A Method for Combining Agile, Internal Control, and Stakeholders' Needs

MSc Thesis Industrial Engineering and Management

University of Twente

Behavioural, Management and Social Sciences Faculty

Commissioned by Cape Groep B.V.

Name:	Jaro J. W. van der Beek
Student number:	s1502905
First supervisor:	Dr. Lucas O. Meertens
Second supervisor:	Dr. Adina I. Aldea
External supervisor:	Niek Staman
Publication date:	8 May 2020

UNIVERSITY OF TWENTE.

CAPE GROEP

Preface

After studying for almost seven years, the end of my student life is here. At the University of Twente I completed my Bachelor Industrial Engineering and Management, and continued my studies by following the Master Industrial Engineering and Management. In addition to the mandatory courses of my Master, I decided to follow some Business & IT courses. To conclude my master, I conducted this research and documented it in this thesis.

In my thesis I reflect upon a problem CAPE Groep faced. CAPE Groep is an interesting company as they combine knowledge about business and IT. CAPE Groep is not the only company within the target group; every company similar to CAPE Groep or fits within the scope of this research could use my approach.

I want to thank CAPE Groep for giving me the opportunity to perform my graduation assignment at their company. More specifically, I want to thank the employees who took the time to participate in my research. They gave me important insights about CAPE Groep and their thoughts about my solution. In particular, I want to thank Niek Staman, my external supervisor, who assisted me during this research. He always took the time to help me when I had questions or got stuck. For example, in the beginning of this graduation project, it was hard to find a suitable research that met the demands of CAPE Groep, the University of Twente, and myself. Niek made sure that with every change my research kept valuable for CAPE Groep, and thereby useful for many more similar companies.

To find a suitable research topic, my first supervisor Lucas Meertens had plenty of patience and new ideas that contributed both to the demands of the University and CAPE Groep. I want to thank him for this input and for all the input he gave me during our meetings. With his double role as Professor at the University of Twente and employee at CAPE Groep, he helped me satisfying both parties. I also want to thank Adina Aldea, my second supervisor of the University of Twente. She provided valuable feedback during our meetings and supported me in my graduation process.

Finally, I want to thank my parents, girlfriend, friends, and fellow students at CAPE Groep for their help and support.

Jaro van der Beek

Enschede, May 2020

Management summary

Businesses want to be Agile in a changing world, while they must comply with internal control measures and give insights and trust to their stakeholders. To regulate the combination of Agile, internal control, and stakeholders' needs, the framework designed in this research shows businesses how to deal with this combination.

The designed framework, based on relevant literature, can be found in Figure 15. This framework gives insights into the combination of different perspectives, namely all needs of the stakeholders within an Agile production process while complying with internal control measures.

The framework can be implemented at a company by executing the following steps. First, the necessities of the company, stakeholders' needs, and the internal control measures must be described. Next, the corresponding step of the Agile process, internal control category, and stakeholders must be defined. The third step is to determine the impact on the needs of the stakeholders. The final step is to decide whether the internal control measure must be implemented. This decision must also include the financial effects of this measure on the organisation. It is always important that an internal control measure solves a problem, improves a process, mitigate risks, fulfils a need of a stakeholder, etc.

The validation at CAPE Groep does not cover the whole framework due to limitations. The data control category is not involved in validation, only the most relevant stakeholders for this research are chosen for validation, and only a part of the process was chosen to focus on.

After the validation with the stakeholders it is concluded, that the framework is performing as expected. The expected main user of the framework, the Business Controller, recognizes that the framework achieves its goal. Namely, give Agile businesses insights in the procedures of internal control while they comply with the needs of their stakeholders. The Business Controller must ensure that at the least the Management Team and the Manager Information Security get those insights. Applying and understanding the framework will be hard for some other stakeholders. The level of abstractness of the framework is quite high.

As shown in the validation, the users of the framework classify it as useful. Therefore, CAPE Groep and companies similar to CAPE Groep are advised to implement the framework within their business.

List of figures

List of abbreviations

AQ: Additional questions
AQM: Application Quality Monitor
BI: Behavioural intention to use the framework
CIA: Confidentiality, Integrity, and Availability
CIS: CAPE Groep Information System
COSO: Committee of sponsoring organisation of the Treadway commission
DCB: Dutch Central Bank
DevOps: software development and IT operations
DoD: Definition of Done
DoR: Definition of Ready
DPP: Data Protection Directive
DSA: Dutch Supervisory Authority
DSRM: Design Science Research Methodology
DTA: Dutch Tax Agency
EE: Effort expectancy
ERM: Enterprise Risk Management
FC: Facilitating conditions
GDPR: General Data Protection Regulation
ISA: Information Systems Architecture
ISMS: Information Security Management System
ISO: International Organisation for Standardization
IT: Information Technology
MIS: Manager Information Security
PE: Performance expectancy
PO: Product Owner
SAFe: Scaled Agile Framework
SE: Self-efficacy
SLA: Service Level Agreement
SME: Small or Medium-sized Enterprises
SOC: Service Organization Control
SOX: Sarbanes-Oxley Act of 2002
VUCA: Volatility, Uncertainty, Complexity, and Ambiguity

Content

1. Research introduction

This chapter gives an introduction to this research. In section 1.1, the motivation for this research is given. The next section (1.2) is the research design which includes the methodology, the research problem and the research questions. Section 1.3 describes the reliability and validation of the research. The final section of chapter 1 (1.4) is about the scientific and practical relevance.

1.1 Rationale

The rationale of this research is that businesses want to be Agile in a changing world, while they must comply with internal control measures and give insight and trust to their stakeholders. This research is initiated by CAPE Groep. Therefore, the designed method will be tested at CAPE Groep. More information about the terms used above can be found in chapter 2 and chapter 5.

To regulate the combination of Agile, internal control (which includes security and privacy standards, and regulations), and stakeholders' needs, a method should be designed so businesses can deal with this combination. A possible method that can be used in this research is a theoretical framework. According to the BusinessDictionary (2019), a framework is a skeleton of interlinked items which supports a particular approach to a specific objective, and serves as a guide that can be modified as required by adding or deleting items. The description of the interlinked items fits in the idea of the solution where different perspectives of internal control, stakeholders needs, and Agile must be combined. The possibility to modify the solution by adding or deleting certain items, gives this solution the opportunity to be implemented in different situations and organisations. These two arguments determine that a framework is a suitable solution for this problem.

Causes and effects

The main causes of the problem can be divided into two different categories. Namely, internal control causes and Agile causes.

According to employees of CAPE Groep, the internal control causes start with getting and attracting more and bigger customers. Causing that more stakeholders must be pleased as more people are involved (Freeman, 2010). Another effect, which is concluded from the information of CAPE Groep, is that the company must comply with security and privacy standards to show reliability to these big customers. The third effect is that the company itself is growing. The company must comply with additional regulations and legislations that appear after exceeding certain criteria (Van Noort Gassler & Co., 2018; Maxius, 2019), and more employees are hired. Hiring more employees results in decreasing informal control. Key managers and employees can sit around the same table and informally explore the impact of emerging threats and opportunities as long as companies are small (Simons, 1995). However, Simons (1995) stated that as an organisation grows larger and senior managers have less and less personal contact with people throughout the organisation, formal control procedures must be created to share important information and to utilise the creativity of employees.

The Agile causes start with a changing world. The Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) that come with a changing world, cause that an approach is needed to stay in control, namely Agile (Thummadi, Shiv, & Lyytinen; 2011). About the combination of the internal control causes and Agile causes is little written. The desired situation prefers to keep these causes intact.

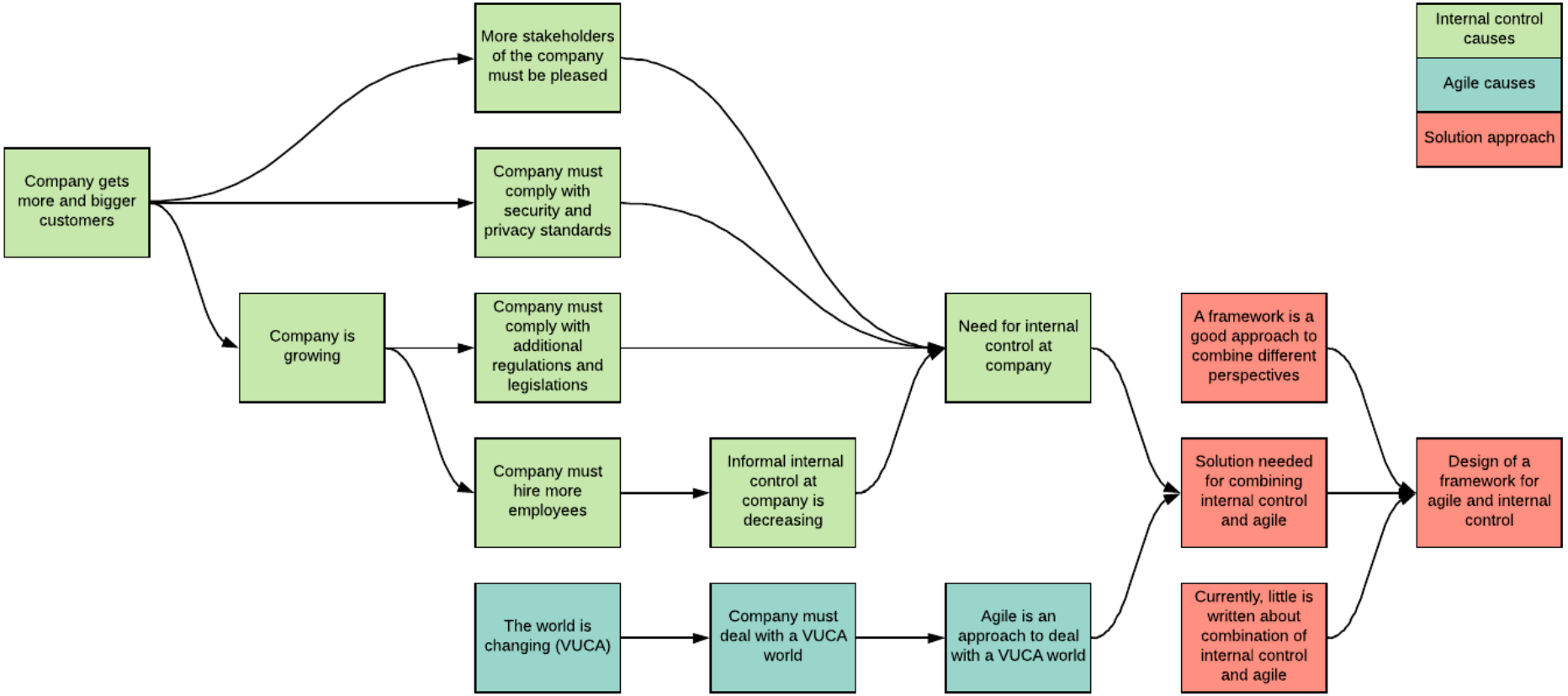


Figure 1: Preliminary cause-and-effect tree of the problem

Companies that ignore more and bigger customers, that ignore regulations and legislations, and that don't hire more employees will not expand their businesses. The key to a healthy growing company is to solve these problems. A framework about the combination of internal control causes, Agile and stakeholders' needs must be designed to show how this can be done. The corresponding preliminary cause-and-effect tree as described above is shown in Figure 1.

Scope

The scope of the research is IT consultancy businesses which can be described as Small or Medium-sized Enterprises (SME). These businesses should use Agile or must be willing to start. Besides, it must be a growing company by getting more and bigger customers. CAPE Groep fits these conditions and is therefore a representative company.

1.2 Research design

In this chapter the design of this research is discussed. First, the methodology used in this research is discussed, then the data collection is discussed, and finally the main research question and the research questions are discussed.

Methodology

The approach of the report is based on the Design Science Research Methodology (DSRM) (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007) which is shown in Figure 2. The methodology starts with the identification of the problems (including the cause-and-effect tree) and motivation of the research. From this point, the main question and research questions can be formulated. All of this together drives the whole problem-solving project. The next step is to define the objectives for a solution. This includes the description of a new framework and how this framework should support in resolving the problems. To gain knowledge, a literature study is conducted. The third step is the design and development of the framework. The framework's testing is executed in the next step, the demonstration. How problems of CAPE Groep are solved with this framework are also discussed in this section and the general implementation plan is included. The last section in this report is the evaluation. The evaluation of the implementation at CAPE Groep, and conclusions and recommendations about the framework are included in this section. The last part of the approach is the communication. This part is executed but not included in this report. The thesis is published online at the website of the University of Twente and a presentation is given, in which the communication part is completed.

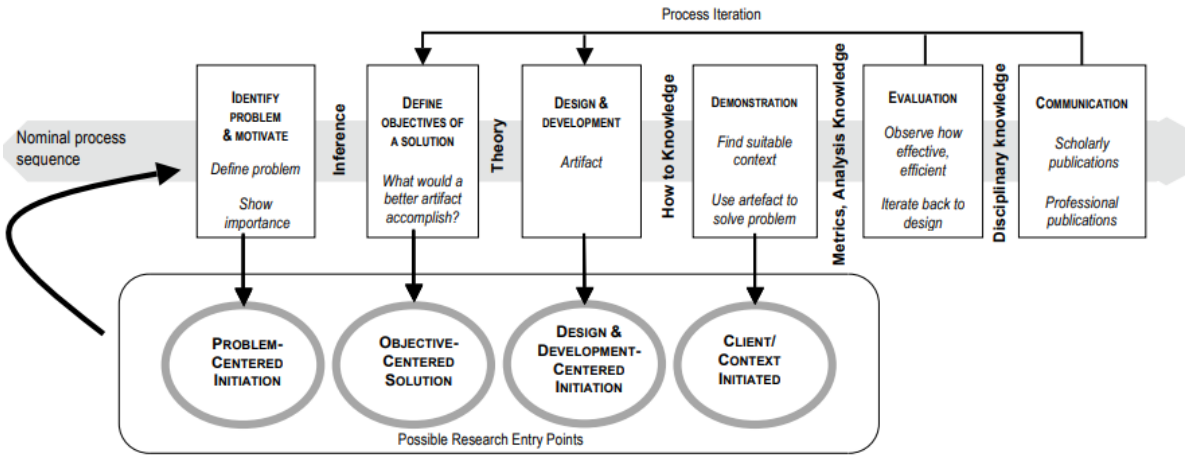


Figure 2: The Design Science Research Methodology (Peffers et al., 2007)

Table 1 shows the steps of the DSRM and the corresponding chapters within this report. The corresponding research questions, data collection methods and deliverables are also mentioned within this table. This table makes clear how the DSRM is linked to the layout of this research.

Table 1: Chapter layout (Peffers et al., 2007), with corresponding research questions, data collection methods, and deliverables

DSRM	Chapter	Research questions	Data collection method	Deliverable
Identify problem & motivate	1. Research introduction	-	Unstructured interviews	Introduction to the problem
Define objectives of a solution	2. Literature review	RQ 1-6	Desk research	Summary of relevant literature
Design & development	3. Design of the framework	RQ 7	-	Framework design
	4. General implementation plan	RQ 8	-	Implementation plan
Demonstration	5. Framework validation at CAPE Groep	RQ 9	Semi-structured and structured interviews	Validated framework
Evaluation	6. Validation	RQ 10	Semi-structured interviews	Evaluation and validation
	7. Conclusions	-	-	Conclusions and recommendations
Communication	-	-	-	Report and presentation

Data collection

In this paragraph an explanation of the methodology, which should help to find satisfactory answers for the research questions, is given. This methodology corresponds with the used approach of Peffers et al. (2007). The methodology is summarized in Table 1.

Literature review

Chapter 2 describes a collection of relevant literature for this research. The literature is collected by desk research. The desk research consisted of consulting reliable web pages, educational books, and journal articles retrieved from, among others, Scopus. This literature provides information about the different aspects of the designed framework. After the research questions of chapter 2 are answered sufficiently, the framework is designed.

Interviews

The second data collection method is interviewing CAPE Groep stakeholders. Three different kind of interviews can be distinguished, namely unstructured, structured, and semi-structured interviews (Hofisi, Hofisi, & Mago, 2014).

Unstructured interviews

Unstructured interviews are interviews where the interviewer has certain topics to discuss during the interview with no predetermined questions. This type of data collection is mainly used for the identification of problems. The unstructured interviews are also used for mapping the important processes of CAPE Groep for this research. Unstructured interviews can be used in both cases, because

the interviewees are experts in specific fields. According to Hofisi et al. (2014), the strength of unstructured interviews is that respondents will not leave out important topics. However, the authors stated that this is also the weakness. The respondents can give all the input they want, which can result in (a lot of) irrelevant information. The first interview is conducted with the supervisor of this research at CAPE Groep, and checked by interviewing other employees of CAPE Groep.

Structured interviews

Structured interviews are interviews where each interview includes the same questions and in the same order. The goal of using structured interviews is to generate answers that can be seen as reliable and to generate many responses in a short period (Hofisi et al., 2014). Hofisi et al. (2014) also stated that this type of interview is inflexible because the respondents can only answer the pre-defined answers. Structured interviews are not used in this research, because gathering a lot of answers in a short time is not needed within this research.

Semi-structured interviews

The semi-structured interviews are a combination of structured and unstructured interviews (Hofisi et al., 2014). Hofisi et al. (2014) stated that a list of pre-defined questions or topics should be drawn up, which can be seen as the guide of the interview. It is possible to deviate from this guide by looking deeper into questions or topics that are more relevant for a specific interviewee. The semi-structured interviews are used in this research for filling the framework and evaluating the mapped processes. This type of interviews is also used for the validation of the framework.

Research goal and questions

As explained in paragraph 1.1, a framework will be designed for the combination of procedures of internal control and Agile in a growing business. To achieve this, the main question and research questions are formulated. After the design of the framework, it is tested at CAPE Groep to see how the framework performs and to validate the framework. Finally, the results and the conclusions are discussed.

Research goal

The goal of this research is to give Agile businesses insights in the procedures of internal control while they comply with the needs of their stakeholders. These insights are given by a framework which is designed in chapter 3. The framework is applied on CAPE Groep and the results are evaluated.

Main research question

The main research question gives an answer to the main research problem. The main problem is that a solution for the combination of internal control and Agile is not available while it is needed. The main question is formulated as follows:

> *How should the procedures of internal control be designed within an Agile business while complying with the needs of their stakeholders?*

Research questions

To be able to answer the main question, ten research questions are formulated. Research questions 1 till 6 are about obtaining useful literature. Research question 7 answers how the framework must be designed. Research question 8 answers how the framework can be implemented. Research question 9 answers the problem as formulated by CAPE Groep, by implementing the framework at CAPE Groep. The performance of the framework will be measured by research question 10.

Research question 1: *What information about VUCA and Agile is needed from literature to develop a framework for the main problem?*

The answer of this question must provide enough information about Agile such that the part of the framework about the Agile production process can be designed. Literature about VUCA must be gathered because this is the reason to use Agile. Desk research is executed to gather relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in a short introduction about VUCA, information about the Agile methodology, most used Agile methods, and the importance of Agile. This is described in section 2.2.

Research question 2: *What information about internal control is needed from the literature to develop a framework for the main problem?*

The answer of this question must provide enough information about internal control so the part of the framework about internal control can be designed. Desk research is executed to gather the relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in a short introduction about internal control and descriptions of multiple internal control categories, levers of internal control, importance of internal control, and how the combination of Agile and internal control is made in an already existing framework. This is described in section 2.3.

Research question 3: *What information about stakeholders is needed from the literature to develop a framework for the main problem?*

The answer of this question must provide enough information about stakeholders so the part of the framework about stakeholders can be designed. Desk research is executed to gather the relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in a description of standard stakeholders within a company. A selection of these stakeholders will be made by using the literature and information that is provided by a company which falls within the scope of the research. This is described in section 2.4.

Research question 4: *What information about already existing relevant frameworks is needed from the literature to develop a framework for the main problem?*

The answer of this question must provide enough information about already existing relevant frameworks so these can be used as inspiration for the design of the framework. Desk research is executed to gather the relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in descriptions of already existing relevant frameworks and their use within this research. This is described in section 2.5.

Research question 5: *What information about security and privacy standards is needed from the literature to develop a framework for the main problem?*

The answer of this question must provide enough information about security and privacy standards to understand how these standards must be used. Desk research is executed to gather the relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in descriptions of multiple security and privacy standards. These standards can be applied on the framework, because these measures exist of internal control measures. The security and privacy standards are described in section 2.6.

Research question 6: *What information about Enterprise Risk Management is needed from the literature to develop a framework for the main problem?*

The answer of this question must provide enough information about Enterprise Risk Management to show the importance of internal control. Desk research is executed to gather the relevant literature. The databases Scopus, Web of Science, and Google Scholar are used. This will result in a description

of Enterprise Risk Management, importance of internal control, and importance of stakeholders. This is described in section 2.7.

Research question 7: *How can a proper framework be designed and validated for the main problem?*

The answer of this question must provide an answer to the designing problem. With the correct requirements for the solution, a useful framework can be designed. These requirements are derived from the literature and practical experience of stakeholders. This question is answered in the third chapter of this thesis, where the framework is designed according to the literature.

Research question 8: *How should companies implement the framework within their business?*

The answer of this research question shows how companies can make use of the framework and how they should implement the framework. This is done by writing an implementation plan, described step by step. The implementation plan is written in chapter 4. This implementation plan will help companies to implement and start using the framework.

Research question 9: *How is the framework implemented and validated at CAPE Groep?*

The answer of this research question must provide the implementation and the validation method at CAPE Groep. The implementation plan from chapter 4 is used to implement the framework at CAPE Groep. Chapter 5 shows how the framework is performing at CAPE Groep. Here is described how the framework is implemented at CAPE Groep and useful results are provided. Only a part of the framework is tested due to certain limitations, which can be found in chapter 5.

Research question 10: *How is the framework experienced by CAPE Groep?*

The last research question is about the experience with the framework of participants. This question must show if CAPE Groep wants to use the framework. By making use of a validation model, the experience of the stakeholders can be analysed and used for the evaluation. This research question is answered in chapter 6.

1.3 Validity and reliability

According to Brink (1993), this research is a qualitative research as it is about people's belief, experience and meaning systems from the perspective of the people. Methods used are more subjective than in quantitative research and do not include statistical analysis and empirical calculation. Brink (1993) also stated that validity in this kind of research is about the accuracy and truthfulness of scientific findings, and reliability is about the consistency, stability, and repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately.

Validity

As stated before, validity is about the accuracy and truthfulness of scientific findings. A study is valid if it demonstrates what actually exists and if a valid measure should actually measure what it is supposed to measure (Brink, 1993). So this research can be classified valid if the findings are a correct reflection of the truth. To ensure the validity of this research, all interviews will be recorded and worked out so all important information is always available. The framework that is designed during the research is also valid because scientific literature is used for the design, and validation is performed with an already existing validation method.

Reliability

As stated before, reliability is about the consistency, stability, and repeatability of the informant's accounts as well as the investigators' ability to collect and record information accurately. Brink (1993) also stated that it refers to the ability of a research method to yield consistently the same results over repeated testing periods. To ensure a high reliability, interview questions were asked objectively. This made sure every respondent could think about his own opinion and vision. Besides, the interviews are recorded, so that the researcher could listen to interviews multiple times and take the exact statement into account instead of his own interpretation of the answer. Moreover, pre-defined questions where used to ensure every interview was as similar as possible.

There were also conditions that reduce de reliability of this research. For example, only seven people where interviewed, chosen by availability, job function and knowledge about other stakeholders. Research is not clear about the amount of qualitative data that is needed to generalise a research, however in most research it lies above seven.

1.4 Scientific and practical relevance

The scientific relevance of this research is the framework (designed in chapter 3) about the procedures of internal control within an Agile business while complying with needs of their stakeholders. Such a framework is not available in the literature, so this research fills that gap while it is needed. This framework delivers a solution for the combination of Agile and internal control categories (Financial, IT and data) and how to deal with the needs of stakeholders. The framework shows the difference between all the combinations of categories, steps of an Agile process and the needs of stakeholders. Next to this, internal control measures can be put in the framework to see if a specific measure fits within the needs of these stakeholders. These deliverables ensure that this research is a contribution to the scientific world.

