijn van invloed op de toepasbaarheid van de huidige automatische IT controls?
    a) Welke factoren leggen beperkingen op, of creëren mogelijkheden, voor de toepassing van automatische IT controls in het controleproces?
    b) Welke specifieke eigenschappen van de publieke sector spelen hierbij een rol, en op welke manier doen zij dit? (eerst open, naderhand bespreken van de geïdentificeerde eigenschappen)

Bespreken van mogelijkheden van toenemende/volledige automatische controle

14. Op welke manier(en) zou het huidige controleproces meer/volledig geautomatiseerd kunnen worden m.b.v. automatische IT controls, waardoor de controle op externe fraude verbeterd wordt? (eerst open, naderhand worden ook voorstellen gedaan door de interviewer)
    a) Gebaseerd op risicoanalyse? (Risk Management approach)
    b) Preventieve/Detectieve/Correctieve werking? En waarom?
    c) Welke soort controls zijn het belangrijkst voor externe fraude preventie?
    d) In hoeverre kunnen automatische IT controls op legitimiteit controleren?
15. Kunnen control frameworks (of elementen daarvan) gebruikt worden om deze automatische IT controls te ontwikkelen?
16. Waarom maakt de organisatie nu of in de toekomst geen gebruik van deze manier(en)?

17. Welke factoren zijn van invloed op de toepasbaarheid van deze manier(en) van automatische controle d.m.v. automatische IT controls?
    a) Welke factoren leggen beperkingen op, of creëren mogelijkheden, voor de invoeging van automatische IT controls in het controleproces?
    b) Welke specifieke eigenschappen van de publieke sector spelen hierbij een rol, en op welke manier doen zij dit? (eerst open, naderhand bespreken van de geïdentificeerde eigenschappen)
18. Kunnen gerelateerde concepten gebruikt worden om het huidige controleproces te verbeteren?

Bespreken van ideale automatische controle

19. Hoe zou een automatisch controleproces m.b.v. automatische IT controls in een ideale situatie ingericht zijn zodat externe fraude tot een minimum beperkt zou worden? (eerst open, naderhand worden ook voorstellen gedaan door de interviewer)
    a) Gebaseerd op risicoanalyse? (Risk Management approach)
    b) Preventieve/Detectieve/Correctieve werking? En waarom?
    c) Welke soort controls zijn het belangrijkst voor externe fraude preventie?
    d) In hoeverre kunnen automatische IT controls op legitimiteit controleren?
20. Kunnen control frameworks (of elementen daarvan) gebruikt worden om deze automatische IT controls te ontwikkelen?
21. Waarom kan de organisatie dit ideale automatische controleproces niet bereiken?
22. Kunnen gerelateerde concepten gebruikt worden om dit ideale controleproces te bereiken?
23. Welke factoren zijn van invloed op de toepasbaarheid van automatische IT controls in dit ideale automatische controleproces?
    a) Welke factoren leggen beperkingen op, of creëren mogelijkheden, voor de invoeging van automatische IT controls in het controleproces?
    b) Welke specifieke eigenschappen van de publieke sector spelen hierbij een rol, en op welke manier doen zij dit? (eerst open, naderhand bespreken van de geïdentificeerde eigenschappen)
24. Kunnen gerelateerde concepten gebruikt worden om dit ideale controleproces te bereiken?

Appendix C Scenarios made upfront

The scenarios for potential improvements by automated IT controls that were made upfront for the interviews, are presented below. Only the cases that were actually discussed are included. These are presented in the native language of the interviewees (Dutch), as they were discussed during the interviews.

The purpose of using scenarios has been previously discussed. In short, the goal of these scenarios was to pose potential improvements by automated IT controls to the experts, and accordingly cause a discussion in which the possible influences of public sector characteristics on applying those controls, are revealed.

These scenarios consist of textual descriptions of how automated IT controls could possibly mitigate certain external fraud risks, and how an ideal control process could look like with the use of automated IT controls. We deliberately did not make detailed descriptions of individual IT controls. By starting with high-level scenarios, it is also more understandable for the experts, because we explain the underlying approach of a potential solution. From here on, it might be possible to discuss some controls in more detail if experts want to know more about their functionality, or in case certain controls are influenced by the effect of public sector characteristics.

We used publicly accessible sources to gain an understanding of the organisations in general, the control processes within them, and the current solutions that are used in control processes. Gained knowledge from the literature was used to assess the possibilities for automated IT controls in control processes. High-level scenarios could be developed accordingly.

Organisation A

<Confidential>

Organisation B

<Confidential>

Organisation C

<Confidential>

Organisation D

<Confidential>