The practical relevance of this research is the framework that is designed in chapter 3 and implemented at CAPE Groep in chapter 5. This framework makes clear how CAPE Groep can remain Agile while they comply with the procedures of internal control, and the needs of their stakeholders. With the growth of CAPE Groep, the introduction to security and privacy standards becomes necessary. The framework must be used by implementing the internal control measures.

At the end of the research, CAPE Groep stays an Agile business with clear procedures of internal control while they comply with the needs of their stakeholders. This gives more control for the stakeholders, because they can see CAPE Groep as a reliable partner, supplier, and employer.

2. Literature review

This chapter provides the relevant literature to answer research question 1 until 6. Section 2.1 shows the search method for the literature gathered during this research. The second section shows information about VUCA and Agile. The third section gives information about internal control and internal control categories (Information Technology (IT), financial, and data). The next section describes the standard stakeholders of a company. The fifth section is about existing relevant frameworks and how they can be used by designing the framework. The sixth section consists of security and privacy standards. The last section describes Enterprise Risk Management.

At the end of every section, except of section 2.1, a short summary is provided to show the importance of that part for the research. This chapter supports in answering research questions 1 till 6, which can be found in section 1.2.

2.1 Search method

This chapter must provide a detailed description of the literature. The scientific databases Scopus and Web of Science are used to find relevant literature. The third database that is used is Google Scholar. This database contains scientific papers. Not only these databases are used for gathering literature. When these search engines do not provide the necessary information, webpages found via Google are used. Because of the lower reliability of these webpages, at least two webpages providing the same information are needed. Of course, it must be checked if the webpages can be marked as reliable.

Before the search engines can be used with search words, the relevant topics must be pointed out. The relevant topics are the headings of the upcoming sections within this chapter, like section 2.2.

The headings are mainly used as the search words at the search engines. At a subsection, more specific search words can be used. This can be demonstrated by this example: First, internal control has been used as the search word. Next, IT, financial and data are added one at a time.

Most of the searches will give a lot of scientific literature. To filter these articles, multiple selection criteria are used. First, the article must be openly available. Without access to the files, a source is useless. The next filter is the abstract of the articles. Most of the time, the abstract gives a clear overview of the content of an article. The remaining articles will be scanned (if there are still too many articles) to see which articles seems to be useable. The last step is reading the whole article and use the important information in this chapter.

Another method that will be used is consulting the references of relevant papers. This is done after reading a paper, but crucial information is missing in that specific paper. Related papers can easily be found within the references of the previous found papers. Then, the process starts again with analysing the abstract of the papers and selecting.

2.2 VUCA and Agile

Literature about Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) is needed because the world is VUCA at the moment. A short description about VUCA can be found below. This is just a short description because VUCA is not of great importance, but only the cause of using Agile. Namely, Agile is a method to deal with this VUCA world as mentioned in section 1.1. Literature about Agile is needed so the part of the framework about the Agile production process can be designed. This is the reason why VUCA and Agile must be included in this literature review.

VUCA

In the current business world, VUCA describes an environment where confident diagnoses and managers are confused (Bennett & Lemoine, 2014). The only constant factor in the current VUCA world is change (Sousa, Tereso, Alves, & Gomes, 2018). To be able to deal with change and to remain competitive, they stated that innovation is the key. Bennett & Lemoine (2014) also stated that in a VUCA world, strategic planning and other core activities which are essential to the performance of the organisation are seen as non-value adding to the whole organisation. The conditions of a VUCA world make it useless to predict the future and to plan on responses (Bennett & Lemoine, 2014).

Agile

Agile can be defined as: "able to move quickly and easily", or in more detail as: "used to describe a way of working in which the time and place of work, and the roles that people carry out, can all be changed according to need, and the focus is on the goals to be achieved, rather than the exact methods used" according to the Oxford Learner's Dictionaries (2019).

	Traditional	Agile
Fundamental Assumptions	Systems are fully specifiable, predictable, and can be built through meticulous and extensive planning.	High-quality, adaptive software can be developed by small teams using the principles of continuous design improvement and testing based on rapid feedback and change.
Control	Process centric	People centric
Management Style	Command-and-control	Leadership-and-collaboration
Knowledge Management	Explicit	Tacit
Role Assignment	Individual—favors specialization	Self-organizing teams—encourages role interchangeability
Communication	Formal	Informal
Customer's Role	Important	Critical
Project Cycle	Guided by tasks or activities	Guided by product features
Development Model	Life cycle model (Waterfall, Spiral, or some variation)	The evolutionary-delivery model
Desired Organizational Form/Structure	Mechanistic (bureaucratic with high formalization)	Organic (flexible and participative encouraging cooperative social action)
Technology	No restriction	Favors object-oriented technology

Figure 3: Traditional versus Agile software development (Nerur, Mahapatra, & Mangalaraj, 2005)

The biggest difference when comparing the Agile methodology with the traditional waterfall model, where the process consists of sequential steps, is that Agile is adaptive. Deviating from the plan is the standard and should contribute to the result (Thummadi et al., 2011). Most of the time, Agile is characterized as the successor of the waterfall model (Ralph, 2016). The waterfall model has become unpopular due to the high level of bureaucracy, which created the demand for the Agile methodology (Conboy & Fitzgerald, 2004). Agile helps teams to deal with uncertain environments. It is the ability to quickly respond to changes (Thummadi et al., 2011). Figure 3 shows an overview of the differences between traditional (waterfall) and Agile software development.

Beck et al. (2001) stated some new views on business items in their Manifesto for Agile Software Development, which can be seen as the birth of Agile. They prioritise individuals and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation, and responding to change over following a plan. All the second appointed items are important for businesses, but the first mentioned items are of more value.

Figure 4 shows the benefits of the use of Agile within a company. These numbers were gathered by a research of CollabNet & VersionOne (2019). The largest benefits according to this research are: ability to manager changing priorities, project visibility, Business/IT alignment, team morale, delivery speed/time to market and increased team productivity.

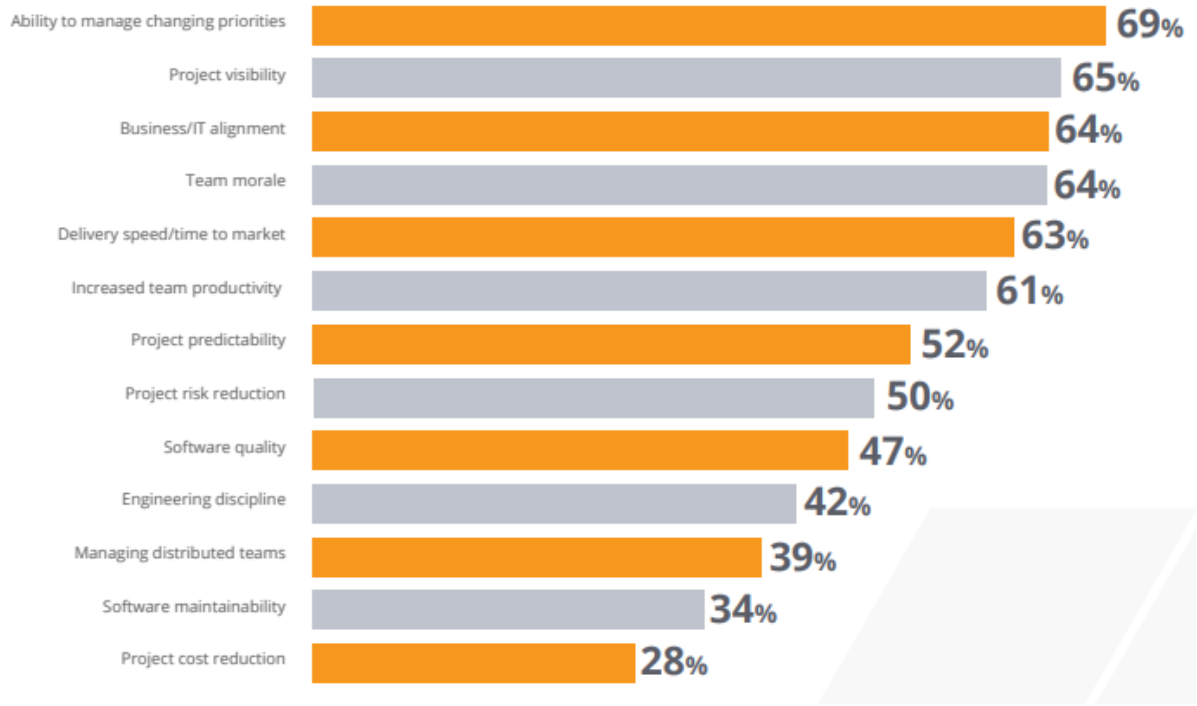


Figure 4: Benefits of Agile development (CollabNet & VersionOne, 2019)

A possibility to use Agile is by making use of sprints, according to the SCRUM principle. 72% of the respondents of the survey of CollabNet & VersionOne (2019) reported that they use the SCRUM principle. This makes SCRUM the most used agile method (CollabNet & VersionOne, 2019). The second most used principle is SAFe, with a 30% use by the respondents. More information about the SCRUM principle is depicted in Figure 5 and described in section SCRUM. More information about SAFe is depicted in Figure 7 and described in section Scaled Agile framework in relation to internal control.

SCRUM

The SCRUM principle as described by Sutherland & Schwaber (2011) is depicted in Figure 5. The SCRUM process is iterative for development of projects and products.

According to Sutherland & Schwaber (2011), the iterative cycles at SCRUM are called sprints, which take normally 1-4 weeks. The next sprint starts immediately after the last sprint ended. Changes in duration or goals during the sprint are not allowed. The sprint starts with a cross-functional team selecting desired features from the product backlog, which were enumerated by the Product Owner (PO). These features become tasks for that sprint, and are enumerated in the sprint backlog. These tasks are known as user stories. Every day a short meeting take place where every team member gives an update about the progress, and which steps are needed to finish the product. At the end of the

sprint, a shippable product is created which will be reviewed together with all stakeholders. After the review, a retrospective will take place with only the project team where they will evaluate the process of the sprint.

The project team must provide the PO with estimates of the required effort for a feature. Probably, the project team needs more information to make a good estimate. Gathering those information is done in the product backlog refinement session. It is also possible to split features into multiple features if the feature is too large or to analyse the detailed requirements. 5 to 10 per cent of the sprint must be dedicated to refining (Sutherland & Schwaber, 2011).

There are three different roles within a SCRUM team, namely, PO, project team, and SCRUM master (Sutherland & Schwaber, 2011). They stated that the PO must ensure that the return on investment is maximized. The PO will achieve this by constantly filling, refining and prioritizing the product backlog. The project team builds the application with the features from the sprint backlog during a sprint. This project team is cross-functional and self-organizing. The SCRUM master is not the (project) manager but protects the team from outside interference, and educates them the skills of SCRUM. The SCRUM methodology is shown in Figure 5.

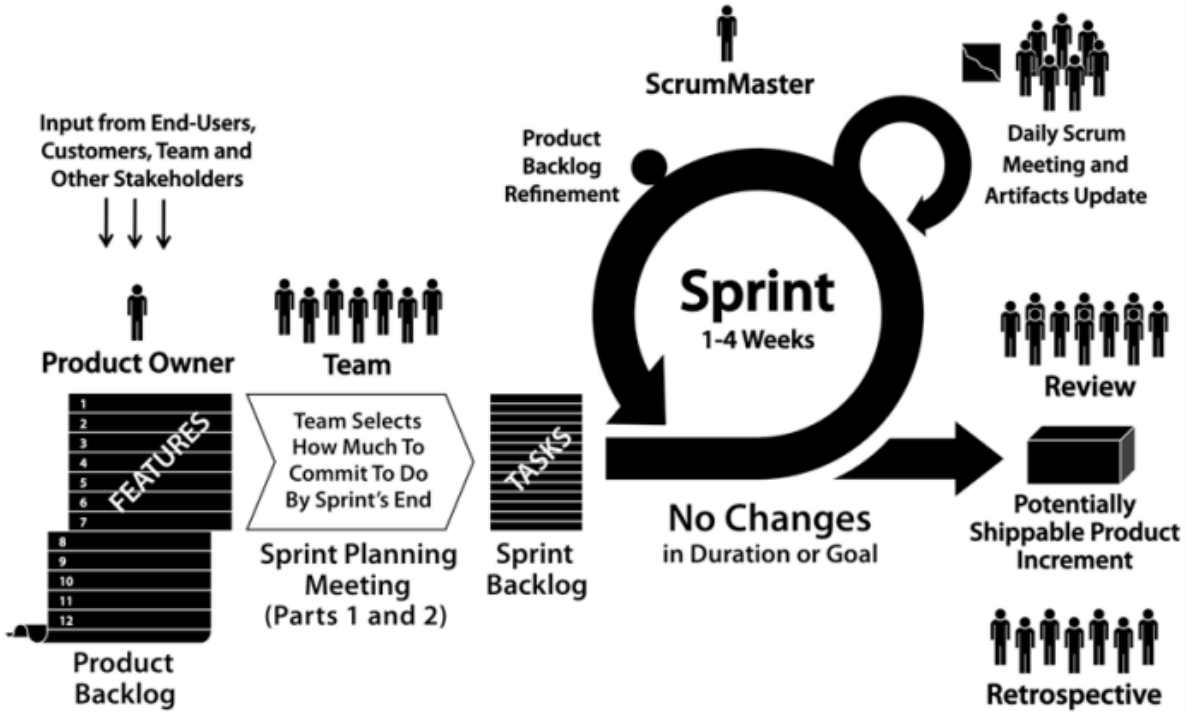


Figure 5: Agile/SCRUM framework (Sutherland & Schwaber, 2011)

According to a survey conducted by Sutherland & Schwaber, 68% of the respondents indicate that SCRUM is increasing their productivity and 27% of the respondents indicate that they do not see a decrease or increase in their productivity (Sutherland & Schwaber, 2011). They also indicated an increase in team morale, adaptability, accountability, and collaboration and cooperation.

At SCRUM, two definitions must be formulated to ensure that user stories and products fulfil the needs of a stakeholder. The first definition is the Definition of Ready (DoR). This is a checklist where a feature/task/user story must comply with, before it can be placed in the sprint backlog (Rubin, 2012). The second definition is the Definition of Done (DoD). Rubin (2012) stated that the sprint results must be a potentially shippable product increment. This means that the project team must do what they

agreed on at the start of the sprint. He stated that the DoD specifies the degree of confidence that the quality of the product is good, and if it can be shipped potentially.

Standard steps of an Agile production process

The Agile development cycle consists of 6 stages (Lucidchart, 2017; Smartsheet, 2019). These stages are enumerated below, including a short description per stage.

1. Concept – Proposal and prioritize projects.
2. Inception – Requirements for first sprint are defined. These requirements include: identify team members, funding, and initial environments.
3. Construction/iteration – The sprints are performed in this stage.
4. Release – Quality testing, internal and external training for end users, documentation, and finally the release of the product.
5. Production and support – Production of the product and ongoing support.
6. Retirement – End-of-life activities, and customer notification and migration.

Use in this research

This section provides information about Agile, which helps by designing the framework. This information is needed for this research because the scope is focused on companies using Agile. The Agile methodology must be understood to be able to develop a framework based on an Agile production process. This section also provides information about the most used Agile method, SCRUM. Next, this section shows why companies should start using Agile (and VUCA), why Agile is a good method to use, and why they should keep making use of Agile.

2.3 Internal control

Internal control is defined as a connected set of activities that is placed above the standard business operations and processes (Bragg, 2018). He stated that the intention is to protect assets, to mitigate errors, and to ensure that all the operations and processes are performed well. At first sight, internal control seems to slow down the process due to extra checks which results in less efficiency. On the other hand, prevention is better than cure and lost time can be regained. Even if the internal control slows down the processes, the risk reduction can be more important than the small loss in efficiency, according to Bragg (2018). Three types of internal control are discussed in this research; Information Technology internal control, financial internal control, and data internal control. Other types of internal control can be used if one wants to use the framework in another industry, like healthcare.

Information technology internal control

Most of the companies nowadays make use of Information Technology (IT) and are even dependent of this technology to conduct their business operations (Chang, Yen, Chang, & Jan, 2014). This dependence on IT, together with increasing complexity and the interconnectedness of IT systems and infrastructure, and also constantly changing threats and regulations, result in growing risks (Stoel & Muhanna, 2011). These growing risks should be limited by implementing IT internal control according to Stoel & Muhanna (2011). Useful methods that can be used for IT internal control are Service Organization Control (SOC) 2 and SOC 3. Section 2.6 Security and privacy standards explains why these methods are useful in this case.

Financial internal control

According to the B Resource Guide: Implementing Financial Controls (Certified B Corporation, 2019), financial control measures are needed for directing, monitoring, measuring and protecting the resources of the organisations. They also stated that these measures play important roles in the accuracy of reporting and eliminating fraud. Some measures that they offer are: separation of duties

(Accounts Receivable/Accounts Payable), access to accounting software systems, access to credit cards and ATM cards, and inventory management. A useful method that can be used for financial internal control is SOC 1.

Data internal control

The third type of internal control that is discussed in this research is data internal control. This type of internal control is about the security of information and (personal) data. Useful methods that can be used for data internal control to reduce the chance of a breach are International Organisation for Standardization (ISO) 27001, ISO 27701 and General Data Protection Regulation (GDPR) (IT Governance UK, 2019). These methods are correlated in a certain way according to IT Governance UK (2019). This correlation is described in section 2.6 Security and privacy standards.

Levers of internal control

Simons (1995) stated that in the 1950s and 1960s senior managers protected their companies from control failures by telling their employees how they must do their job. These employees where checked constantly to prevent surprises. This approach can still be effective at certain companies. However, at most companies nowadays managers do not have the time to constantly check how an employee is doing his job. Also, just hiring the best employees, aligning incentives, and hoping for the best will not be enough. Managers must encourage employees to improve the working processes and to find new solutions for complying with the needs of the customer, but this should always happen in a controlled way.

According to Simons (1995), most managers will define control as measuring progress against plans to guarantee the predictable achievement of goals. This is only one of the ways to achieve control. The ways of achieving control are described by Simons (1995) as the levers of internal control.

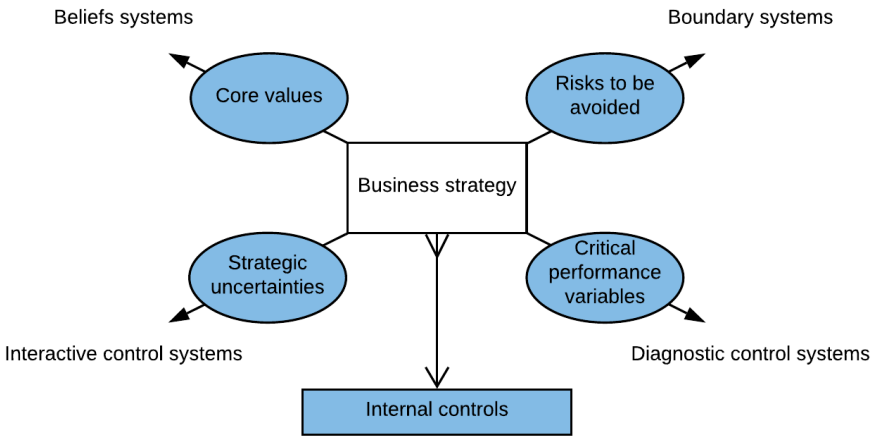


Figure 6: Levers of internal control (Simons, 1995)

The four levers of internal control according to Simons (1995) are depicted in Figure 6. These levers are: beliefs systems, boundary systems, diagnostic control systems, and interactive control systems. The beliefs systems communicate core values and inspire all employees to do their best for the organisation (Simons, 1995). He stated that beliefs systems must show how the organisation creates value, the preferred performance level, and how internal and external relationships should be maintained. About the boundary systems he stated that these systems define the rules and which dangerous situations should be avoided. By telling employees what they should avoid instead of telling them what they exactly should do, the creativity and initiative of the employees will be exploited (Simons, 1995). The diagnostic control systems are the most common systems in most organisations, because these systems ensure that the main goals of an organisation are achieved efficiently and

effectively (Simons, 1995). He stated that these control systems should prevent the manager of constant checking work of employees. The fourth lever of internal control according to Simons (1995), interactive control systems, helps managers to focus on strategic uncertainties, threats, opportunities and to respond quickly. He stated that managers can involve themselves in decisions of employees via this system. If these levers are used effectively, managers can be confident that employees can be creative and initiative without negatively influencing internal control (Simons, 1995).

Importance of internal control

Using internal control is really important for large organisations. This is evidenced by the fraud at some enormous companies like Enron and WorldCom. Enron has become a symbol of corporate excess and fraud (Neuman, 2005). They created of-the-books partnerships to hide debt and to increase executives' wealth, shredding documents, and obstructing justice. Because of the bankruptcy, investors lost in total $64.2 billion. Making use of internal control should decrease the chance of fraudulent situations.

Next to fraud, internal control is also important because errors or misstatements of financial statements can happen (by accident), it helps by understanding and mitigating risks, discovering small errors before they become bigger problems, and to establish company practices (AICPA, 2014; DeBenedetti, n.d.; Zhang, 2016). The internal control measures can ensure that the balances on the balance sheet are correct, so the chance on errors or misstatements of financial statements are decreased. Understanding risks will help by determining if there are measures in place to mitigate those risks. Establish company practice will help by proving that internal control measures are in place. This can be important for some customers, or to achieve security and privacy standard certificates, as described in section 2.6 Security and privacy standards.

Scaled Agile framework in relation to internal control

When Agile methods are used for developing large systems, scaling Agile methods must be used (Reifer, Maurer, & Erdogmus, 2003). They stated that these scaling Agile methods must help when multiple developers are working simultaneously, when teams of teams are working together. The Scaled Agile Framework (SAFe) is the framework that is used the most as Agile scaling method (CollabNet & VersionOne, 2019).

SAFe can be seen in Figure 7. According to Leffingwell et al. (2019), their framework makes use of the power of agile and lean product development to help organisations with their challenges with developing and delivering software and systems which are robust and scalable for the whole organisation.

SAFe can be seen as the bridge between managers and employees (Leffingwell, 2019). Managers need a controlled way of working for their employees and needs should be fulfilled within long term period, at SAFe usually 3 months. Contrary to managers, employees want scalable assignments for a shorter term period, at SCRUM mostly 2 weeks. These shorter periods are the sprints or iterations where the product or service is created and tested. The long term period has a greater goal where the end product should be developed and validated. According to Leffingwell et al. 2019, stakeholders are already involved during the sprints by continually testing the product or service. SAFe is a framework what is designed for lean enterprises. Lean stands for a business strategy and a way of working where everything must has the goal to create customer value (LeanSixSigma, 2019). According to them, all activities that create waste should be eliminated. In this way of working, the customer is the focus and the maximum added value for the customer will be achieved with minimal effort.

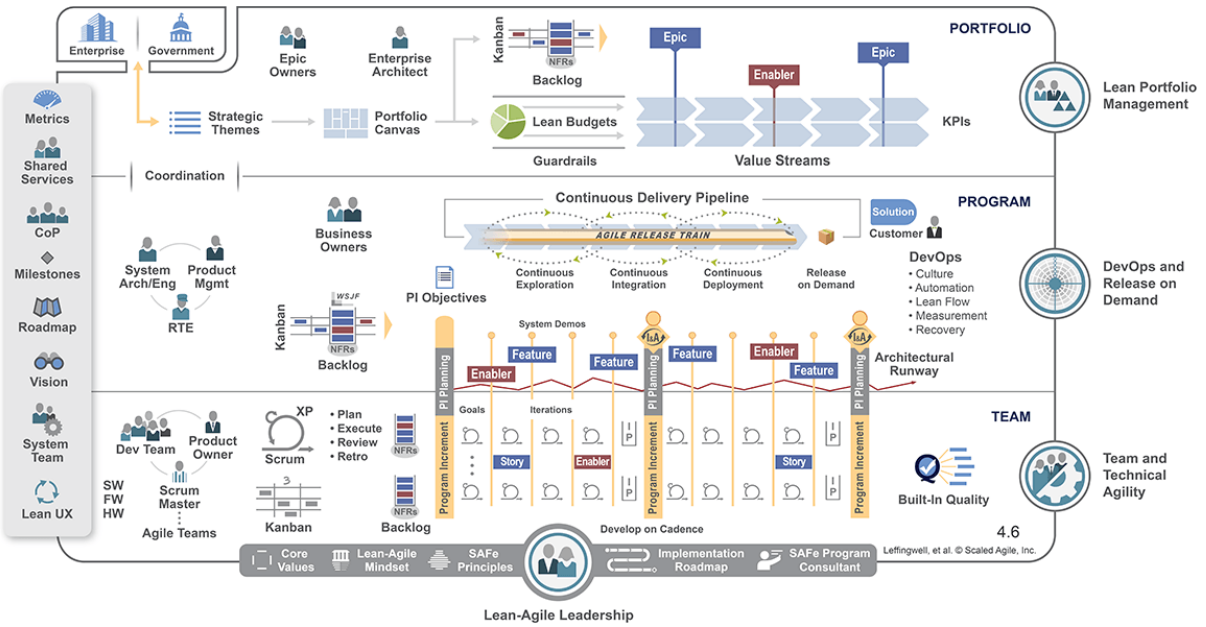


Figure 7: Scaled Agile Framework (Leffingwell et al, 2019)

Use in this research

This section starts with an introduction about internal control. The internal control categories (IT, financial, and data) described in this section, are used for the design of the framework in section 3.2. The levers of internal control are used for a better understanding of internal control. Next, the importance of internal control is described. This part shows that it is really important to use internal control within a company. Lastly, SAFe shows how multiple teams collaborate and how the combination of control (managers) and Agile can be made within a framework.

2.4 Stakeholders

Literature about stakeholders is needed because the stakeholders are a main component of this research. With this literature, the stakeholders in the framework are correct.

According to Bryson (2004), stakeholders can be defined as persons, groups, or organisations that must somehow be taken into account by leaders, managers, and front-line staff. This includes being affected by or able to affect the achievement of an organisation's objectives (Freeman, 2010). Stakeholders become more and more important for organisations because the stakeholders contribute by fulfilling the missions of organisations and creating value (Bryson, 2004).

Stakeholders can be divided into direct and indirect stakeholders (Bonner, 2020). Bonner (2020) stated that direct stakeholders are involved in the daily business. By contrast, indirect stakeholders are not interested in the daily work, but in (the quality of) the end product.

There are a lot of different opinions about the standard stakeholders within a business. Freeman (2010) created a stakeholder map of a very large organisation which is shown in Figure 8. This stakeholder map consists of all the stakeholders that must be considered according to Freeman (2010), so companies can pick the stakeholders that are applicable on there situation.

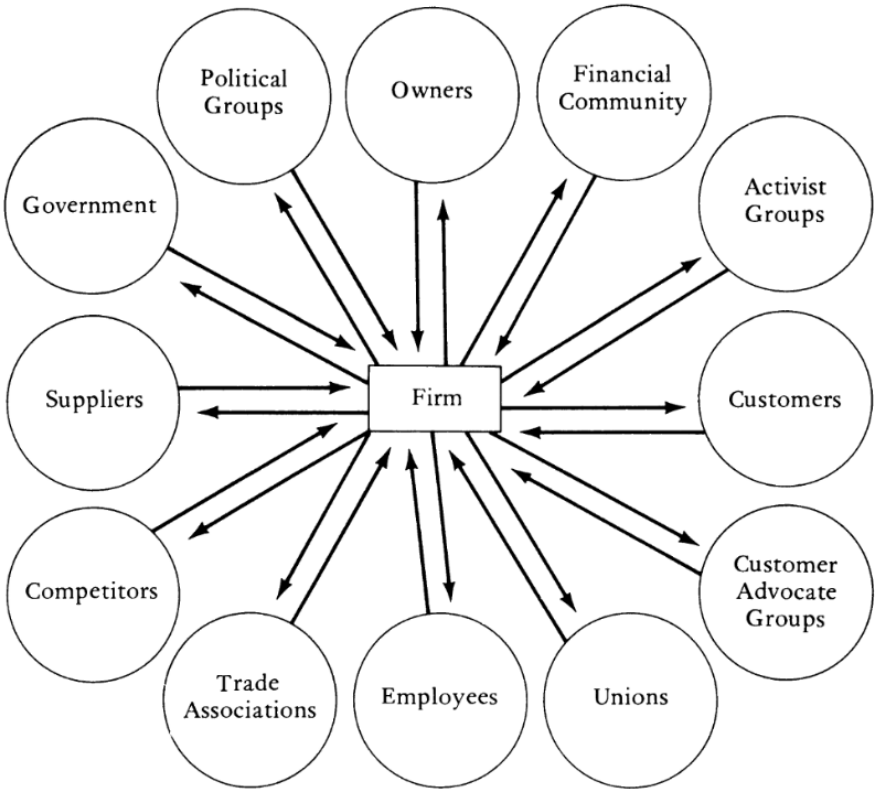


Figure 8: Stakeholder map of a very large organisation (Freeman, 2010)

Use in this research

The stakeholders which must be picked for the design of the framework can be differently in every situation. The choice of the stakeholders for this research is based on this literature and on the stakeholders of the company where the framework is validated, CAPE Groep. The shareholders, employees, customers, government, partners, and suppliers were mentioned by CAPE Groep as possible stakeholders. The stakeholder 'partners' is not mentioned by Freeman (2010), because the partners are part of the suppliers and customers. It depends per company if these categories are separated or not. Next, CAPE Groep did not see competitors as stakeholders. According to Freeman (2010) and Archer (2006), competitors are important to consider as a stakeholder. They stated that competitors will influence your behaviour if: they make an innovative product which you can produce too, a customer, supplier or investor can become a competitor, or a competitor can become a customer, supplier or investor.

2.5 Existing relevant frameworks

A lot of internal control frameworks already exists in the literature. One of the most widely used internal control frameworks is the internal control – integrated framework of COSO (Committee of sponsoring organisation of the Treadway commission). Other interesting frameworks, for the design and place in the literature of the designed framework, are the Zachman framework and Porter's value chain.

COSO internal control – integrated framework

According to previous research (COSO, 2013b; Uwadiae, 2015; Kirkpatrick, 2019), one of the most adopted internal control frameworks is the internal control – integrated framework of COSO. The framework facilitates companies to effectively and efficiently develop systems of internal control that are able to react on a changing environment (COSO, 2013a). They stated that systems of internal

control are also able to mitigate risks to a reasonable level, and support in making good decisions and governance of the organisation.

The five components of internal control are control environment, risk assessment, control activities, information and communication, and monitoring activities (COSO, 2013a). These five components are shown in the front view of the cube in Figure 9. COSO stated that 'control environment' is about the set of standards, processes, and structures that forms the basis for performing internal control. They describe the 'risk assessment' as the dynamic and iterative process for recognizing and evaluating risks so objectives can be achieved. The 'control activities' are described by COSO as the actions established by policies and procedures. These measures should lead to proper implementation of the directives of the management to mitigate the risks of achieving their goals. They wrote about the next layer that 'information' about the organisation is necessary to carry out internal control responsibilities to support the achievement of its objectives. 'Communication' is the continuous process of providing, sharing, and obtaining necessary information. 'Monitoring activities' is about the evaluations to check if all the components of internal control are present and functioning.

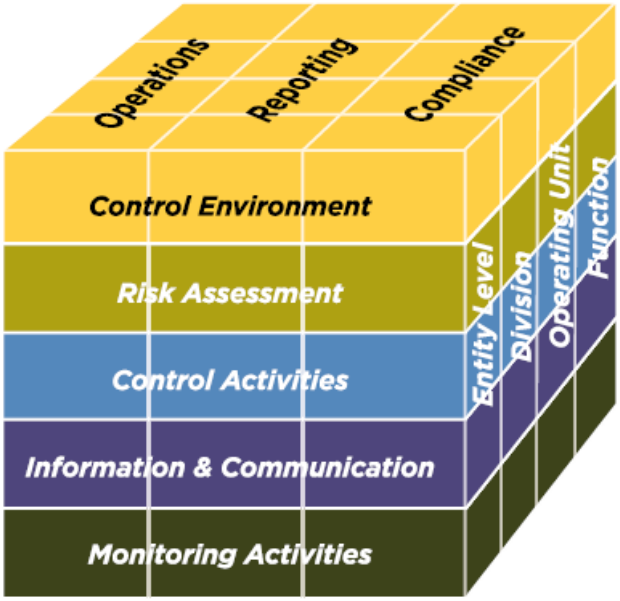


Figure 9: Relationship of objectives and components of the COSO internal control - integrated framework (COSO, 2013a)

The top of the cube in Figure 9 shows the objectives. This are the operations, reporting, and compliance. This is what an entity should strive to achieve. The relationship of the objectives, components, and the organisational structure (entity level, division, operating unit, and function) is visualised by the cube in Figure 9.

COSO (2013a) stated that there are some principles per component that represent the fundamental concepts of internal control. If the principles are applied well, effective internal control will be the result (COSO, 2013a). Effective internal control means reducing the risk of not achieving an entity's objective to an acceptable level. Effective internal control will only be the case if all five components are present and functioning, and operate together in in an integrated manner. The principles defined by COSO are enumerated per component below.

Control environment

1. The organisation demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk assessment

6. The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organisation identifies and assesses changes that could significantly impact the system of internal control.

Control activities

10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organisation selects and develops general control activities over technology to support the achievement of objectives.
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and communication

13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring activities

16. The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Zachman framework

This framework is designed as a tool for Information Systems Architecture (ISA) (Sowa & Zachman, 1992). They stated that the framework should combine the concepts of the real world with the concepts of information systems.

The design of the framework is displayed in Figure 10. The top row shows the interrogative words: *What, How, Where, Who, When,* and *Why*. The first three are about what entities are involved, how they are processed, and where they are located. The last three are about who works with the system, when the events occur, and why the events are taking place. Combining these six interrogative words with the concepts in the first column, gives 36 different perspectives. The last row, the operations classes, are not depicted in the paper of Sowa & Zachman (1992). This row is added later but not always considered.

There are some rules if you want to use this framework according to Sowa & Zachman (1992). The first rule is that the columns have no order. This means that there is no prioritisation between the columns, so there is no prioritisation and bias between the different aspects. The second rule is that each column has a basic model. This are the interrogative words. The third rule is that each column must be unique. Rule number four stated that each row represents a unique perspective. The fifth rule listed that each cell must be unique. Rule number 6 stated that all cells in a row make up a model for that specific perspective. The last rule is that the logic is recursive.

	WHAT	HOW	WHERE	WHO	WHEN	WHY	
SCOPE CONTEXTS	Inventory Identification Inventory Types	Process Identification Process Types	Network Identification Network Types	Organization Identification Organization Types	Timing Identification Timing Types	Motivation Identification Motivation Types	STRATEGISTS AS THEORISTS
BUSINESS CONCEPTS	Inventory Definition Business Entity Business Relationship	Process Definition Business Transform Business Input	Network Definition Business Location Business Connection	Organization Definition Business Role Business Work	Timing Definition Business Cycle Business Moment	Motivation Definition Business End Business Means	EXECUTIVE LEADERS AS OWNERS
SYSTEM LOGIC	Inventory Representation System Entity System Relationship	Process Representation System Transform System Input	Network Representation System Location System Connection	Organization Representation System Role System Work	Timing Representation System Cycle System Moment	Motivation Representation System End System Means	ARCHITECTS AS DESIGNERS
TECHNOLOGY PHYSICS	Inventory Specification Technology Entity Technology Relationship	Process Specification Technology Transform Technology Input	Network Specification Technology Location Technology Connection	Organization Specification Technology Role Technology Work	Timing Specification Technology Cycle Technology Moment	Motivation Specification Technology End Technology Means	ENGINEERS AS BUILDERS
COMPONENT ASSEMBLIES	Inventory Configuration Component Entity Component Relationship	Process Configuration Component Transform Component Input	Network Configuration Component Location Component Connection	Organization Configuration Component Role Component Work	Timing Configuration Component Cycle Component Moment	Motivation Configuration Component End Component Means	TECHNICIANS AS IMPLEMENTERS
OPERATIONS CLASSES	Inventory Instantiation Operations Entity Operations Relationship	Process Instantiation Operations Transform Operations Input	Network Instantiation Operations Location Operations Connection	Organization Instantiation Operations Role Operations Work	Timing Instantiation Operations Cycle Operations Moment	Motivation Instantiation Operations End Operations Means	WORKERS AS PARTICIPANTS
	INVENTORY SETS	PROCESS TRANSFORMATIONS	NETWORK NODES	ORGANIZATION GROUPS	TIMING PERIODS	MOTIVATION REASONS	

Figure 10: The Zachman framework (Visual Paradigm, 2019)

Porter's value chain

Porter's value chain is a method that contains a collection of all the performed activities within an organisation that creates added value for their customers (Porter, 1985). These activities can be divided into primary activities and support activities as shown in Figure 11. He stated that primary activities are: ongoing production, marketing, delivery, and servicing of the product. The support activities are those providing purchased inputs, technology, human resources, or overall infrastructure functions, to support the primary activities. Firms do not only consist of these activities, but these

activities form a network of activities (Porter, 1985). The connections between the activities arise when the result of an activity influences another activity according to Porter (1985).

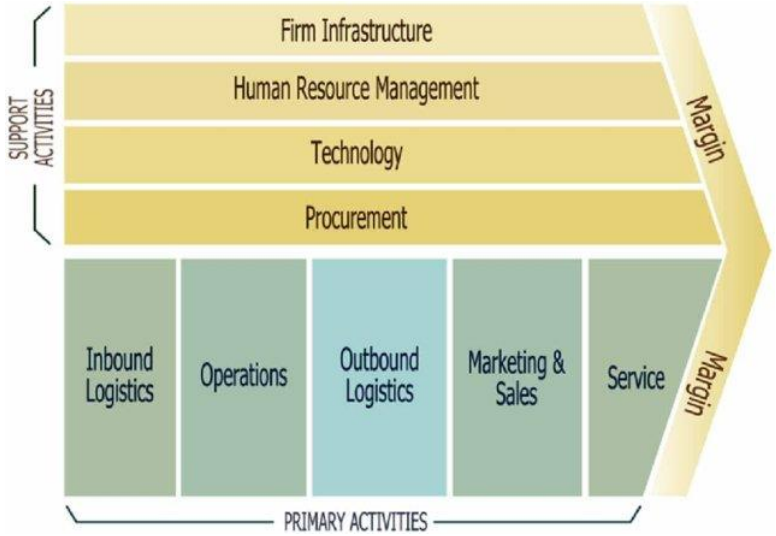


Figure 11: Porter's value chain (Porter, 1985)

One of the support activities is the firm infrastructure. This activity includes all the systems that support and allow functions to be able to operate. Departments of the company that are part of the firm infrastructure are accounting, legal, administration, finance, planning, quality assurance, and government relations.

Use in this research

The principles of COSO are used for the design of effective internal control measures, which can be found in section 5.10. The COSO framework and the Zachman framework are used for the design of the new framework. The layout of the Zachman framework is used for the design of an internal control category perspective. COSOs design is used for the design of the whole framework. The design of the framework and the design of an internal control category perspective can be found in section 3.2. Next to that, some of the rules of the Zachman framework are used in the designed framework, which is described in section 3.2. Porter's value chain is used to show that the firm infrastructure, which support and allow functions to be able to operate, covers all business processes.

2.6 Security and privacy standards

Some of the discussed standards in this section are obligated according to the laws and rules of the Netherlands for certain companies. Namely, the financial external audit and the General Data Protection Regulation. The other standards are not obligated for any company, but are used by companies to show their reliability to their customers or to improve their internal processes.

Importance of security and privacy standards

Sarbanes-Oxley Act of 2002 (SOX) is the reaction of the US Congress on the scandals at Enron and WorldCom in the early 2000s (Pfister, 2009). He stated that SOX presented a set of requirements for companies that are registered on the US exchange. A part of these requirements, section 404, focuses on the effectiveness of the internal control over financial reporting according to Pfister (2009). A system that performs the same function as SOX, is the Service Organisation Control (SOC) compliance, but with another reasoning and techniques (Holbrook & Manter, 2018). They stated that the same function includes being protective for consumers and organisations. They also stated that the SOC compliance is an audit of internal control measures to ensure data security, minimal waste, and

shareholder confidence. More information about SOC can be found in the section about SOC 1, 2, and 3.

Financial external audit in the Netherlands

Every organisation or corporation in the Netherlands must comply with the rules regarding a financial external audit (Van Noort Gassler & Co., 2018; Maxius, 2019). These rules stated how the financial statements should be delivered by the board. An accountant performs a financial external audit to check if the financial statement is delivered correctly. But, Van Noort Gassler & Co. (2018) and Maxius (2019) stated that not all organisations and corporations are required to be checked by an auditor. The check is needed if two of the three upcoming statements are true. Total turnover is at least €12 million, balance sheet total is at least €6 million or number of employees is at least fifty.

General Data Protection Regulation

General Data Protection Regulation (GDPR) is a sophistication of the Data Protection Directive (DPP) from 1995 (Hoofnagle, van der Sloot, & Borgesius, 2019). The DDP had poor enforcement and compliance, which causes a low implementation ratio, in contrast to the GDPR. The GDPR is a legal document consisting of legal rules, organisational rules, and technical rules stated by the European Union (Gonçalves, Correia, & Cavique, 2019). They stated that these rules are needed to achieve a high level of protection of personal data. To be compliant to the GDPR, business should have a dynamic approach where the personal data is protected continuously, and the personal data should be considered as a valuable asset (Gonçalves et al., 2019). Hoofnagle et al. (2019) stated that the GDPR assumed that personal data are so important that interacting with data require a careful planning. The protection of personal data is part of the extensive privacy process to prevent personal data from unauthorized access, use, modification, recording, and destruction (Gonçalves et al., 2019).

Data protection and information security have some common ground, but there are some major differences according to Gonçalves et al. (2019). They stated that information security is about the confidentiality, integrity, and availability, also known as the CIA model. Data protection goes a step further than the information security. Data protection also includes the processing of data, handling information, and the acceptance of security measures.

Personal data protection can be defined as the effect of uncertainty due to a deficiency of information that hinders achieving organisational objectives (Gonçalves et al., 2019). To successfully perform the challenge of personal data protection risk management, an understanding of the potential risks to personal data assets of an organisation is needed. More information about risk management is given in section ISO 31000 and section 2.7.

SOC 1, 2, and 3

If a company provides services to other organisations, the other organisations' auditors need to be sure that the internal control measures at the company are designed effectively and operating effectively (Gallagher, 2019). One method to show the assurance is by undergoing a SOC audit.

Three different versions of SOC compliances are defined in literature. These are known as SOC 1, 2, and 3. SOC 1 contains mainly examining internal control measures over financial reporting, while SOC 2 and 3 reports about the pre-defined, standardized benchmarks for internal control measures related to security, processing integrity, confidentiality, or privacy of the data centre's system and information (OTAVA, 2019; Gallagher, 2019). The pre-defined, standardized benchmarks are described in the TSP Section 100, 2017 Trust services criteria for security, availability, processing integrity, confidentiality, and privacy (AICPA Assurance Services Executive Committee, 2017). A comparison between SOC 1, 2, and 3 is shown in Figure 12.

SOC 1 does not only report about the internal control measures which are directly connected to the financial statements of an organisation, but also about the design and existence of control and their operation (AuditConnect, n.d.). SOC 2 reports can be used for an oversight of the organisation, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight (OTAVA, 2019; Gallagher, 2019). SOC 2 reports are only accessible by management, regulators, and companies or customers to whom the report has been provided (OTAVA, 2019). By contrast, SOC 3 is available for everyone. SOC 3 provides the highest level of certification and assurance of operational excellence that a data centre can receive, and it provides a system description and the auditor's opinion (OTAVA, 2019). SOC 2 also contains the auditor testing and results according to OTAVA (2019). SOC audits has become more important because more services are being outsourced to data centres (Gallagher, 2019).

There are two types of SOC audits within SOC 1 and SOC 2, SOC type I and SOC type II (Gallagher, 2019; strongDM, 2019). The difference is that type I focuses on a description of service organisation's control and the suitability of how those internal control measures are designed to achieve the control objectives on a specified date, while type II added the opinion on the operating effectiveness to achieve related control objectives throughout a specified period, mostly 6 months (Gallagher, 2019; Dunkelberger, 2019; strongDM, 2019). The type II covers more time and are a more intensive investigation of the design and the processes (Dunkelberger, 2019). Both types gives the possibility to perform critical risk assessment procedures.

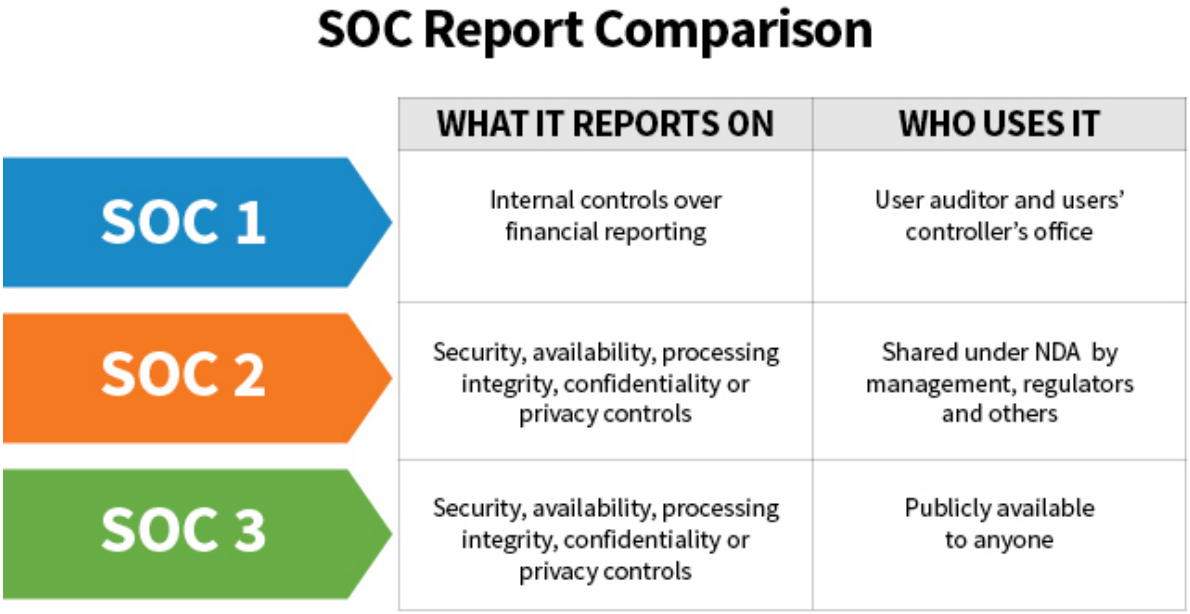


Figure 12: SOC 1, 2, and 3 comparison (OTAVA, 2019)

ISO 9001 (quality management)

International Organisation for Standardization (ISO) 9001 is the international standard that specifies the basic requirements for a quality management system (Melicharova, 2018). The most recent version is released in 2015 and will be reviewed again in 2020 (Melicharova, 2018; ISO, 2019b). The website of ISO (2019b) also stated when an organisation should use ISO 9001. The first argument they provide to make use of this quality management system is when an organisation wants to show that they are able to produce products and deliver services that meet the wishes of their customers and the regulations. The second reason is when an organisation wants to improve their customer satisfaction by effective applying the system. This system includes the processes for improving the

system, and the commitment to their customers and the regulations. This is described by Melicharova (2018) as: ISO 9001 defines the basic requirements that organisations should fulfil to meet customer requirements and to comply with the regulations.

The implementation of ISO 9001 has some internal and external benefits (Casadesús & Giménez, 2000). They stated that the most important internal benefits are: improvement of the definition and standardisation of the work procedures, improvement in the definition of the workers, increase in the company quality confidence, better involvement in work, and improvement in guidelines thus reducing improvisation. At the other side, they stated that the most important external benefits are: the response of the clients' requirements, access into new markets, improvement in customer relations, improvement in services to customers, and minimising customer audits. Both internal and external benefits are ranked in importance starting with the most important one.

ISO 27001 (information security management)

ISO 27001 is the most famous Information Security Management System (ISMS) in the series of ISO 27000 (ISO, 2019a). In the last updated version, ISO 27001:2013, the requirements for establishing, implementing, maintaining, and continually improving an ISMS of an organisation are specified (ISO, 2019d). Next to that, they mentioned that the standard also includes assessment and treatment requirements of information security risks with regards to the needs of the organisation. These requirement are generic so the standards can be implemented in every organisation according to ISO (2019d).

The CIA model, mentioned in the section General Data Protection Regulation, is about protecting information so there will be no loss of confidentiality, integrity, and availability. ISO 27001 is the standard created by ISO for securing this information. The CIA model shaped our theoretical understanding of information security and the practical side of developing and implementing security in organisations (Samonas & Coss, 2014).

ISO 27701 (privacy information management)

ISO 27701 is the guide for establishing, implementing, maintaining, and continually improving a privacy information management system, which is an extension on ISO 27001 (ISO, 2019e). ISO 27701 is a document that specifies the requirements for personally identifiable information and provide guidance for controllers and processors. The most recent version is the ISO 27701:2019.

ISO 31000 (risk management)

ISO 31000 provides guidelines for managing risk within an organisation. The most recent version of ISO 31000 is published in 2018. These guidelines provides a generic approach that can be applied on any company and on any risk type (ISO, 2019c). Risk management can also be done by using other methods. Other methods of risk management are described in the next section.

Use in this research

This section shows different privacy and security standards, which can be applied on a company within the scope of this research. All these privacy and security standards can be seen as internal control measures, or consists of a set of internal control measures. The description of these standards will help companies to apply these standards on the framework.

2.7 Enterprise Risk Management

Enterprise Risk Management (ERM) is the approach that gives organisations the ability to deal with dilemmas and risks (Abu Saleem, Zraqat, & Okour, 2019). Dealing with risks is important, because every choice we make to fulfil objectives has its risks (COSO, 2017). They stated that the increasing

Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) impacts the reliability, relevancy, and trust of an organisation. As reaction, stakeholders want to be more involved, seeking greater transparency and accountability for managing the impact of risk while evaluating the leadership's ability to form opportunities (COSO, 2017). They also stated that organisations must be more adaptive to change. The companies should think on strategic level about the VUCA of the world. A method to deal with these aspect is Enterprise Risk Management (COSO, 2017). Further, Abu Saleem et al. (2019) and COSO (2017) stated that ERM is an effective approach to take on the responsibilities of the needs of the stakeholders.

On the long term, ERM can increase the ability to anticipate and respond to changes (COSO, 2017). They also stated that ERM is not a function or a department, but it are the culture, capabilities, and practices that an organisation integrates with their strategy. ERM addresses the next topics according to COSO (2017): internal control, strategy-setting, governance, communicating with stakeholders, and measuring performance.

Optimizing strategy and performance by an effective ERM give many benefits. The most important benefits are: increasing the range of opportunities, identifying and managing risk entity-wide, increasing positive outcomes and advantage while reducing negative surprises, reducing performance variability, improving resource deployment, and enhancing enterprise resilience (COSO, 2017).

Figure 13: Enterprise Risk Management - integrating with strategy and performance framework (COSO, 2017)

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Figure 14: Principles with regards to the COSO ERM framework (COSO, 2017)

The ERM framework of COSO (2017) is shown in Figure 13. The framework consists of five components, namely, governance & culture, strategy & objective-setting, performance, review & revision, and information, communication & reporting. Principles per department are defined by COSO (2017) and are shown in Figure 14. They also stated that following these principles will lead to the organisation understanding and striving to manage the risks.

There are two major characteristics of today's world, namely, circumstances change faster than ever before, and we are more inter-connected than we have ever been (Byatt, 2017). He stated that these two characteristics demands an Agile approach to ERM. Five steps are formulated for enabling and maintaining an Agile approach to ERM. The five steps are: focus constantly on objectives, create the proper work environment and culture, be pragmatic in managing risk, track the value added by risk management, and continuously improve (Byatt, 2017).

The first step stated by Byatt (2017), focus constantly on objectives, is required for an effective risk management system. Everything you do within an organisation, is to achieve the objectives. The risks that come together with the objectives, are the risks where ERM should focus on by implementing internal control measures. The second step, create the proper work environment and culture, is about how people manage risk. Everyone has his own approach to risk management, but Agile ERM should ensure that the work environment and culture allow the right approach of managing risk. The third step, be pragmatic in managing risk, is about ensuring that all used frameworks and methods use the same terms. These frameworks and methods must be easy to apply and be designed to help people to respond quickly to the VUCA and inter-connected world. The fourth step, track the value added by risk management, is about measuring the value that is added by making use of risk management. The value of actions and internal control measures can be measured by the effectiveness of the risk management and the achievement of the objectives. The last step, continuously improve, is about insightful information of risks to make the right decisions with regard to risks, which enables continuously improvement. This can be done by making use of the enormous amount of data that is available.

Use in this research

As mentioned in section 2.3, internal control measures are needed to mitigate risks. This is recognized by COSO (2017), because they stated that internal control is one of the topics of risk management. This shows the importance of applying internal control measures within organisations. By implementing internal control measures correctly, the first step of ERM is already done. This makes it easier to make use of ERM after using the framework.

COSO (2017) also stated that stakeholders want to be more involved than before, due to the increase of VUCA. This shows even more why the stakeholders must be involved by designing the framework.

3. The framework

In this chapter the framework about Agile and internal control is presented. First, the requirements of the framework are described shortly. Next, the design of the framework is presented and the validation is discussed. This chapter supports in answering the corresponding research question of chapter 3, which can be found in section 1.2.

3.1 Requirements

While designing the framework, some requirements must be considered all the time. The requirements are: the framework must be modular, applicable on Agile companies, and the combination of Agile, internal control and stakeholders' needs must be present.

The first requirement, modularity, means that parts of the framework can easily be replaced. This requirement is important because this makes it easier to implement the framework at a specific company. If a company has specific stakeholders or departments, or is missing some specific parts, the company must still be able to use the framework.

The second requirement is that the framework must be applicable on companies that are using the Agile methodology. This research focuses on companies using the Agile methodology in combination with other requirements. So the Agile methodology must be a main component of the framework.

The third requirement is that the combination of Agile, internal control, and the needs of stakeholders is present. It must be possible to use the framework to discover the influence of internal control measures on the needs of stakeholders within an Agile environment. This includes the requirement that the needs of stakeholders must be clearly shown, so a quick analysis of the needs is possible.

3.2 Design

The Agile internal control framework should allow the combination of Agile, internal control and the needs of stakeholders. To combine different perspectives, the framework of COSO (2013) can be used. This COSO framework is shown in Figure 9. In this framework, all three sides of the cube present a different perspective, namely, objectives, components, and organisational structure. The relationship between these three sides is visualized by the cube (COSO, 2013). The Agile internal control framework that is designed to deliver an approach for the problem of this research can be seen in Figure 15, which shows similarities with the COSO framework.

On the top side of Figure 15, the standard stakeholders of a company can be found. The seven different type of stakeholders are defined according to the literature review, section 2.4. On the right side, three internal control categories are displayed. These categories are IT, financial and data. Employees of a business that falls within the scope came up with these categories during interviews. These categories are recognized by the literature review, and will be evaluated during the validation of the framework. The IT category is focused on all applications that are used or developed by the company. The financial category is focused on all financial transactions and documents. And the data category is focused on all data that is processed by the applications. On the left side, the steps of a standards Agile production process are depicted as derived from the section Standard steps of an Agile production process. The combination of Agile, internal control and the needs of their stakeholders is visualized in Figure 15.

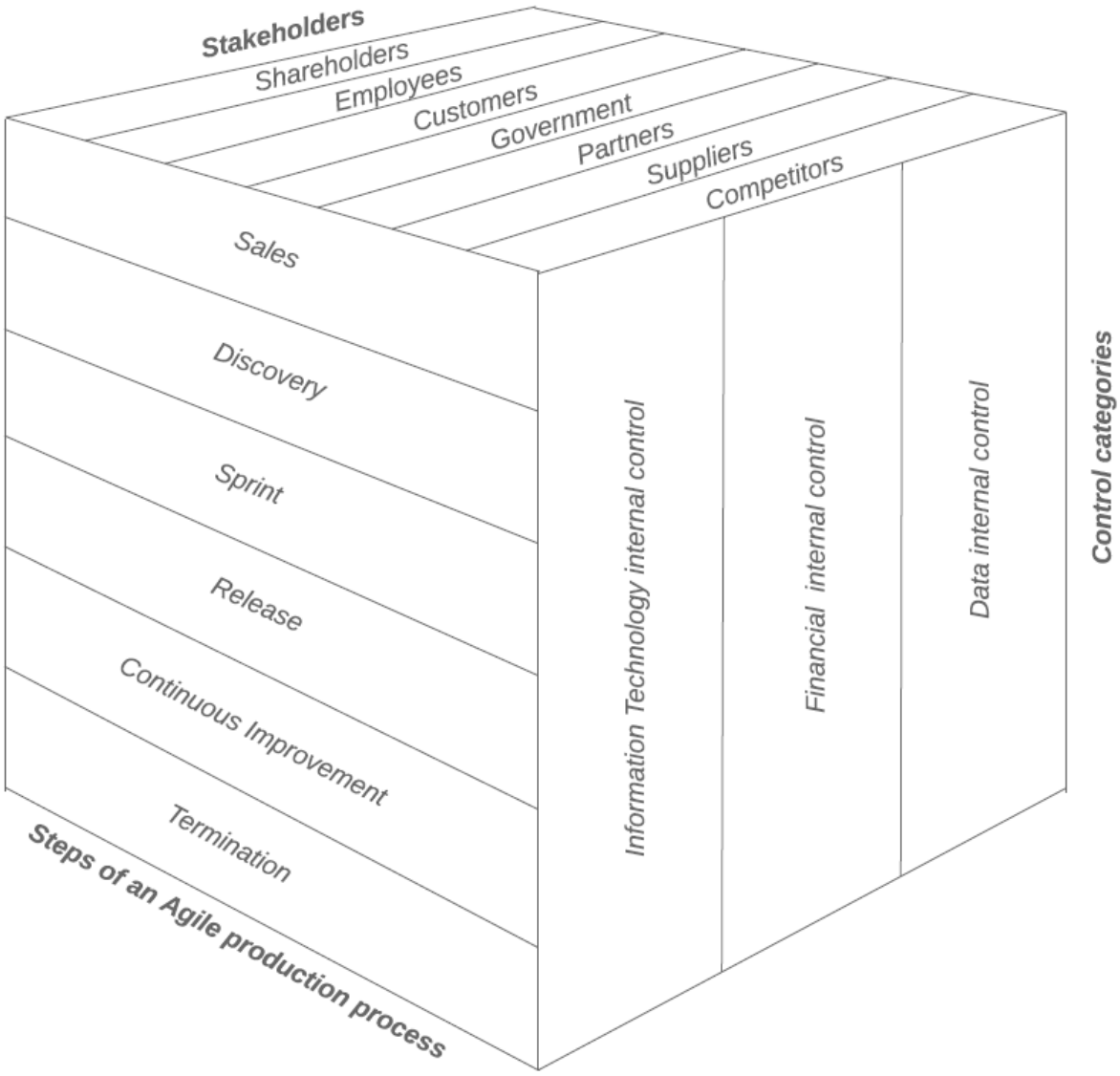


Figure 15: Agile internal control framework design

Figure 16 shows the view of a certain internal control category perspective. Appendix A shows a large version of this figure. This design is based on the design of the Zachman framework (1992). On the left side, the steps of an Agile production process are depicted. On top the standard stakeholders of a company are shown. In this figure, every cell will be filled with the needs of a specific stakeholder in a specific step of an Agile production process within a specific internal control category. If the whole framework will be applied at a company, every control category (IT, financial, and data) gets a perspective like Figure 16.

The rules of the Zachman framework (1992) as stated in section 2.5, are also used for the design of the Agile internal control framework. The first rule stated that there is no prioritisation of the columns. This rule is applied in the design of the Agile internal control framework, because there is no prioritisation within the internal control categories and the stakeholders. The importance of a certain category depends on the organisation, so the sequence of the control categories can be changed. There is also no prioritisation between the stakeholders, but they are divided as direct and indirect stakeholders. The direct stakeholders include the shareholders and employees. The indirect stakeholders are the customers, government, partners, suppliers, and competitors. The other rule that is used for the design of the framework is rule number 6. This rule stated that all cells in a row make

up a model for that specific perspective (Sowa & Zachman, 1992). This way of thinking is also important for the Agile internal control framework. All the cells of a particular row should make up the needs for all relevant stakeholders on a specific part of the Agile production process. This is needed when an internal control measure will be applied on the framework. The rest of the rules of the Zachman framework is not used in the design of the Agile internal control framework.

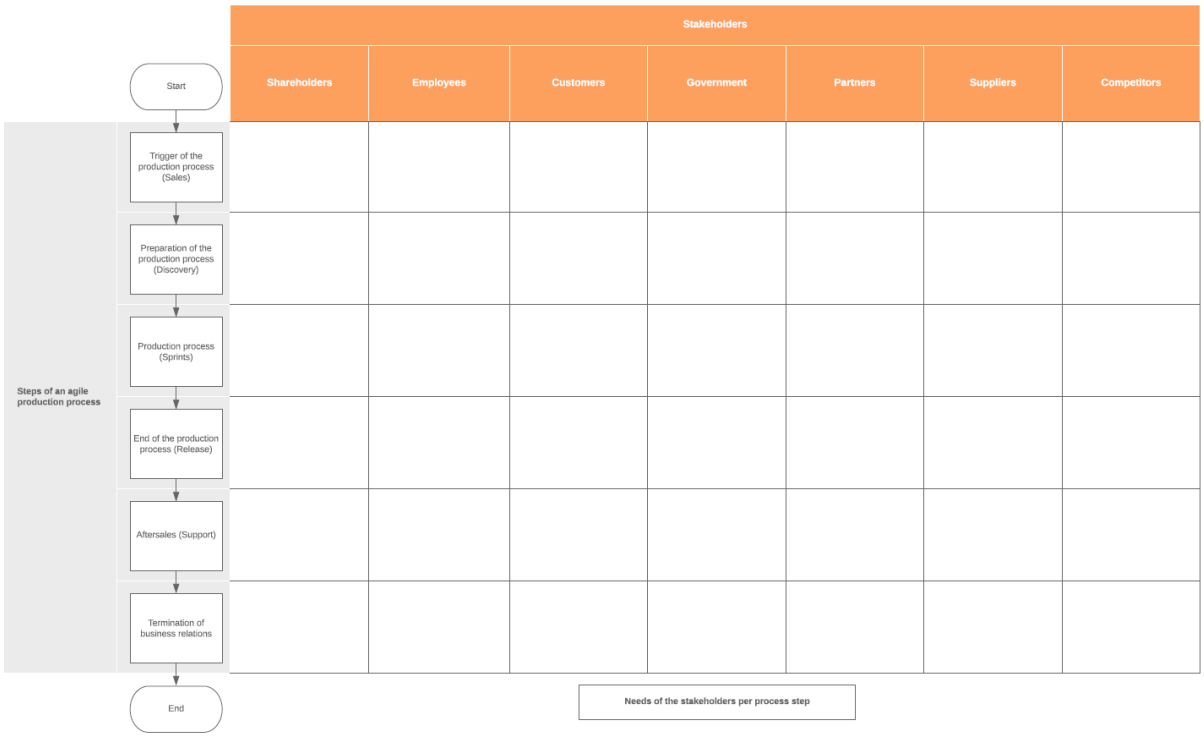


Figure 16: Agile internal control framework design: control category perspective

3.3 Validation

The performance of the framework is measured by using the UTAUT questions. These questions examine if the framework can be successfully implemented within CAPE Groep, and what the stakeholders' expectations are about the framework. This validation is executed in chapter 5. The stakeholders who were interviewed to gather information about the needs of the stakeholders, to map the processes correctly, and to gather the internal control measures, are also interviewed to validate if their needs are correct and what their opinion is about the framework.

Due to the chosen research design, it is not possible to validate the whole framework. So within this research, only a part of the framework is validated.

3.4 Conclusion

In this chapter, a framework is designed which must solve the problem as mentioned in section 1.1. The framework complies with the important requirements and the design is explained. Also, the use of literature is explained. The framework must be validated at a company that falls within the scope of this research to know if the framework will achieve his goal.

4. General implementation plan

This chapter includes the implementation plan for all companies that fit within the scope of the framework. First, the prerequisites are described before the framework can be used. In the next section, the use of the framework will be discussed. This contains all the steps of the framework. This chapter supports in answering the corresponding research question of chapter 4, which can be found in section 1.2.

4.1 Prerequisites

To be able to make use of the framework, context of the company is needed. The context of the company is needed for implementation of the framework within the company, so outsiders of the company are able to implement the framework. If an employee of the company wants to implement the framework, not all the information is necessary to gather. Namely, he knows how the company is working so some information is not needed.

The information about a company that is needed to use the framework depends on the company. Some suggestions are given, but per company should be evaluated which information is needed and available. The possible prerequisites are: a short introduction about the company, a Business Model Canvas (partners, customers, value proposition etc.), resources of the company, core processes, organisational structure, Agile and internal control within the organisation, and their stakeholders (who are probably already mentioned in the Business Model Canvas).

4.2 Use of the framework

This section explains how the framework should be used. The approach of the interviews is discussed, and how internal control measures can be placed within the framework.

Interviews

For every stakeholder that is considered during the implementation, at least one stakeholder must be interviewed, but preferably more. If more stakeholders from the same perspective are interviewed, the needs of that stakeholder will be more complete. It would be wise to interview stakeholders with different roles within the organisation. For example at the stakeholder 'Employees', a consultant, a team lead, a project manager, and a member from the Management Team can be interviewed. They will all have different needs which must be considered.

The stakeholders who must be considered when applying the framework depends on the company. Every stakeholder who is present at the company, must be considered. Every stakeholder has his own needs within the process, and they can all be affected by an internal control measure.

The sequence of conducting the interviews is also important. First, the stakeholders with most knowledge about internal control measures within the organisation must be interviewed. With this knowledge, the process maps can be completed and adjusted with internal control measures. Afterwards, the other stakeholders can be interviewed. The consultants know the most about the processes itself. They can give their opinion about the process maps and the shown internal control measures. They must describe what they think about the internal control measures that are depicted. Are the measures obstructive? Are the measures helping by achieving the goal of the measure (like mitigating a risk), or the goal of the process?

At the start of the interview, it must be gauged what the interviewee already knows about Agile and internal control. Some basic knowledge about Agile and internal control is needed to participate in the interviews. If the required information is not present, the interviewer should explain and provide the required information.

After that, the processes should be checked by the stakeholder. This contains improvements of the processes but also interpret and inform the stakeholder about the processes, because not all stakeholders will be aware of the exact processes. The internal control measures that are shown in the process maps will be discussed next. This is also the moment for the interviewee to tell about other internal control measures present at the company, and ask their opinion about these internal control measures. The last thing that is interesting to discuss in this part, is to ask if they know internal control measures which are not implemented at the moment at the company but could be beneficial.

Next, the needs of the stakeholder within that internal control procedure should be defined. This is the input for the control category perspective shown in Figure 16.

Applying internal control measures

The internal control measures that are discovered during the interviews must be shown in a clear overview. This overview must consists of the measure itself, but also the reason to use this internal control measure. This will help by defining the involved stakeholders, which is done in the next step of applying the framework. Every already existing and every new internal control measure must be applied on the framework.

Before an internal control measure can be applied on the framework, it must be defined at which step of the Agile process the measure will take place, which internal control category is applicable, and which stakeholders are involved. This is important because this will ensure that the right needs are taken into account. When the internal control category or categories are determined, the correct control category perspective(s) must be picked, like Figure 16. The needs of the involved stakeholders during the determined step of the Agile process must be considered now.

For every need and requirement within the scope, the impact of implementing an internal control measure must be determined. A consideration with all positive and negative impacts on the needs must be made. Accordingly, a conclusion must be drawn from the positive and negative impacts. If the weight of the positive impact is bigger than the weight of the negative impact, it can be a good idea to implement this internal control measure. But there is a lot of room for discussion at this moment. The importance of needs will be assessed differently by different people with different roles within the same organisation. The last step is that the employee responsible for implementing internal control measures decides if the measure must be implemented. Figure 17 gives an overview of the implementation method.

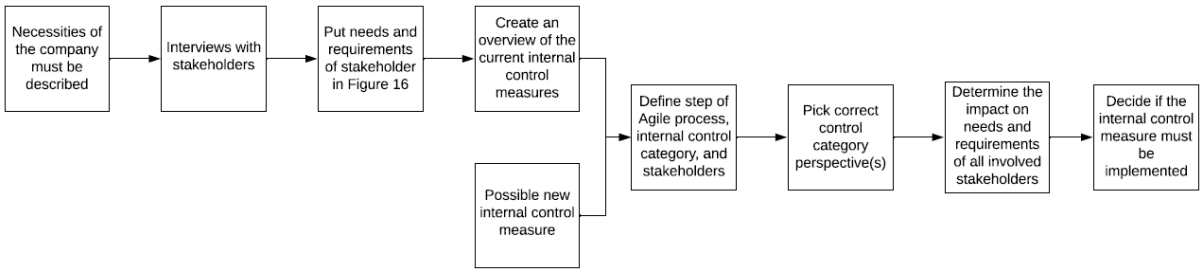


Figure 17: Implementation method of the framework

4.3 Conclusion

When a company wants to use the framework, it can make use of the implementation plan as described in this chapter. Chapter 5 shows how this implementation plan can be used in practice.

The goal of every internal control measure must be, of course, important. Implementing an internal control measure must always serve a goal. Not solving a problem, improving a process, mitigating a

risk, fulfils a need or requirement of a stakeholder etc., will never be a good idea. This is described by the principles of COSO in section 2.5. It is really important that this is always considered when using the framework.

5. Framework implementation at CAPE Groep

CAPE Groep is the company that introduced the problem of this research. This is the reason why the framework is implemented at CAPE Groep. In this chapter a detailed description of CAPE Groep's resources and processes is given to get more context about CAPE Groep. This chapter supports in answering the corresponding research question of chapter 5, which can be found in section 1.2.

5.1 Company introduction

CAPE Groep located in Enschede realizes digital innovation and transformation in construction and logistics (CAPE Groep, 2020). They see digital transformation as a strategic instrument for realizing business goals and delivering tailor-made applications and integrations. Digital transformation encompasses all business operations; from strategy to daily processes. At CAPE Groep, they transform strategic issues into clever and versatile solutions.

CAPE Groep is a SME which is growing fast during the last years. CAPE Groep is employing approximately 90 people at the moment. CAPE Groep produces low-code solutions build by business-oriented employees. The market consists of a lot of transactions due to high demand and high speed. With this high demand, fast company growth should be realized. CAPE Groep wants to keep growing and is ambitious to serve as many customers as possible, but it is hard to handle more customers now. In the current situation, there is room for improvement in the areas of the administrative organisation and internal control to support the core processes of the company. These areas satisfy the demands at the moment, but it will not be sufficient when the company keeps growing the coming years.

Collaboration is the key term on the website of CAPE Groep (CAPE Groep, 2020). They use collaboration with the customer to discover opportunities. Combining this with collaboration with students, they can get valuable insights and useful results. They also use collaboration with the customer to discuss the experience of previous projects, so they can choose the best technology for the new project. The delivered applications are practical, user-friendly and flexible, so the customer can understand and use the application. To improve the collaboration, CAPE Groep offers courses for customers if they are not able to handle the delivered application themselves and to get them more familiar with the used techniques. So, CAPE Groep is really customer oriented when customers are concerned.

5.2 Business Model Canvas

Osterwalder, Pigneur, & Clark (2010) defined a business model as the rationale of how an organization creates, delivers, and captures value. They created the Business Model Canvas which exists of 9 building blocks. Namely: Customer Segments, Value Proposition, Channels, Customer Relationships, Revenue Streams, Key Resources, Key activities, Key Partnerships, and Cost Structure. The Business Model Canvas of CAPE Groep is shown in Figure 18.

The Customer Segments show which customers CAPE Groep aims to reach and serve. The customers shown in the Business Model Canvas are retrieved from the website of CAPE Groep (CAPE Groep, 2020). The Value Propositions describe the products and services within CAPE Groep and eMagiz that create value for their customers. The Channels describe how CAPE Groep communicates with their customers to deliver value. The Customer Relationships describe the types of relationships with their customers. The Revenue Streams show what CAPE Groep earns by creating value for their customers. The Key Resources are the most important assets required to make a business model work. The Key Partners show the network of suppliers and partners that make the business model work. The last part is the Cost Structure, which describes all costs to operate the business model. These descriptions

are made with assistance of the book Business Model Generation (Osterwalder, Pigneur, & Clark, 2010).

The Cost Structure and Revenue Streams of CAPE Groep are classified and not shown in Figure 18.

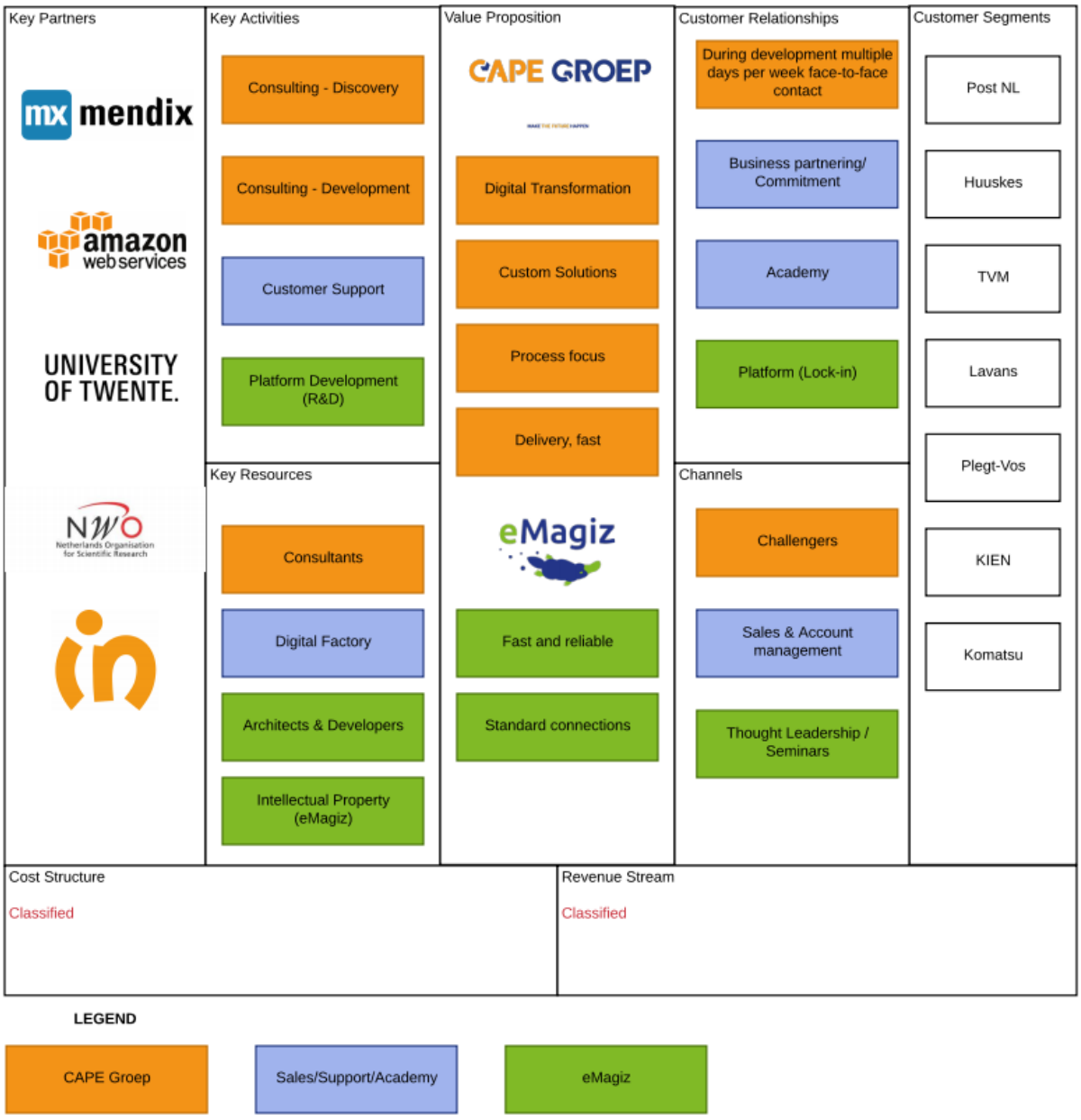


Figure 18: Business Model Canvas of CAPE Groep

5.3 IT software applications

This section gives a short overview of the most important IT software of CAPE Groep. The two most used IT software applications are Mendix and eMagiz. Power BI, PTV, and AWS are the other three IT software applications of CAPE Groep and are briefly described in this section. This information is retrieved from the website of CAPE Groep (CAPE Groep, 2020).

Mendix

Mendix is one of the two model-driven development platforms used at CAPE Groep. This platform is the foundation for dynamic and process-oriented customized applications. Mendix is the fastest and easiest low code development platform to build and continuously develop mobile and web

applications. CAPE Groep is a Mendix partner from the first hour. They are specialized in different areas like supply chain, logistics, construction and energy. With numerous certified consultants, they can deliver business critical applications at high speed.

Mendix is used at CAPE Groep to help the digital transformation of other organisations. They realize that by building functionalities that are not present in the standard applications, are unique and differentiating, or if a customer wants to experiment in the market and be able to quickly adapt.

eMagiz

eMagiz is the other model-driven development platform used at CAPE Groep. This platform is used to build integrations, conclude EDIs, host APIs and form ETL (extract, transform and load) processes. eMagiz is the fastest and simplest low code development platform to build and continuously develop integrations. Just like Mendix, CAPE Groep is a partner from the first hour and has already built more than 10,000 integrations. CAPE Groep can deliver critical integrations at an incredible pace thanks to a significant number of certified consultants.

eMagiz is used at CAPE Groep to aid the digital transformation of organisations. This process is performed by joint teams and at unprecedented speed at the offices of the client.

Others

Power BI, PTV, and AWS are the other three IT software applications at CAPE Groep. Power BI makes data easy to view on any device. It is also capable of making real time overviews to control the data with just one click. PTV is a planning software to schedule transport assignments in optimal tours taking all the relevant variables in mind. The last software application is AWS. AWS is a cloud platform with a significant amount of cloud services. These three software applications are not relevant for this research and are for that reason briefly described.

5.4 Core processes

In this section, the core processes of CAPE Groep are discussed. It starts with the standard production process, and second the DevOps production process.

Standard production process

The core business of CAPE Groep is digital transformation, the value creation of the company. The consultants work for other companies which pay CAPE Groep for their services and labour, and the finished products most of the time in Mendix. This is about half of the revenues of CAPE Groep. The other part is the resale of Mendix licenses and the sales of eMagiz applications, which arise from the consultancy work.

According to multiple employees of CAPE Groep, the consultancy process of CAPE Groep consists of five stages. These stages are Sales, Discovery, Sprints, Releases, and Support. These four stages can be recognized as the second till the fifth step of a standard Agile production process.

For mapping the processes of CAPE Groep, their standard format is used, SIPOC. Every letter stands for a part of the process. The S stands for Suppliers, the I for Inputs, the P for Process, the O for Outputs, and the C for Customers. Figure 20 shows the SIPOC process map of CAPE Groep. Below, every step of the process is discussed.

Before the consultants start their job, the Sales department makes the first contact with interesting businesses. They investigate if the business is capable for a digital transformation and how the process will look like. If the Sales employee decides at the go/no-go moment to proceed, a quotation for

Discovery will be made. Another output of the Discovery step is the business case made by the customer. Without a business case, CAPE Groep will not start the Discovery.

To start the next step, the quotation for Discovery must be signed by the customer and the business case must be finished. This is the required input for the Discovery. The employees who are executing the Discovery are the consultants (sometimes called: Professional Services) and they should make the demand of the customer clear. At the end of the Discovery, the Service Level Agreement (SLA) and the quotation for realisation are sent to the customer. The solution design and the acceptance criteria & test scenario's are available for the project team.

The next stage are the Sprints. To start with sprint 0, the solution design and the acceptance criteria & test scenario's are needed. Next to that, the customer must provide the signed quotation for realisation and the desired functionalities of the application. For every other sprint a plan of approach and user stories are needed.

In every sprint, the consultants work on a part of the solution. They work a couple of weeks on the solution during one sprint. At the end of every sprint, the results are discussed with the customer. A satisfying solution can be reached in that way, because the customer can give feedback on every new part. If something is not to the wishes of the customer, it can be changed before it is interwoven with the rest of the (upcoming) parts.

The output of sprint 0 are the user stories, a plan of approach and a product backlog. A revised quotation for realisation can be made if the Discovery showed that the first quotation for realisation is not realistic. This will also results in a revised solution design. The product backlog and the sprint backlog are a combination of inputs and outputs for the sprint process. The product backlog is the place where all required functionalities are kept. This is a combination of refined and unrefined functionalities. The sprint backlog consists of the refined functionalities for that sprint. The backlogs are only visualized as output in Figure 20, to reduce the complexity of the process map. The most important output of the sprint process is the increment. This is a combination of all the finished user stories and can be seen as the intermediate application.

After every sprint, the product will be released and a new sprint will start. The final sprint, sprint *n*, is the delivery of the final product in Mendix and/or eMagiz. This final sprint also ends with the last release. To be able to release the application, the increment of the sprint is needed as input, just like the acceptance criteria & test scenario's. One of the outputs of the release phase is a working application, which will be maintained and improved in the next step. Other output is the sales invoice, which must be forwarded to the customer.

Collaboration does not end after the final release. The customer and CAPE Groep keep collaborating on some aspects. The application needs preventive health checks, monitoring of the application, and it must be secure. Next to that, employees of the customer must be able to handle the application and make some small adjustments by themselves. CAPE Groep offers courses for these employees, so they become capable of using the application. If the application needs maintenance, it depends on the SLA how fast the maintenance can be done. Some customers have a 24/7 service, but they have to pay more than customers with a lower service level. The output of this step is a working application.

The last stage of a standard Agile production process is the termination. This stage shall be triggered if the customer or CAPE Groep wants to terminate the cooperation.

DevOps production process

The DevOps (software development and IT operations) production process is a little different than the standard production process. The biggest difference is that the customer do not demands a specific end product. The consultants are constantly developing new applications for the customer. While in the standard production process, the sprints are focused on delivering one application at the end (and intermediate applications at the end of every sprint). This difference does not change the process map, so the process map in Figure 20 is for the standard and the DevOps production process.

Figure 19 shows the legend of all process maps depicted in this thesis. The process maps in this thesis are Figure 20, Figure 26, and Figure 27.

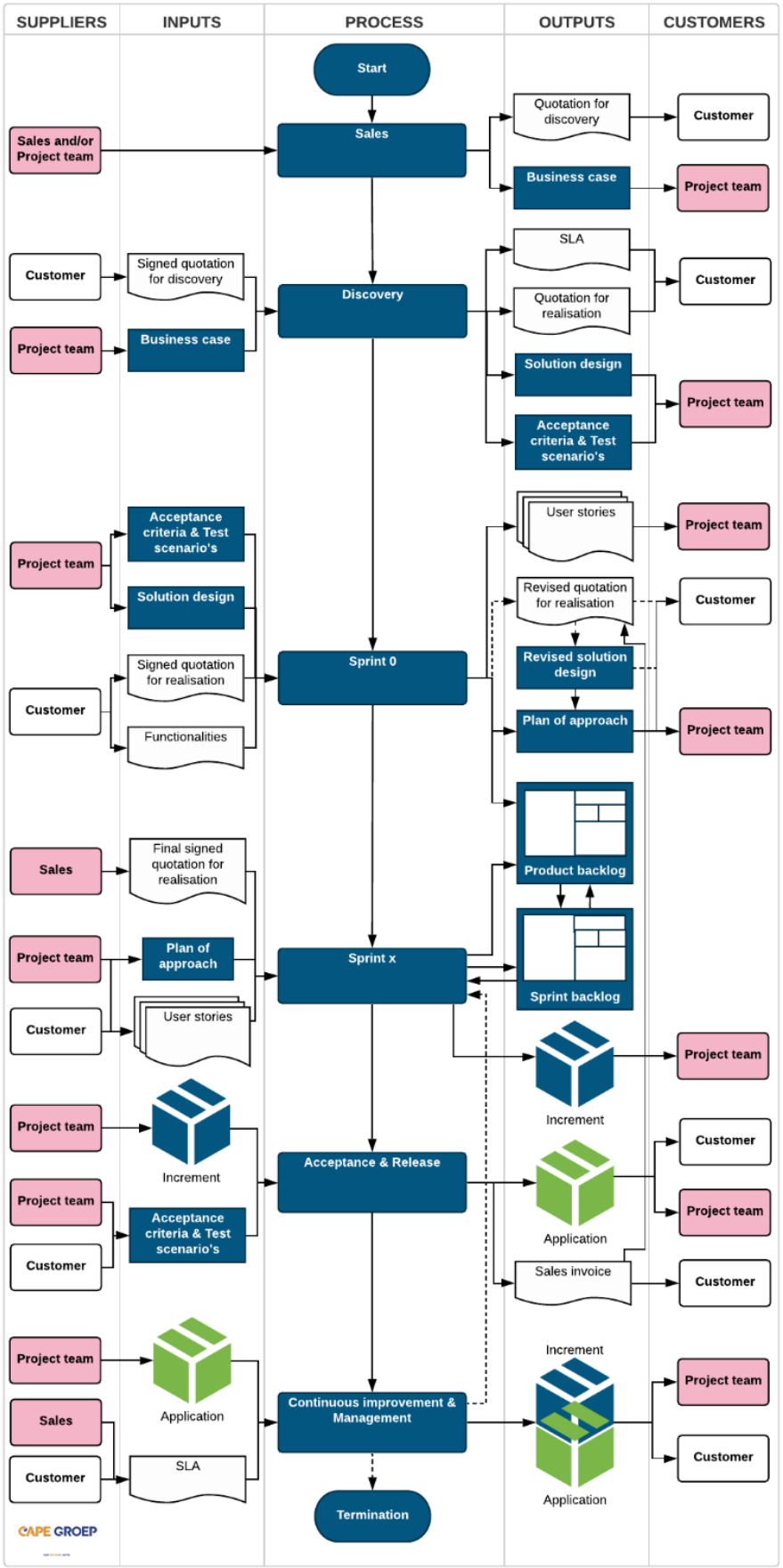


Figure 19: Legend of all process maps

Figure 20: Core process of CAPE Groep (derived from process maps of CAPE Groep, by N. Staman)

Organisational structure

There are four different categories of employees at CAPE Groep. The first category is the Management Team and consists of the CEO, the Business Controller, the Commercial Manager, the Manager Professional Services, and the Manager Customer Support. The second category consists of the Marketing and Communication Specialist, the Office Manager, and the Manager Information Security. The third group is an external/independent employee and is the trust person of CAPE Groep. The last group is eMagiz staff, including the CTO eMagiz. The hierarchy of these four groups is shown in Figure 21. The other employees are also placed in the organigram. The Product Manager eMagiz, eMagiz developers, and eMagiz Architects fall under the CTO eMagiz. The Sales Executives fall under the Commercial Manager. The Program Managers, Project Managers, Consultants, and Expert Services fall under the Manager Professional Services. Support Staff fall under the Manager Customer Support.

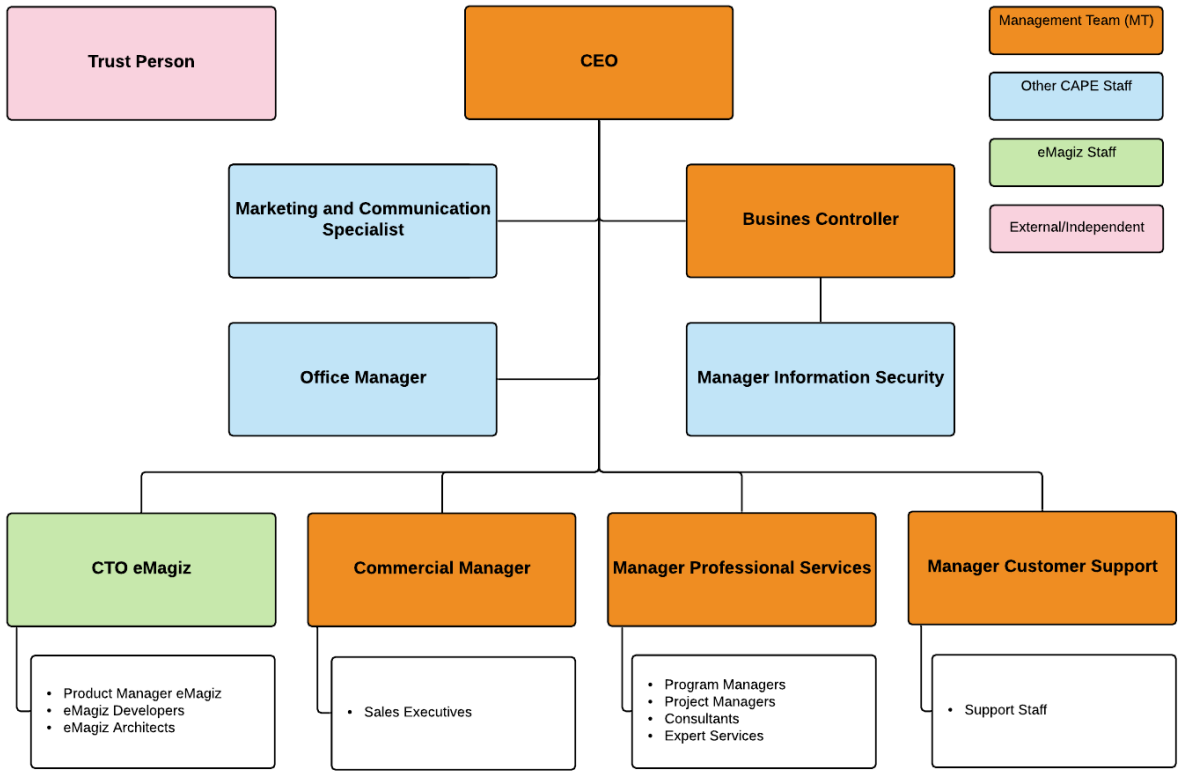


Figure 21: Organigram of CAPE Groep

5.5 CAPE Groep methodology - Big Mama

The views of Beck et al. (2001) stated in section Agile are also of great importance to CAPE Groep. The employees of CAPE Groep should ensure flexibility to maximize customer value. One of the ways CAPE Groep uses Agile methods is adapting the SCRUM framework. This is presented in Figure 5. Every two weeks a goal is set for that period. Depending on the project, the length of a sprint can change from two to four weeks. Also, a planning meeting, daily stand-ups, user stories, a unit test, a review/demo, a retrospective and refinement sessions are made for that specific sprint. After a sprint, a new sprint is defined with all the aforementioned aspects. These sprints should avoid big gaps between the intermediate product and the desired product in the end.

Agile is not the only method CAPE Groep is using. They developed a methodology by themselves which is called the Big Mama. The Big Mama takes the SCRUM process as a foundation, but integrates concepts, methods and techniques from PRINCE2, results-driven project management, Lean, Six

Sigma, best practices by practical experience, SDM (System Development Methodology), and IPM (integral project management).

5.6 Internal control

In this section, the security and privacy standards and other internal control methods which are used at CAPE Groep are discussed. This are the CAPE Information System, financial external audit, ISO 27001, and SOC 2. During the interviews, a lot of already existing and possible internal control measures are discussed. These are enumerated in section 5.10.

CAPE Groep Information System

CAPE Groep Information System (CIS) is the ERP system of CAPE Groep. Customer Relationship Management (CRM), hours registration, project control, and planning are included in CIS.

Financial external audit

Due to the growth of CAPE Groep, two of the three requirements as stated in section 2.6 Security and privacy standards are reached this year, so a financial external audit will be conducted for the first time at CAPE Groep. This financial external audit will be conducted by an accountant. This audit will also help by getting the SOC 2 certificate.

ISO 27001

ISO 27001 is the information security management standard which is used at CAPE Groep. This is the only ISO certificate that is used by CAPE Groep at the moment. This certificate ensures that CAPE Groep must comply with specific internal control measures, like describing the processes. Other ISO certificates can be easier achieved with a clear overview of all the internal control measures, because the certificates will demand proof of some internal control measures.

SOC 2

At the moment of writing, CAPE Groep is working on the implementation of SOC 2. Also for achieving a SOC 2 certificate, proof of some internal control measures must be provided. The found internal control measures during this research can help by achieving this certificate.

5.7 Stakeholders

The stakeholders of CAPE Groep can be labelled as direct and indirect stakeholders. The direct stakeholders are the stakeholders that are directly involved with the daily business. These are the shareholders and employees. The only shareholder of CAPE Groep is the CEO. During this research, the CEO is interviewed as a shareholder, and not as the CEO. There are no other shareholders or financiers of CAPE Groep. The indirect stakeholders are the customers, government, partners, suppliers, and competitors.

Shareholder

The only shareholder of CAPE Groep, the CEO, expects from CAPE Groep to be successful and profitable on the long term. To be so, CAPE Groep must ensure that they deliver, maintain, and manage secure solutions.

Employees

The stakeholder ‘Employees’ consists of a lot of different employees of CAPE Groep. The managers of the Management Team are included within this stakeholder, but also the Consultants are identified as this stakeholder. Everyone within the Organigram of CAPE Groep (Figure 21), excluding the CEO and the Trust Person, is identified as ‘Employees’.

Customers

The 'Customers' of CAPE Groep are companies that want to make use of digital transformation. Some of the customers are visualised in the Business Model Canvas, Figure 18. Some large companies expect that CAPE Groep complies with some security and privacy standards like: ISO 27001, SOC 2, and they want evidence of compliancy.

Government

Three important governmental bodies for CAPE Groep are: the Dutch Tax Agency (DTA), the Dutch Central Bank (DCB), and the Dutch Supervisory Authority (DSA). The DTA expects from CAPE Groep that the accounting is in order and that the timeliness, availability, and integrity of this data is high. Most of the customers of CAPE Groep are supervised by the DCB when concerning financial affairs. The compliance requirements coming with the supervision are mirrored on CAPE Groep, so CAPE Groep should also meet these requirements. The DSA demands compliance to the General Data Protection Regulation.

The stakeholder 'Government' also includes the governance side of CAPE Groep. These are the employees within CAPE Groep that must ensure that CAPE Groep is compliant with regulations, legislations, and security and privacy standards. These employees are the Information Security Manager and the Business Controller. Based on conversations with employees, it is expected that the needs of these employees fit better within the needs of the 'Government' stakeholder, than within the needs of the 'Employees' stakeholder.

Partners

CAPE Groep has two main partners, namely Mendix and the University of Twente. CAPE Groep is a big partner of Mendix so failures will damage CAPE Groep and Mendix. Mendix can also help CAPE Groep with the security of their applications, while Mendix can learn from CAPE Groep about situations in the field. The University of Twente is a partner of CAPE Groep because they work together by sharing research results and a lot of University of Twente students are working part time at CAPE Groep. More partners of CAPE Groep are shown in the Business Model Canvas of CAPE Groep in Figure 18, but they are not relevant to discuss.

Suppliers

Mendix is not only a partner of CAPE Groep, but it is also an external supplier of CAPE Groep. They supply the platform where CAPE Groep develop their applications. Another relevant supplier is eMagiz, which is an internal supplier of CAPE Groep. eMagiz is developed and supported by CAPE Groep itself, so delivering good work is important for CAPE Groep as supplier and recipient.

Competitors

Via a transparent and independently auditable way CAPE Groep can be in control of their information security and differentiate from their competitors.

5.8 Prototype

Figure 22 shows the specific problem that must be solved within CAPE Groep. This figure is designed with inspiration from the Zachman framework. Some of the interrogative words as used in Zachman can be found in this figure. The stakeholders are mentioned on top and are the *Who.* All these stakeholders have goals, which is the *Why*. The stakeholders have goals which must be achieved by executing processes, the *What.* The internal control measures must be applied efficiently and effectively, but these internal control measures can still conflict with the goals of the stakeholders. The friction is shown in Figure 22 by the lightning bolt between 'Goals' and 'Internal controls'. This situation must be improved by this research.

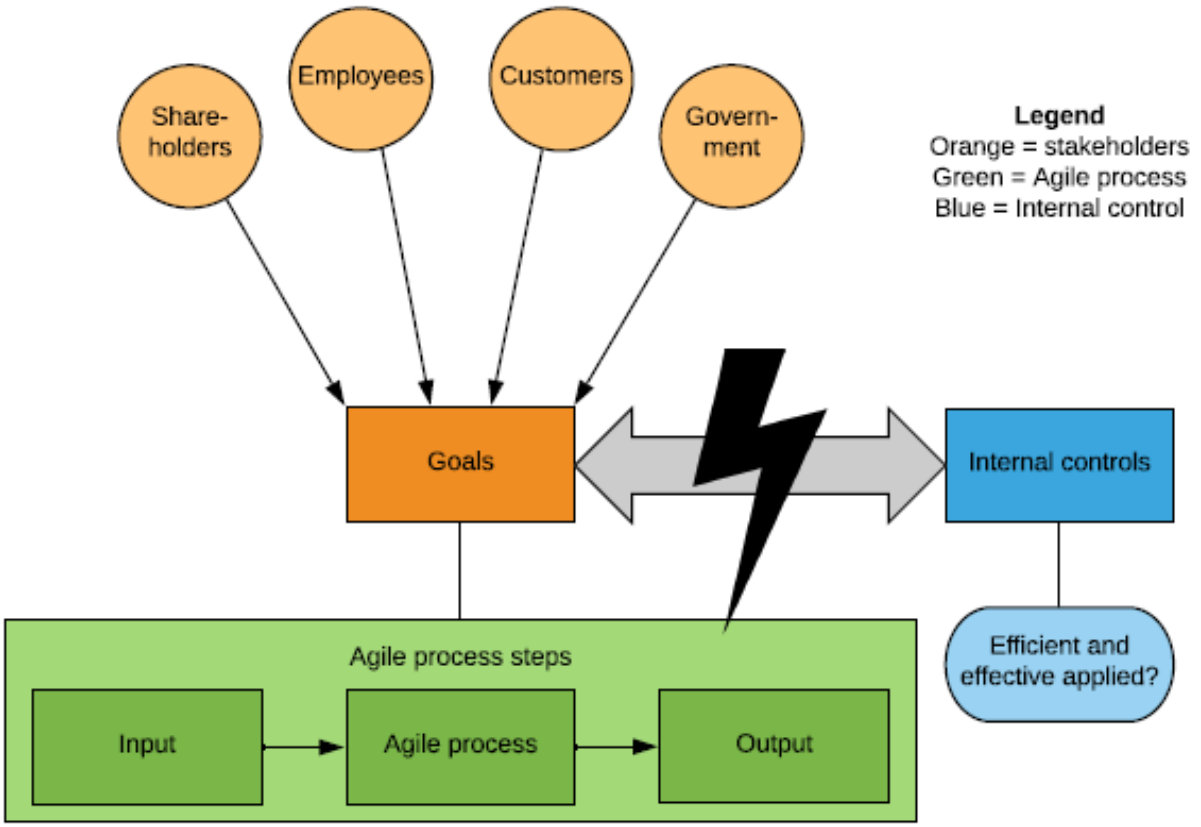


Figure 22: Problem to solve at CAPE Groep

As described in section 3.2, the importance of a particular internal control procedure depends on the organisation. After discussion with multiple CAPE Groep managers, the IT and financial internal control perspectives seems to be the most important categories for this organisation. The data internal control perspective is not used for the validation of the framework.

Also, not all stakeholders are considered for the validation of the framework. The most relevant stakeholders for this research are at least the direct stakeholders, so the 'CEO' and 'Employees'. The CEO is the only shareholder of CAPE Groep and he is a relevant stakeholder because a shareholder expects a company to be successful and profitable. If a company do not sufficiently comply with security and privacy standards, it will lose big customers or lose their license, which results in less profit. The CEO is not only shareholder, but also the owner of CAPE Groep. 'Employees' are relevant stakeholders because they have to work with internal control measures. They must know why they should do specific tasks regarding security and privacy standards and what the impact will be if they do not meet these tasks. Other relevant indirect stakeholders are the 'Customers' and the 'Government'. The 'Customers' are relevant for this research because they demand compliance to security and privacy, and some large customers demand compliance to specific standards. The 'Customers' are also effected by the quality of products. The 'Government' is a relevant stakeholder because they oblige CAPE Groep to comply with the regulations and legislation, for example GDPR.

Figure 23 marks the parts that are considered during this validation at CAPE Groep in the Agile internal control perspective. Figure 24 shows how the framework for validation at CAPE Groep looks like. Figure 25 shows the perspectives which will be filled by the validation at CAPE Groep. There will be a perspective focussing on the IT and one on the financial aspects.

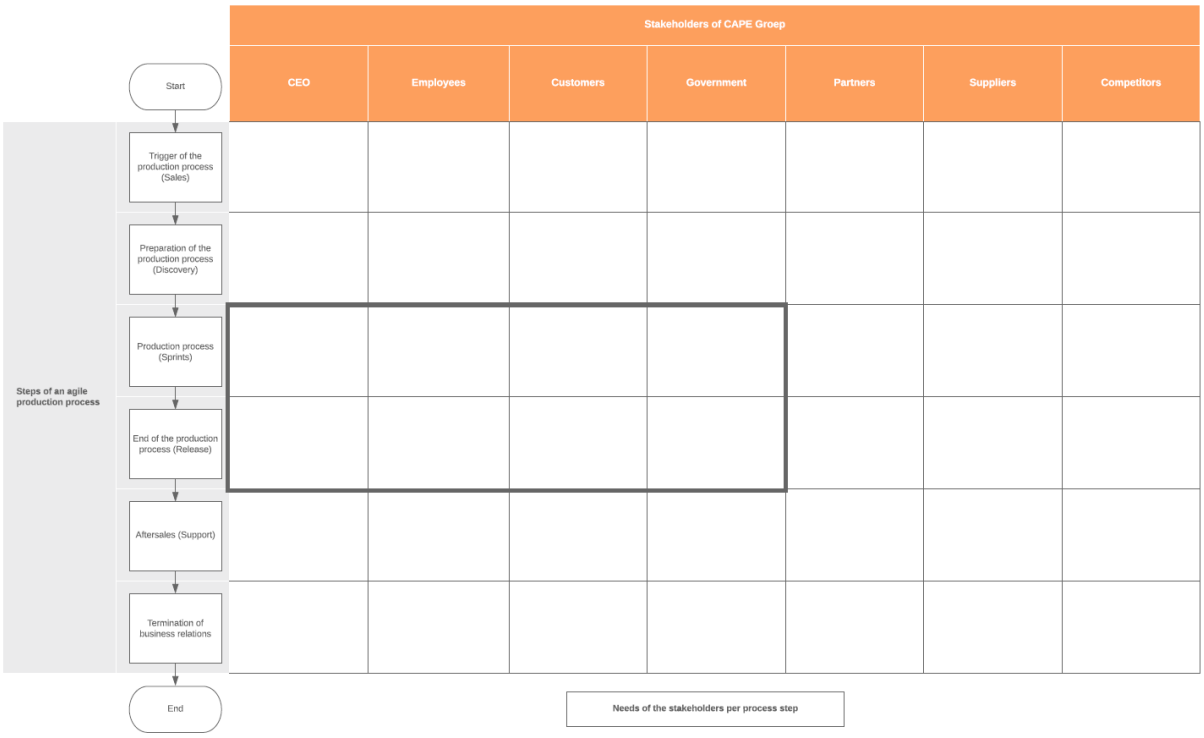


Figure 23: Marked Agile internal control framework perspective for validation at CAPE Groep

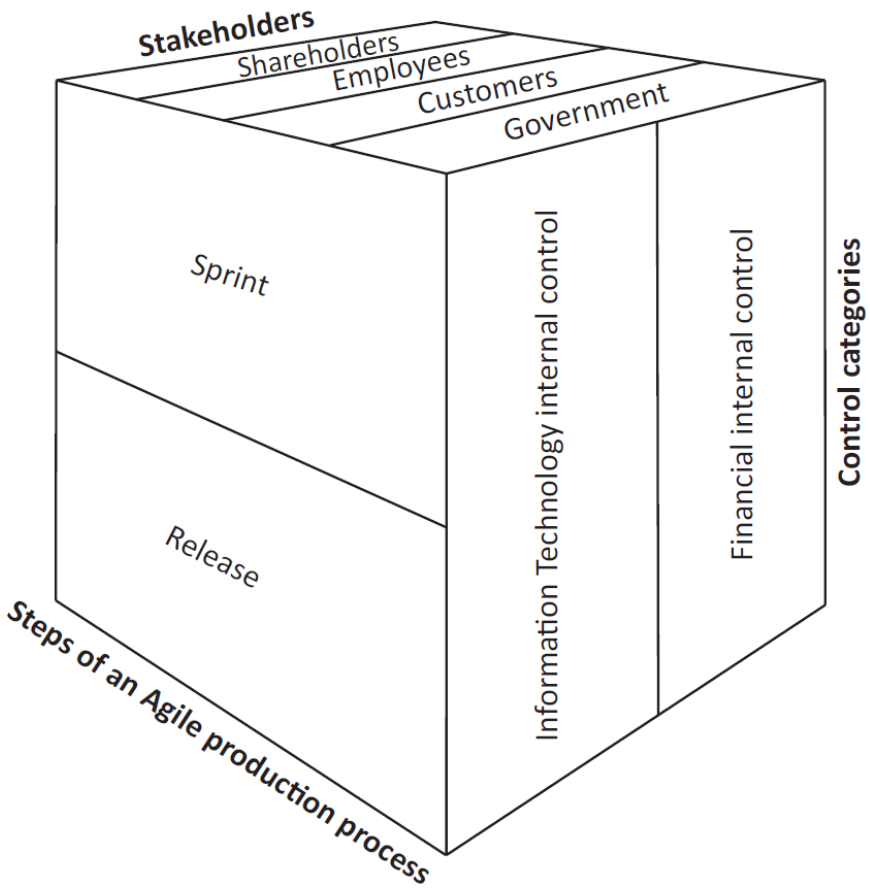


Figure 24: Agile internal control framework for validation at CAPE Groep

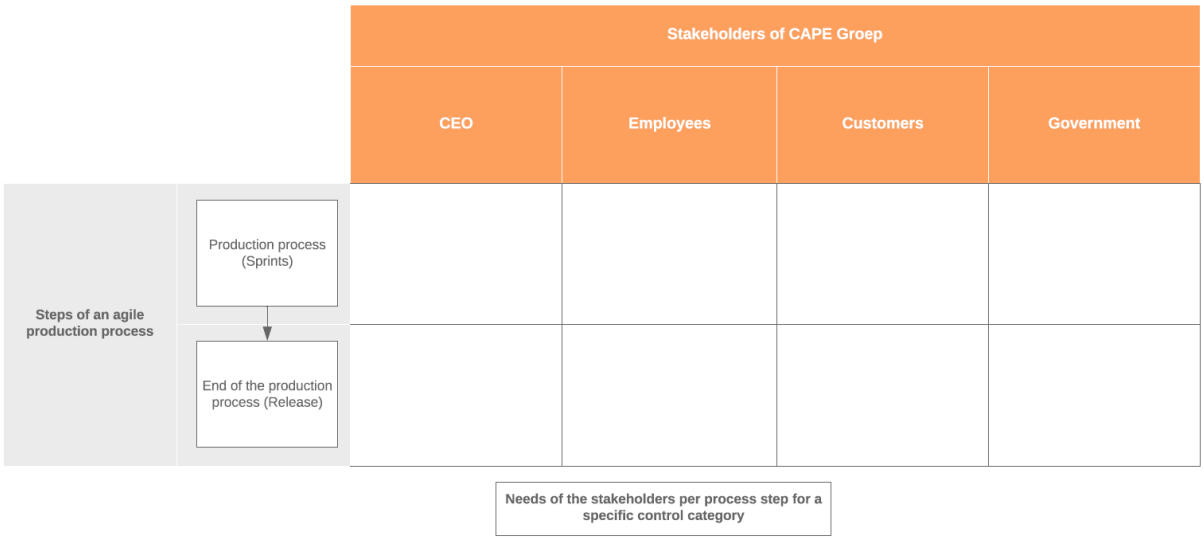


Figure 25: Part of the internal control framework that is validated at CAPE Groep

5.9 Interviews

Semi-structured interviews are held with employees of CAPE Groep so the framework can be applied on their environment. The interviews are held with: Manager Information Security, Consultant (Team lead), Commercial Manager, Financial Controller, CEO, Consultant, and Manager Customer Support. These employees are selected because of their ability to reflect the needs of the four stakeholders (CEO, Employees, Customers and Government), because of their involvement in specific projects or their working experience within CAPE Groep. The Manager Information Security is interviewed as 'Government', 'Customers' and 'Employees' stakeholder. He knows a lot about the needs of customers regarding to the security and privacy standards. The consultants as 'Employees' stakeholders. The Commercial Manager as 'Employees' and 'Customers' stakeholder, because he has a lot of experience with customers and knows their demands. The Financial Controller as 'Employees' and 'Government' stakeholder. The CEO as the 'Shareholders' and 'Customers' stakeholder. The Manager Customer Support as 'Employees' and 'Customers' stakeholder.

To get valuable results from the interviews, semi-structured interviews are used. These give valuable results, because specific information about processes, internal control, and Agile is needed, but the diversity between the interviewees is large so space for personal input is important. If a certain employee wants to tell more about a specific topic, there is the possibility in this type of interviews.

All interviews had the same structure. The interviews started with asking permission of the interviewee if the interview may be recorded. All interviewees agreed. Next, the goal of the research, Agile and internal control definitions, the framework, and the importance of this research/interview for that specific stakeholder are discussed. The last part of the interview was about the complete production process, the sprint process, and the release process, and the internal control measures within these processes.

Multiple questions were pre-determined and asked during all interviews:

- Is the process map complete?
- What are the current internal control measures within this process?
- Do these measures hinder your daily work?
- What internal control measures can be added within the process to mitigate important risks?

- What are the needs of the specific stakeholder at the sprint/release process, looking at the financial/IT perspective?

Some interviews contained pre-determined questions that were specific for that stakeholder.

The Information Security Manager got specific questions about ISO and SOC certificates:

- What are the influences of SOC and ISO certificates on the processes?
- What does SOC and ISO certificates say about the importance of process maps?

The CEO got a specific question about the stakeholders used in the framework:

- Are these stakeholders applicable to CAPE Groep?

The Consultant (Team lead) and Consultant got specific questions about the sprint process:

- How long does a sprint take at a project at Post NL?
- Is it allowed to deviate from the sprint planning?

The Manager Customer Support got specific questions about a transition moment in the process:

- Which internal control measures are used at the transition moment from Professional Services to Customer Support?

5.10 Analysis of interviews

The interviewees told a lot of internal control measures, more details about the process maps, and their needs within the process. The internal control measures and details about the process maps are shown in this section. The needs of stakeholders are shown in the next section, 5.11.

Internal control measures at CAPE Groep

The lists below show all the possible internal control measures for CAPE Groep per category. All these measures are mentioned by stakeholders during the stakeholder interviews. The categories are based on the mentioned measures during the interviews. Three of the four categories can be recognized as the internal control categories of the framework. The other category, Methodology, seems to be important according to the interviews. After describing an internal control measure, the risk that is mitigated with this measure is described.

The internal control measures per category are divided into already implemented internal control measures, and not yet implemented or inconsequently applied internal control measures. The already implemented internal control measures are the measures that are consequently applied by CAPE Groep. The not yet implemented or inconsequently applied measures are measures that CAPE Groep should use more consequently. Some of these measures are known by the employees but not used every time it is needed. These employees are not aware of the importance of those measures. The list with the measures must help CAPE Groep with creating awareness. These measures are ranked on importance. In the end, CAPE Groep must decide which measures are the most important for them and implement those first.

As described in section 2.5, COSO defined 17 important principles for effective internal control. CAPE Groep must comply with these principles to ensure that their internal control measures will be effective.

First, the management must ensure that CAPE Groep is a supportive environment for internal control measures. These control environment principles are not in scope of this research, because they are focused mainly on the organisation and the management. The last five principles, which are within the components information and communication, and monitoring activities, are also not in scope of this research. They are out of scope because they are focused on the organisation, and not on the internal control measures itself.

The principles within the second component focus on risk assessment. This includes specifying the objectives and identifying the corresponding risks. This step is really important because the internal control measures must be designed so they cover the risks and achieve the objectives. This is impossible if the objectives and risks are not correctly specified. The component control activities is also important. These principles ensure that you apply internal control measures if they contribute to the mitigation of risks, and that measures are doing what is expected.

Methodology

The first category is one that is not mentioned before as a possible category but mentioned a lot during the interviews, namely methodology. As stated previously, the methodology of CAPE Groep is the Big Mama.

Already implemented internal control measures

- Personal mentor. All just started employees have a personal mentor, who can help by contact with customers and other problems that happen especially to starters. This reduces the chance of mistakes while customers are directly involved, so customer satisfaction is not affected. (**Methodology**)
- Customer reports. Customer gains at the end of every sprint insights into the results of the Application Quality Monitor (AQM). This reduces the chance of disappointing results for customers in the end. (**Methodology**)
- Process improvement. A project team decides how many story points they want to dedicate to process improvements. The velocity should increase if the process improves. There must be a check if the velocity actually improves and how many improvement is achieved. An improved velocity will lead to the ability of handling more user stories in the same time. (**Methodology**)
- Contract for laptop, phone, etc. This contract should make clear if you can use it for private purposes. This reduces the chance of improper use of borrowed things. (**Methodology**)
- Project monitoring. Project monitoring is keeping track of all the metrics that are related to the project so the project is within scope and budget, and the deadlines are met. Progress reports are reports with these progress which are made every week. This reduces the chance of running out of scope and budget, and missing deadlines. (**Methodology/financial/IT**)
- Application Quality Monitor (AQM). AQM performs static analysis of Mendix applications. It provides a dashboard with quality ratings. This reduces the chance of low-quality applications, because CAPE Groep uses a minimum value of 4 (out of 5). Used at the moment at Post NL, but can possibly be used in all projects. (**Methodology/IT**)
- Human control. (**Methodology/financial/IT/data**)

Not yet implemented or inconsequently applied internal control measures

- Guideline/checklist with all possible tests. The acceptance and release process consists of testing the increment on certain aspects. The Team Lead decides on which aspects the increment will be tested. There is no guideline for the choice of the aspects. Developing a

guideline with all possible tests and when a certain test must be ran reduces the chance of applications that are not tested on the correct aspects. (**Methodology/IT**)

- Checklist and risk presentation every two sprints. This standard checklist and risk presentation for a release are only demanded by Customer Support at the first release. The application will not be accepted by Customer Support if the checklist or risk presentation is not sufficient. All upcoming releases do not require these checklists and risk presentations, while new releases can be totally different than the first one. Using the checklist and risk presentation every other sprint makes a release more reliable and makes the control not obstructive. (**Methodology**)
- Value delivering DevOps teams. DevOps teams do not have to deliver a specific application within a specific timeframe. They are just continuous developing an application, but they must deliver value all the time. A control must be developed to keep control of this process. This reduces the chance of DevOps teams not delivering value. (**Methodology**)
- Big Mama checklist. Develop a checklist to check if all the aspects of the Big Mama are included within the sprints and releases. Following the Big Mama is really important for CAPE Groep because they can rely on their methodology. If all employees are using the Big Mama aspects that are needed for a specific project (so specify this per project type, like DevOps), the chance of a successful project will increase. (**Methodology**)
- Comply with DoR criteria. Measure the percentage of stories which is accepted by the project team, but does not comply with the DoR criteria. Determine a minimum value for the percentage and determine a consequence if this value is too low. This consequence reduces the amount of wrong user stories (Not explainable in only one way? Not buildable? Not testable? Not complete?) ending up in the Sprint Planning, and finally ending up in the application with the wrong functionality. (**Methodology/IT**)
- Comply with DoD criteria. Measure the percentage of stories which is finished, but does not comply with the DoD criteria. Determine a minimum value for the percentage and determine a consequence if this value is too low. This reduces the chance of user stories which are not totally finished ending up in the application. (**Methodology**)
- Test loops. Check how many times a certain test loop is executed during the acceptance and release process. If a certain loop is executed every user story multiple times, something is going wrong on a specific part of building or testing, so CAPE Groep should take action. This action reduces the chance of errors during this certain test loop, so speeding up the process and reducing costs. (**Methodology/IT**)

Financial

The second category is the financial category. This is one of the categories presented in the framework.

Already implemented internal control measures

- Quotation monitoring. Project manager must monitor if the project will be completed within the budget, if there is some space for running late within the quotation, and if there are exclusions within the quotation. Monitoring this reduces the chance of problems at the end of the sprint when the customer must pay the invoice. (**Financial**)
- Hours registration. Hours should be registered strictly. Hours must be registered on user story and time. This reduces the chance of problems at the end of the sprint when the customer must pay the invoice because the customer gets a clear insight in the invoiced hours. (**Financial**)
- Declarations. Photo and description of the declaration are needed. This reduces the chance of employees trying to commit fraud. (**Financial**)
- Separation of duties. This means that at least two persons are needed for completing a task, like buying a expensive product. This reduces the chance of employees trying to commit fraud or to harm the company, and reduces the chance on errors. (**Financial**)

- Project monitoring. Project monitoring is keeping track of all the metrics that are related to the project so the project is within scope and budget, and the deadlines are met. Progress reports are reports with these progress which are made every week. This reduces the chance of running out of scope and budget, and missing deadlines. (**Methodology/financial/IT**)
- Human control. (**Methodology/financial/IT/data**)

Not yet implemented or inconsequently applied internal control measures

- Audit by an accountant. This internal control measure is an upcoming one for CAPE Groep this year. They are obliged that an account must check their financial state. Executing this internal control measure is not only obligated, but it also ensures that security and privacy standards are more easily achieved. (**Financial**)
- Velocity. Velocity says something about the collaboration and delivering value (the primary process of CAPE Groep). Check if the velocity company-wide is on the right level. If this is not the case, there is something structurally wrong, or there is a bottleneck in the process. An improved velocity will lead to the ability of handling more user stories in the same time. (**Financial/IT**)

IT

The third category is the IT category. This is also one of the categories presented in the framework.

Already implemented internal control measures

- Product Owner acceptance. Applications can only be released if the Product Owner of the customer accepted all finished user stories. This reduces the chance that a customer will be unsatisfied about the application, which is directly used at the customer. (**IT**)
- Pair programming. This means that at least two persons are needed for completing a task, like building and releasing a user story. This reduces the chance on errors within the application. (**IT**)
- Give Customer Support the responsibility to provide access rights. At this moment, CAPE Groep wants to implement this approach. With this approach, it is clear for all employees where they should go if they want to get access to a system for example. Customer Support can also document who they gave access and at what time. These measures reduce the chance of wrong access authorization and they can be in control of all current authorizations. (**IT**)
- Password policy. Employees/applications/customers/users must comply with some requirements if a password is created. This reduces the chance of hackers hacking the system/application. (**IT/security**)
- Access controls for releasing application. Only internal employees are authorized to release an application. This reduces the chance of wrong or low-quality releases. (**IT/security**)
- Project monitoring. Project monitoring is keeping track of all the metrics that are related to the project so the project is within scope and budget, and the deadlines are met. Progress reports are reports with these progress which are made every week. This reduces the chance of running out of scope and budget, and missing deadlines. (**Methodology/financial/IT**)
- Application Quality Monitor (AQM). AQM performs static analysis of Mendix applications. It provides a dashboard with quality ratings. This reduces the chance of low-quality applications, because CAPE Groep uses a minimum value of 4 (out of 5). Used at the moment at Post NL, but can possibly be used in all projects. (**Methodology/IT**)
- Information security by CIA. CIA stands for Confidentiality, Integrity, and Availability. Confidentiality is the set of rules that limits access to information. Integrity is the assurance that information is trustworthy and accurate. Availability is the guarantee of reliable access to

information by authorized people. This reduces the chance of information leaked to unauthorized people. (**IT/Security**)
- Human control. (**Methodology/financial/IT/data**)

Not yet implemented or inconsequently applied internal control measures

- Release checklist. Check if permission for releasing is given by the right person, if the most recent version is checked by the Product Owner, if all CAPE Groep requirements (testing, DoD, etc.) are executed, and if Customer Support is informed about the upcoming release. This reduces the chance of releasing an application while it is not ready at that moment, which will lead to more application maintenance. (**IT**)
- Application Quality Monitor (AQM). AQM performs static analysis of Mendix applications. It provides a dashboard with quality ratings. This reduces the chance of low-quality applications, because CAPE Groep uses a minimum value of 4 (out of 5). Used at the moment at Post NL, but can possibly be used in all projects. (**Methodology/IT**)
- Keep track of the applications that are tested and accepted. Measure how many applications need maintenance or are sent back to Customer Support with feedback within a particular timeframe (like two weeks) after releasing. Evaluate the results per project team and take action if a project team does not perform as expected. This reduces the chance of applications released need maintenance or are sent back to Customer Support with feedback, because the project teams will be made more aware of the value of delivering the application the first time right. (**IT**)
- How many times does an application needs maintenance at customer X with product type Y? If CAPE Groep can gain insight into which type of application needs maintenance most of the time, they can possibly prevent this need or anticipate that Customer Support will get this application back soon. CAPE Groep can also try to improve quality of applications that mostly need maintenance, so maintenance is less needed. (**IT**)
- Guideline/checklist with all possible tests. The acceptance and release process consists of testing the increment on certain aspects. The Team Lead decides on which aspects the increment will be tested. There is no guideline for the choice of the aspects. Developing a certain guideline reduces the chance of applications that are not tested on the correct aspects. (**Methodology/IT**)
- Workload Customer Support. Check if the workload for Customer Support is stable during the week or if there is a peak at the end of the week because all project teams release their applications at the end of the week. If there is a peak during the week, more communication between the project team and Customer Support is needed so the project team knows when it is best for Customer Support to release the application. This reduces the chance of longer waiting times before applications can be maintained or reduces the amount of overwork for Customer Support. (**IT**)
- Project team members access. A monthly check by the team lead if the access of employees within that project team is still correct. Who has access to specific files and information? Do they still need that access or should it be removed? This reduces the chance of employees trying to commit fraud, or the access for hackers if they hack the account of an employee. (**IT/data security**)
- Comply with DoR criteria. Measure the percentage of stories which is accepted by the project team, but does not comply with the DoR criteria. Determine a minimum value for the percentage and determine a consequence if this value is too low. This consequence reduces the amount of wrong user stories (Not explainable in only one way? Not buildable? Not testable? Not complete?) ending up in the Sprint Planning, and finally ending up in the application with the wrong functionality. (**Methodology/IT**)

- Finished product. The finished product can also be used as control on the quality. If the finished product is of good quality, the process of developing this product is sufficient. If the finished product is of low quality, the process must be improved. This reduces the chance of developing a low quality product. (**IT**)
- Test loops. Check how many times a certain test loop is executed during the acceptance and release process. If a certain loop is executed every user story multiple times, something is going wrong on a specific part of building or testing, so CAPE Groep should take action. This action reduces the chance of errors during this certain test loop, so speeding up the process and reducing costs. (**Methodology/IT**)
- Velocity. Velocity says something about the collaboration and delivering value (the primary process of CAPE Groep). Check if the velocity company-wide is on the right level. If this is not the case, there is something structurally wrong, or there is a bottleneck in the process. An improved velocity will lead to the ability of handling more user stories in the same time. (**Financial/IT**)

Data

The fourth category is the data category. This is also one of the categories presented in the framework, but this category is not further considered in the validation of the framework.

Already implemented internal control measures

- Data minimization, so less internal control on data is needed. Make fields in applications obliged if they are really needed. Otherwise, just remove the field or the obligation so people can decide by themselves if they want to provide the data. This reduces the chance of data leaks. (**Data**)
- Access controls for releasing application. Not all employees are authorized to release an application. This reduces the chance of wrong or low-quality releases. (**IT/data security**)
- Information security by CIA. CIA stands for Confidentiality, Integrity, and Availability. Confidentiality is the set of rules that limits access to information. Integrity is the assurance that information is trustworthy and accurate. Availability is the guarantee of reliable access to information by authorized people. This reduces the chance of information leaked to unauthorized people. (**IT/data security**)
- Human control. (**Methodology/financial/IT/data**)

Not yet implemented or inconsequently applied internal control measures

- Project team members access. A monthly check by the team lead if the access of employees within that project team is still correct. Who has access to specific files and information? Do they still need that access or should it be removed? This reduces the chance of employees trying to commit fraud, or the access for hackers if they hack the account of an employee. (**IT/data security**)
- The DoD includes security and privacy requirements. These security and privacy requirements must comply with the CAPE security policy, so CAPE Groep knows that the security and privacy requirements in the DoD are correct. (**Data security and privacy**)
- If data is processed, it must be registered in a report (data processing register) at the customer. At this moment, CAPE Groep do not check if the customer does this in the right way. It would be wise for CAPE Groep to ask the customer to share the report so it can be checked by CAPE Groep employees. (**Data**)

Human control

At all internal control categories, human control is an already implemented internal control measure at CAPE Groep. As described in section 2.3, the beliefs systems must communicate the core values and inspire all employees to do their best for the organisation. The core values ensure that all employees know how they must act within the organisation, so employees can correct another employee if needed. This also counts for the other three control levers. Employees know how they should do their job, so they can correct colleagues if they do not comply with standards of the organisation.

Process maps

The interviews focused mainly on the sprint and the acceptance & release processes. These were not mapped at the moment at CAPE Groep. More specified process maps are needed because these process maps can show where internal control measures are already implemented, and where the measures can be implemented easily. This will make it easier to decide where a specific measure should be used.

Sprint process

The sprint process in Figure 26 is a zoomed-in version of the main process of CAPE Groep, shown in Figure 20. Figure 26 focusses especially on the process during a sprint. A sprint at CAPE Groep takes usually two weeks. Every week starts with a refinement session. After the first refinement session, the sprint planning for the coming two weeks will be made. All the working days starts with a daily stand-up or daily scrum. The rest of the day, the consultants will work on the application. When the application is finished, the employee will test the application by himself. Next, the application will be peer tested by a colleague. The final test will be executed by the Product Owner. If the Product Owner approves the application or changes that are made, documentation about the application must be made by the CAPE Groep employee. If one of the tests fails, the application will go back to the developer, and the application must be fixed by him. This developing and testing cycle will continue every day after the daily stand-up.

At the beginning of the second week, a new refinement session will take place. In contrast to the first week, the sprint planning will not be the next step. The sprint planning is only made in the first week, because it is a 2-week planning. The production process is the same as the first week. At the end of the second week, a sprint review and a sprint retrospective will take place. Afterwards, the increment will go to the acceptance & release process.

Some internal control measures can be found in the process map. Product Owner acceptance and pair programming are two measures which can be found in the sprint process map.

Some of the internal control measures cannot be found in the process map, because they are performed continuously during the sprints. Two example of these measures are: Project monitoring (during the project) and AQM (during building). Other internal control measures cannot be found in the process map because they are defined on a lower level than the process map. An example of this is human control. Human control can be found across the whole organisation and is interwoven with the low level processes.

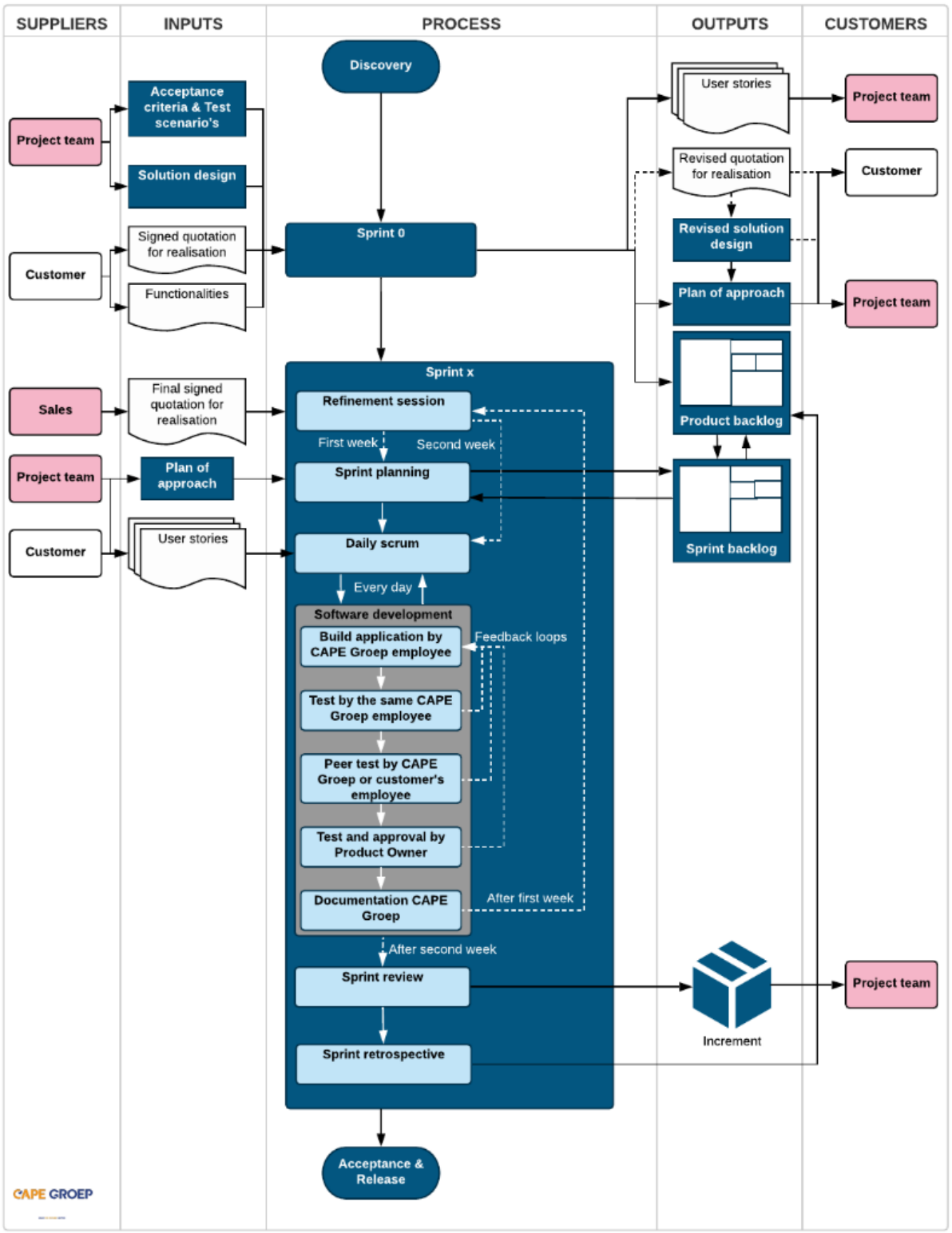


Figure 26: Sprint process (derived from process maps of CAPE Groep, by N. Staman)

Acceptance and release process

The interviewees explained a lot of tests that can be performed at CAPE Groep. Three types of testing are executed during the sprint process, namely, self-testing (directly after building), peer-testing (after builder put it through), and tester-testing (at large projects, after peer-tester put it through). At these three types of tests, it is clear that they all must be executed (at large projects) and at what point of time. A lot of other types of testing are available at which it is unclear when they should be used. This depends on the demands of the customer and if the Team Lead decides if it is needed or not.

All the other types of testing within CAPE Groep are enumerated below:

- Acceptance testing: executed directly after building the application.
- Unit testing: done after every sprint and tests just a small part of a functionality. A piece of code is written where yes or no will be the result, on the basis of 1 till X variables or a microflow. Unit testing is only done if a customer request this. Building unit tests take time but will recoup during the project.
- Integration testing: testing the cohesion between single units.
- Performance/load testing: tests if the application will keep working with a high amount of messages. This test must be performed multiple times, at least after the integration testing.
- Regression testing: tests all important functionalities together.
- Automated testing: testing with certain values without human actions. Automated testing can be used with regression testing.
- Chain testing: can be used when working with microservices. This test ensures that the input and output are right. The bigger the project, the more important chain testing becomes.
- User load testing: tests if the application will keep working with a high amount of users.

A guideline should be developed for the decision about the different types of testing, as described in section 5.10 as: guideline/checklist with all possible tests. This measure will lead to a lower amount of applications sent back with feedback after releasing.

The guideline that must be developed fits within the current process of CAPE Groep, as can be seen in Figure 27. An undefined amount of tests are ran during the Acceptance & Release phase. If the test failed, the feedback must be processed and a new release will be created. If the test succeeded, the next test must be executed. This process stops when all tests, which are needed, are executed. Before the increment will be released and will become an application, the standard checklist and risk presentation must be made and discussed with Customer Support.

The guideline and the standard checklist & risk presentation are two examples of internal control measures within the process map.

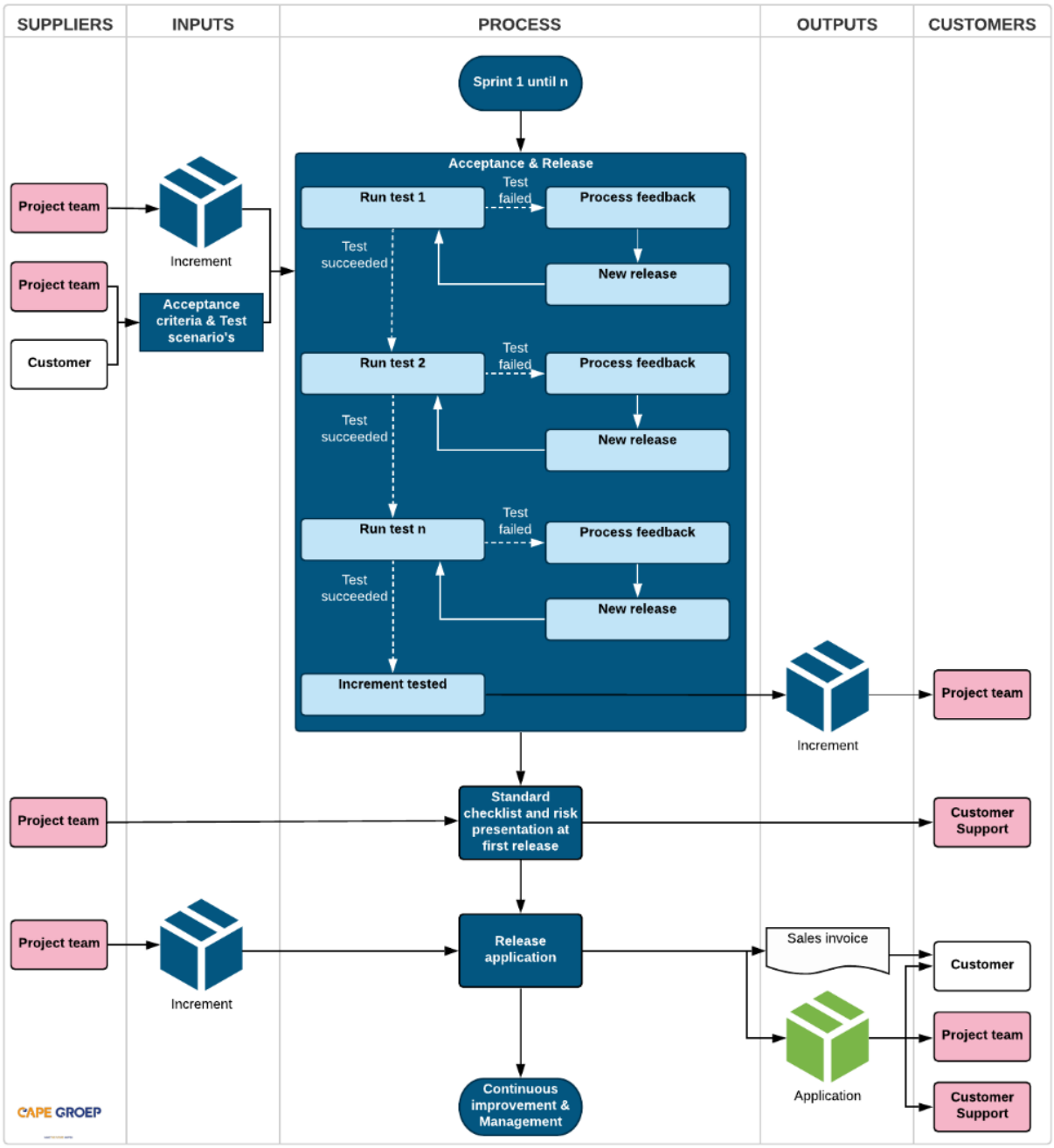


Figure 27: Acceptance & Release process (derived from process maps of CAPE Groep, by N. Staman)

5.11 Filled framework

This section contains two filled framework perspectives and two internal control measures placed in the framework.

Filled framework perspectives

During the interviews, the stakeholders explained their needs within the IT and financial perspective. The needs are visualized in Figure 28 and Figure 29. The needs of the stakeholder 'Government' also includes the needs of the Information Security Manager. These are closely related to the needs of the 'Government'. The needs are validated by showing the filled frameworks during the validation interviews.

The needs of the CEO are focused on the customer. The CEO wants that the customer is satisfied with the end result and that the customer is willing to pay the invoice at the end. There are no big differences between the financial and IT perspective for the needs of the CEO.

There is just a little amount of needs from the employees at the financial perspective. It is only important for the employees that the project manager keeps track of the forecast to complete, so the employees do not need to focus on the financial aspects. Other financial needs are not mentioned by the employees. From the IT perspective, there are more needs from the employees. These are mostly focused on the user stories, the parts of the Big Mama which focus on building applications, and releasing the application. This shows that the employees are focused on delivering a good end product by following the CAPE Groep methodology.

The financial perspective for the customer is about clarity and predictability. The customer wants to know what the costs will be, and they want to be able to track if CAPE Groep can produce the product for these costs. In the end, the customer wants a product as promised during the Discovery. This is also where the IT perspective of customers is focussing on. Customers want an application that is secure as possible and the end product must be working with the right functionalities.

The most important thing for the government stakeholder is that processes are described in the right way and executed well. This is mainly based on the interviews with the Manager Information Security. Describing the processes is also needed for getting certain certificates, like SOC and ISO.

There are a lot of differences between the needs of the different stakeholders. This is not a strange result, because all the stakeholders have different goals within the production process.

		Stakeholders of CAPE Groep			
		CEO	**Employees**	**Customers**	**Government**
Steps of an agile production process	Production process (Sprints)	Acceptable costs. Within reasonable time. All hours must be registered correctly. Met customer expectations and maximize customer value.	Project manager must keep track of the forecast to complete.	Clarity about costs and predictability. Transparency in production process. Effective and efficient production process so costs are reduced.	Process is described and executed well.
	End of the production process (Release)	Deliver what the customer expects, so the customer is willing to pay the invoice.	-	Get what CAPE Groep promised during the discovery in the quotation.	Process is described and executed well.

Financial internal control perspective.
Needs of the stakeholders per process step.

Figure 28: Financial internal control perspective

		Stakeholders of CAPE Groep			
		CEO	**Employees**	**Customers**	**Government**
Steps of an agile production process	Production process (Sprints)	Qualitative product. Met customer expectations and maximize customer value.	There must be sufficient amount of refined user stories in the backlog. User stories must be explainable in one way, buildable, testable and complete. Follow the Big Mama methodology. Internal control measure should not be obstructive.	Application must be secure. Transparency in production process.	Process is described and executed well.
	End of the production process (Release)	Met customer expectations and maximise customer value.	Follow the Big Mama methodology. Checklist must be filled before application is released. High quality of testing.	Permission must be given before releasing an application. Application must be secure. Working product with the right functionalities.	Process is described and executed well. Acceptance of Product Owner of most recent version is recorded.

IT internal control perspective.
Needs of the stakeholders per process step.

Figure 29: IT internal control perspective

Internal control measures placed in the framework

As explained in section 4.2, an internal control measure can be applied on the framework when the measure and the mitigated risks are clearly described. For every measure, it must be defined at which step of the Agile process the measure will take place, which internal control category is applicable, and which stakeholders are involved. Next, the correct control category perspective(s) must be chosen. The following step is to determine the impact for the needs of the stakeholders. The last step is that the employee responsible for implementing internal control measures decides if the measure will be implemented.

Application Quality Monitor

The first internal control measure that is applied on the framework is: Application Quality Monitor (AQM). As explained before, AQM performs static analysis of Mendix applications. It provides a dashboard with quality ratings. This reduces the chance of low-quality applications, because CAPE Groep uses a minimum value of 4 (out of 5). Afterwards, customer reports are created with the results of AQM.

All stakeholders are involved at this internal control measure, except Government. The CEO is involved because this method helps by achieving higher quality, which results in higher customer value. The Employees are involved because they are building the application. The Customers are involved because they will receive an application of higher quality. The Government is not involved because there are no security or privacy standards involved, and the processes are not part of AQM. This measure is present in the IT perspective during the sprints. Because of the costs of using AQM, the financial category is also important. Next, it must be checked if this internal control measure fits within the needs of the involved stakeholders.

The needs of the CEO are a qualitative product and meeting the customer expectations. This internal control measure will help by achieving this, because the application is monitored on his quality and the customer gets insight in the application. This will help by maximizing the customer value.

This internal control measure will not help by achieving the needs of the employees, but this measure does also not hinder achieving these needs. It is not obstructive because AQM is running automatically.

The needs of the customers will be achieved by this internal control measure. The quality of the security of the application will be higher because AQM checks if the quality of all parts of the application is right. There is also more transparency in the production process because the customers get insights into the results of the AQM.

So, this internal control measure achieves his goal and does not feel obstructive for the other stakeholders. If CAPE Groep thinks that the risk can be mitigated with this measure, they should decide if it is worth the money. CAPE Groep also must decide if they will use AQM at all customers, and if all the costs of AQM are passed on to the customers. This is possibly not necessary, because higher quality of applications will lead to a lower amount of applications needing maintenance. This will decrease the maintaining time of CAPE Groep, so they will earn their money (partly) back.

Give Customer Support the responsibility to provide access rights

The second internal control that is applied on the framework is: give Customer Support the responsibility to provide access rights. As described before, CAPE Groep wants to implement this approach at the moment. With this approach, it is clear for all employees where they should go if they want to get access to a system for example. Customer Support can also document who they gave

access and at what time. These measures reduce the chance of wrong access authorization and they can be in control of all current authorizations.

The only stakeholder that is involved is the Employees. The CEO, Customers and Government will not be involved when Customer Support is the only one who can give access rights. The Employees are involved, because they are the ones that will demand the access rights and they must provide the access rights.

The only needs that must be considered are those of the Employees, because they are the only stakeholder involved. This measure is present in the IT perspective during the whole process. Next, it must be checked if this internal control measure fits within the needs of the involved stakeholder.

The only need and requirement within the sprints and releases which is affected by this measure is that an internal control measure should not be obstructive. The biggest problem of this internal control measure is that it will be obstructive for executing personnel. In the old situation, an employee must ask a Team Lead to provide access, which can be done easily and fast. In the new situation, an employee must go to Customer Support. This will be obstructive for the employee because Customer Support is more difficult to reach than their Team Lead. Also, it will be obstructive for Customer Support, because they get an extra task to execute.

The internal control measure has, of course, objectives that it must achieve. It should prevent access rights given to the wrong person if that person did not really need specific access. It will also prevent that employees get too much access rights. Most of the time, employees do not need all possible access rights but only a small part. It also provides a clear overview of all the given access rights.

As been made clear, this internal control measure will be obstructive for a lot of employees, but it can achieve important objectives for CAPE Groep. CAPE Groep must assess if implementing this internal control measure is the right choice while not complying with the needs of a lot of stakeholders. This obstructive measure will take time, which results in costs.

Another possible internal control measure to mitigate these risks can be to give the responsibility to provide access rights to the Team Lead, just like the current situation. Different to the current situation, the Team Lead should be informed better about providing access rights and they must record who demands specific access rights. Instead of Customer Support, the Team Lead will experience the obstruction, but the other employees will no longer experience this obstruction. This will results in a better situation because less people will experience obstructions.

Use of the framework for every interviewee

This section describes how the involved stakeholders can make use of the framework. One new stakeholder pops up, namely the Business Controller. He was closely related to this research, and his feedback is continuously used during this research. This is the reason why the Business Controller is considered here, while there was no specific interview with him.

Business Controller

The Business Controller will most likely be the main user of the framework. All stakeholders want that their own needs are fulfilled. The Business Controller must ensure that the amount of fulfilled important needs of all stakeholders is maximized. The framework will help him by showing the different perspectives of all stakeholders.

The framework can also be used to place all internal control measures in their own spot. If all measures are in place, the connection between different measures can be easily shown. These measures can

cover the same needs. The framework can also show the overlap of a measure with multiple internal control categories. This can help the Business Controller by creating a clear overview, and use this for creating insights for other stakeholders.

Manager Information Security

The Manager Information Security can use the framework to check if all important aspects are included in the decision making of applying a specific internal control measure. Are all involved stakeholders included? Are the right categories included? The framework gives an overview of all the stakeholders and their needs, and the possible categories. Especially the combination of all needs of different stakeholders must help the Manager Information Security by making the right choice of implementing a new internal control measure.

Consultants

The framework should give insight why an internal control measure is implemented at CAPE Groep. The measure is implemented to serve a need of a stakeholder, or to mitigate a risk. When a measure feels obstructive for employees, the framework can help by showing the needs of other stakeholders which are pleased by implementing the measure.

The framework also gives consultants the chance to come up with internal control measures by themselves. The framework provides the needs of all stakeholders. If they notice that an internal control measure could improve a situation, like a part of the process or a need or requirement of a stakeholder, they can already guess the impact on the needs of the stakeholders. If the impact will be negatively and high, the idea will most likely not be accepted.

The third possibility to use the framework as Consultant is by getting insight in the amount of internal control measures. If a small part of the process contains a lot of internal control measures within one control category, it would probably wise to decrease the amount of measures by combining or removing measures. The Business Controller will recognize and solve this problem. This will have indirect and positive effects for the Consultants.

Commercial Manager

The Commercial Manager can use the framework to check if financial internal control measures fits within the needs of the stakeholders. Are all involved stakeholders included? Are the right categories included? The framework gives an overview of all the stakeholders and their needs, and the possible categories. Especially the combination of all needs of different stakeholders must help the Commercial Manager by making the right choice of implementing a new internal control measure.

Financial Controller

The Financial Controller can use the framework to check if financial internal control measures fits within the needs of the stakeholders. Are all involved stakeholders included? Are the right categories included? The framework gives an overview of all the stakeholders and their needs, and the possible categories. Especially the combination of all needs of different stakeholders must help the Financial Controller by making the right choice of implementing a new internal control measure.

CEO

The CEO will not use the framework by himself. By using this framework within CAPE Groep, it can be ensured that his needs are considered when needed. The framework also ensures that all needs of the other stakeholders are considered. As CEO, it must be important that all stakeholders are satisfied, so the effort of all stakeholders is maximized.

Manager Customer Support

The Manager Customer Support can use the framework to check if all important aspects are included in the decision making of applying a specific internal control measure. Are all involved stakeholders included? Are the right categories included? The framework gives an overview of all the stakeholders and their needs, and the possible categories. Especially the combination of all needs of different stakeholders must help the Manager Customer Support by making the right choice of implementing a new internal control measure.

5.12 Conclusion

This chapter describes the current situation of CAPE Groep and the implementation of the framework on this company. As explained in section 4.1, a company introduction is needed before the framework can be applied. After the introduction, the framework is applied on CAPE Groep. This implementation is done as described in section 4.2. On of the deliverables of implementing the framework is a list of internal control measures. Two of these measures are applied on the framework, which results in a conclusion if the measure must be implemented.

6. Validation

This chapter contains the validation of the framework at CAPE Groep. First, the validation method is described, including the UTAUT questions. Next, the results of the interviews that are conducted for the validation are described per stakeholder. Finally, the combination of Agile and internal control at CAPE Groep is described and recommendations for CAPE Groep are given. This is concluded in the last section of this chapter. This chapter supports in answering the corresponding research question of chapter 6, which can be found in section 1.2.

6.1 Validation interviews

The validation interview was a semi-structured interview which exist of two parts. The first part is an unstructured interview, the second part is an structured interview. The first part is focused on feedback on the filled frameworks, which are shown in Figure 28 and Figure 29. The interviewees indicated if their needs are correctly depicted in the filled frameworks. The second part is the validation of the framework. The validation of the framework is done by making use of the Unified Theory of Acceptance and Use of Technology (UTAUT) model. This is a unified model that integrates elements across eight prominent models about the acceptance of IT (Venkatesh, 2003). These models consists of items about the acceptance of a system. These items are divided into eight determinants. These determinants are: Performance expectancy, Effort expectancy, Attitude toward using technology, Social influence, Facilitating conditions, Self-efficacy, Anxiety, and Behavioural intention to use the system. Every category contains multiple items. Use of the different determinants of the method of Venkatesh (2003) is discussed below.

Performance expectancy (PE) is really important for the validation of the framework as this part of the validation shows if the employees think the framework would improve their performance. The second determinant that should be there is the effort expectancy (EE). This illustrates if an employee is willing to use the framework. Facilitating conditions (FC) are also crucial. These conditions make clear if the company can start using the framework. The next determinant that is important for the validation of the framework is the self-efficacy (SE). This determinant shows if people can really work with the framework. What will happen if an employee has questions about the framework? The last relevant determinant for validating the framework is the behavioural intention to use the framework (BI). This shows the intention of a specific stakeholder if he will start using the framework in his job.

Attitude towards using technology, social influence, and anxiety are not used for the validation of the framework. Attitude towards using technology is not used because the performance expectancy already validates if the interviewees think that the framework is relevant for their job. It is less relevant if the employees enjoy using the framework, because they have to work with it professionally. Social influence is not used for the validation because most of these questions are based on experience with using the framework for a longer time. It is also still unknown how the interviewees think about the use of the framework, as it is not yet implemented at CAPE Groep. The last determinant which is not used in the validation is anxiety. This determinant is not used because it consists of questions that are focused on systems, and are not relevant for frameworks.

Below, the used questions are summed up per determinant. This includes the additional questions (AQ) about their role and knowledge of Agile and internal control.

Performance expectancy

1. I would find the framework useful in my job.
2. Using the framework would enable me to accomplish tasks more quickly.
3. Using the framework would increase my productivity.
4. If I use the framework, I will increase my chances of getting a raise.

Effort expectancy

1. My interaction with the framework would be clear and understandable.
2. It would be easy for me to become skilful at using the framework.
3. I would find the framework easy to use.
4. Learning to operate the framework would be easy for me.

Facilitating conditions

1. I have the resources necessary to use the framework.
2. I have the knowledge necessary to use the framework.
3. The framework is not compatible with other systems/frameworks I use.
4. A specific person (or group) would be available for assistance with framework difficulties.

Self-efficacy

I could complete a job or task using the framework…

1. If there was no one around to tell me what to do as I go.
2. If I could call someone for help if I got stuck.
3. If I had a lot of time to complete the job for which the framework was provided.
4. If I had just the built-in help facility for assistance.

Behavioural intention to use the framework

1. I intend to use the framework in the next 3 months.
2. I predict I would use the framework in the next 3 months.
3. I plan to use the framework in the next 3 months.

Additional questions

Some additional questions are asked to be able to evaluate the framework best. The framework will not be involved in everyone's daily business, so they will probably rate the framework as less useful. Low scores from that particular stakeholder can then be evaluated differently.

1. What is your role within the organisation?
2. How familiar are you with Agile?
3. How familiar are you with internal control?

The questions are scored with the 5 point Likert scale. In every question the word 'system' is replaced by 'framework', and some questions are changed to the future tense. This is done because a framework is designed instead of a system, and the framework is not fully implemented at CAPE Groep yet.

At the end of the questionnaire, there is an open question so the stakeholders can provide all the feedback and comments they still have.

6.2 Results

This section contains the opinions of the stakeholders which are gathered during the validation interviews. Per stakeholder, it starts with the stakeholders' opinions, and ends with the analysis of the questionnaire. The answers on the questionnaire can be found in Appendix B. At all interviews, the stakeholders gave their opinion about the design. They all agreed that the design is complete, so all main components (steps of an Agile production process, stakeholders, and control categories) are present.

Manager Information Security

From the perspective of the Manager Information Security (MIS), the framework gives a clear overview of all aspects that must be considered. This includes different stakeholders, needs of the stakeholders during a specific process step, and the different categories. Unfortunately, the MIS does not see the relevancy of the framework. He mentioned that he could not see how the framework could directly contribute to his performance. According to him, it is useful to connect the different perspectives, but there is no added value to his job.

He gives two reasons why the framework does not add value to his job. One, a lot of the internal control measures are made mandatory by an accountant, or can be mandatory for achieving a privacy or security certificate, like SOC or ISO. These measures must be implemented, even when it has negative effects on stakeholders' needs. So the framework cannot be used for the decision of implementing this internal control measure. Secondly, the framework does also not add value to his job because all internal control measures have different requirements, and the needs of a stakeholder are also different for every measure. It will take a lot of time to adjust the framework for every different measure. An internal control measure will cost in most cases time or money, so adding an extra step which also costs time will not be beneficial.

Consequently, he does not expect to use the framework in the next three months. This is also shown by his answers to the UTAUT questionnaire, because the scores on the Performance expectancy and Behavioural intention to use the framework are low. On the other side, the scores on the Effort expectancy, Facilitating conditions and Self-efficacy are high. This shows that he understands how the framework works and that he is able to use the framework without help.

Consultant (Team lead)

From the perspective of the Consultant (Team Lead), the framework gives a clear overview of all aspects that must be considered. This includes the different stakeholders, needs of the stakeholders during a specific process step, and the different categories. Unfortunately, the Consultant (Team Lead) does not think he will use the framework soon, because it will not be easily applicable in his job. On the other side, he recognizes the indirect positive effects. The biggest positive effect he recognizes is that all needs of the relevant stakeholders are considered when implementing a new internal control measure, including his needs.

To make sure that the framework will be used at CAPE Groep, multiple examples must be shown. This will help the stakeholders understand how they must use the framework. If CAPE Groep wants to use the framework, it must be included within the methodology and it must be obliged to use when implementing an internal control measure. Including the framework in the methodology will also help by the understanding of the framework for new employees.

The scores on the UTAUT questionnaire are low on the Performance expectancy, which shows that the framework will not contribute in his job. As he is not the intended end user, this result was expected. The scores on the rest of the questionnaire are quite average, because the scores fluctuate from 1 till 5. The use of the framework will be understandable for him, and he knows where he should go if he got stuck. His scores on the intention to use are also average. This is caused by the combination of low added value within his job and the usability of the framework.

Commercial Manager

From the perspective of the Commercial Manager, the framework gives a clear overview of all aspects that must be considered. This includes the different stakeholders, needs of the stakeholders during a specific process step, and the different categories. Besides, he mentioned that it is clear to him how the framework must be used.

Especially the Business Controller will make use of the framework. However, the Commercial Manager must deal with the outcomes of the framework. When an internal control measure with a lot of impact must be implemented at CAPE Groep, the Management Team will be involved. He will be present at the discussion of these decisions as a member of the Management Team.

An option for further research of the framework is to split the customers in large and small. There are big differences between large and small customers in needs, which will result in interesting discussions.

The UTAUT questionnaire shows that he understands how the framework must be used. This is important, because he must be able to understand the framework during Management Team meetings. It can also be concluded from the questionnaire that he is not planning to use the framework soon, as it will not contribute directly to his job.

Financial Controller

From the perspective of the Financial Controller, it is hard to see the applications within CAPE Groep. Most of the possible internal control measures the Financial Controller wants to implement are not focused on multiple stakeholders and are only focused on the financial control category. Consequently, the added value of the framework for the Financial Controller is low at the moment.

A possible cause for the low added value of the framework for the Financial Controller is the type of his job. He has to improve the internal processes by applying internal control measures. These measures are mostly focused on situations where only the employees are involved. Without a division of the managers and employees within the framework, there is no difference between the stakeholders from his perspective.

The Financial Controller shares the opinion of the Manager Information Security about the internal control measures that are made mandatory. Sometimes there is no choice in applying an internal control measure, so the framework will not add value here.

The scores on the questionnaire of the Financial Controller are in general quite low. This corresponds with the information he gave during the interview. He does not think that the framework will be helpful within his job. His scores also show that he does not think that the framework is easy to use.

Business Controller

The results from the interviews of the Manager Information Security and the Financial Controller show the importance of this research according to the Business Controller. The framework should give more insight into these employees about the needs of other stakeholders. They are working in their own

environment, and are good at following the rules. From their origin, they want to implement as many internal control measures as possible to protect their own environment, security and financial. This can result in an enormous amount of measures for security and financial. The Consultants can experience this when they are executing the process. This can possibly be prevented by combining these measures (so combining different internal control categories).

Internal control measures can be implemented within an organisation in different ways. This is not recognized by some stakeholders, because they use a standard way of implementing a specific measure. With this standard implementation, many of the stakeholders' needs can be negatively affected. Applying that measure on the framework will show this. Other ways of implementing this measure should be evaluated and compared by applying them on the framework. The implementation with the least negative effects must be chosen.

CAPE Groep is a growing organisation, and they must ensure that they do not suffocate by all the internal control measures. This framework must provide insight into the process and the corresponding internal control measures. If a security measure is implemented, can another control category, like financial, take advantage of that control? Can measures be combined? This can yield less internal control measures.

It can be hard for employees that have practical work, to understand the framework. This is caused by the level of abstractness. The framework will not show you the right solution straight away. The user has to work with the framework to come to the best solution.

The modularity of the framework is also a strong point, because the framework can be expanded if needed. New stakeholders can be easily implemented in the framework, just like other control categories or even a different production process.

The Business Controller is responsible for bringing the perspectives of different stakeholders together. According to his opinion, the framework would be very useful to do his job effectively. This can also be seen in the questionnaire. Almost all scores on the questionnaire are above average. The framework will add value to his job, the framework is understandable and he is planning to use the framework in the next 3 months.

CEO

From the perspective of the CEO, it would be a good idea to use the framework within CAPE Groep. Considering all perspectives should be done always when implementing a new internal control measure. The framework gives a clear overview of all aspects that must be considered, so stakeholders will not be forgotten.

Despite the positive validation, some questions on the UTAUT questionnaire are scored low by the CEO. The reason for these low scores is that the CEO will not use the framework himself. He thinks that the framework is useful for some of his employees, like the Business Controller. This is the reason why he scored high on the questions about using the framework in the upcoming months.

Consultant

From the perspective of the Consultant, the framework will provide enough material for interesting discussions. Implementing an internal control measure does always affect a stakeholder. The Consultant also liked the design of the framework where all needs of the stakeholders are considered. He would like to work with the framework.

As same as the validation interview with the CEO, the chance of using the framework for the consultant is low. The framework will not help him with his daily tasks. Indirect, he can benefit from the use of the framework by other employees, like the Business Controller. The other employees can implement more internal control measures that comply with the needs of the Consultant.

This can be seen in the scores on the UTAUT questionnaire. The Performance expectancy is about average, while the rest of the scores are above average. The framework is clear and understandable, but it is not useful in his daily job.

Manager Customer Support

From the perspective of the Manager Customer Support, the complete framework will give a clear overview of all aspects that must be considered when applying internal control measures. Did I think about all stakeholders? Did I think about all internal control measures? Did I think about all the process steps?

He wonders if the whole framework (which includes the IT, Financial, and Data control category perspectives) will be used within CAPE Groep, because the most important and most relevant parts are already included in the validated part. If most of the internal control measures fall within the validated control categories, stakeholders and process steps, the two validated control category perspectives can be sufficient. When you do not need to create all control category perspectives with all stakeholders and all process steps, it will save you a lot of unnecessary spent time.

The Manager Customer Support only scored slightly disagree and neutral on the UTAUT questionnaire. He was not able to answer the questionnaire more precisely while the framework was not fully implemented. Despite the slightly negative scores, he thinks that the framework will be useful for CAPE Groep as it creates a clear overview and it makes sure all needs are considered.

6.3 Agile and internal control

The list with internal control measures in section 5.10, shows that the Big Mama, the methodology of CAPE Groep which includes the Agile methodology, comes with many internal control measures. This shows that the combination of Agile and internal control already exists at CAPE Groep.

Combination of Agile and internal control

Many different opinions exist between the interviewed stakeholders about the combination of Agile and internal control.

The Manager Information Security recognizes that colleagues have difficulties when the combination of Agile and internal control must be made. The problem inhere is that people who are working with Agile, do not see the added value of internal control measures. When they will see the added value of internal control, the implementation within Agile processes will be easier.

The Manager Customer Support has a different opinion about the combination of Agile and internal control. He knows for sure that the combination of Agile and internal control is possible, but according to him almost all internal control measures will slow down the process. So, he claims that when internal control measures are implemented, you must be sure that the measures are effective, mitigate the risks, etc. He predicts there will be too many internal control measures which do not comply with these requirements.

Most of the other interviewees recognize the difficulties of the combination, but they do not experience those difficulties within their own tasks all the time.

From this can be concluded that the stakeholders of CAPE Groep see that the combination of Agile and internal control needs attention. It must be ensured that the internal control measures which are implemented are contributing to the goal in such a way that the disadvantages are minimized. The framework can be used by looking at the advantages and disadvantages for their stakeholders.

6.4 Recommendations

This section includes additional valuables and recommendations for CAPE Groep.

Additional valuables

During this research, some practical contributions for CAPE Groep are created while it was not part of the research questions. These are the process maps, and descriptions of (possible) internal control measures. The framework gives a clear overview of the measures when all measures are placed within the framework. Placing all measures in the framework makes the relations between the different measures clear. This helps CAPE Groep by making these internal control measures more specific, which includes the measure itself, the goal or risk, expected results, influence on other measures/processes, etc.

Internal control measures

As mentioned by Byatt (2017), value added by risk management must be tracked. This ensures that internal control measures must deliver value. Risk should not be mitigated at any cost. If the cost of mitigating a specific risk is too high, it is possibly not worth mitigating that risk. Not all possible internal control measures have to be implemented, but CAPE Groep must think about the measures and implement the most important ones. The Management Team should make the final decision if an internal control measure must be implemented. In practice, the Business Controller will be responsible in most of the cases, but measures with much impact will probably also be discussed within the Management Team. Besides, it is important to check if a specific risk is mitigated with an internal control measure. Applying a measure while it is not mitigating the risk, will only cost money.

Some of the possible internal control measures are crucial to implement soon. The most important measures are: Guideline/checklist with all possible tests, checklist and risk presentation every two sprints, and keep track of the applications that are tested and accepted.

A guideline should be developed for the decision about different types of testing. The team lead must use this guideline, so he can make consistent decisions. At this moment, the team lead decides which tests should be run based on their experiences. The team leads are experienced employees but they should be supported to make a conscious decision. A list with all possible tests and a short explanation when a specific test must be used will lead to a lower amount of applications sent back with feedback. Team leads must think about every possible test and document why they will make use of this test or not.

The standard checklist and risk presentation for a release are only demanded by Customer Support at the first release. The application will not be accepted by Customer Support if the checklist or risk presentation is not sufficient. All upcoming releases do not require these checklists and risk presentations, while new releases can be totally different than the first one. Using the checklist and risk presentation every other sprint makes a release more reliable and makes the control less obstructive.

It must be measured how many applications need maintenance or are sent back to Customer Support with feedback within a particular timeframe (like two weeks) after release. The results must be evaluated per project team and action must be taken if a project team does not perform as expected.

This measure reduces the amount of applications released and needing maintenance or are sent back to Customer Support with feedback within the particular timeframe. The project teams will be made more aware of the value of delivering the application the first time right.

Not only new internal control measures must be applied on the framework. Also already existing measures must be applied on the framework, so the impact of these measures can be seen. Applying all already existing measures will show where these measures are applied. This will show which stakeholders' needs are most negatively affected. In addition, it will show at what part of the process the most measures are applied. When many needs of a specific stakeholder are negatively affected, or when a part of the process has a lot of measures, the company must think about the importance of those measures. Possibly, some measures can be combined or can be removed if their yield is low.

The last recommendation for CAPE Groep will be to apply SOC and ISO standards on the framework. A lot of inside information is needed to know all the internal control measures that come with these standards. Especially SOC 2 would be interesting to be applied on the framework, because CAPE Groep is planning on implementing this standard soon.

6.5 Conclusion

In this section, the results of the validation at CAPE Groep are described. It can be concluded that the most relevant stakeholders of this research are positive about the framework. They think that implementing the framework will solve their research problem. On the other side, the framework can be hard to understand for some employees. CAPE Groep must do their best to improve the understanding of all employees. This will help by making the framework successful for all stakeholders.

This section also describes which internal control measures should be implemented directly. These measures have the biggest yield or are marked as the most important issues during the interviews.

7.Conclusions

The framework that is designed in this research must be used by companies to combine Agile and internal control. This chapter contains the answers on the research questions, as defined in section 1.2. Next to that, the goal and the performance of the framework are discussed. This chapter concludes with limitations and further research.

7.1 Main research question

The main question which must be answered during this research is: How should the procedures of internal control be designed within an Agile business while complying with the needs of their stakeholders? This question is answered by the framework which is designed and validated in this research. The framework solves the problem according to the evaluation at CAPE Groep. CAPE Groep and companies similar to CAPE Groep are recommended to use the framework.

Implementing the framework at an organisation will result in an overview of all relevant stakeholders' needs. These needs are categorized per step of an Agile production process and per internal control category. The information can be used to decide whether an internal control measure must be implemented. The decision of implementing an internal control measure must be made based on the impact on stakeholders' needs. The negative and positive effects must be considered together with the goal of the internal control measure.

The framework will help by designing the procedures of internal control within an Agile business while complying with the needs of their stakeholders.

7.2 Research questions

To obtain the answer on the main question of this research, research questions are drawn up and explored. The construction behind each research question can be found in section 1.2.

Information about VUCA, Agile methodology, most used Agile methods, and importance of Agile, are the answers on research question 1: *What information about VUCA and Agile is needed from literature to develop a framework for the main problem?* It turned out that Agile is a good approach to use when a business must deal with the VUCA world. The most used Agile method is SCRUM, which will be used for the design of the framework.

Information about internal control, internal control categories, levers of internal control, importance of internal control, and the combination of Agile and internal control are the answers on research question 2: *What information about internal control is needed from the literature to develop a framework for the main problem?* It stood out that there are at least 3 types (or categories) of internal control which can be used for this research. Also, the importance of internal control is shown. In the end, a framework which combines Agile and internal control in a certain way is discussed. This framework shows that there are already methods to combine Agile and internal control. This framework will help by designing a solution for the research problem.

A description of the standard stakeholders is the answer on research question 3: *What information about stakeholders is needed from the literature to develop a framework for the main problem?* A standard stakeholder map is found in literature and used to determine which stakeholders must be considered within the framework. In combination with the experience of CAPE Groep employees, the final stakeholders are determined.

A description of already existing relevant frameworks is the answer on research question 4: *What information about already existing relevant frameworks is needed from the literature to develop a*

framework for the main problem? The already existing relevant frameworks are used as inspiration for the design of the framework and for defining internal control measures.

A description of multiple security and privacy standards is the answer on research question 5: *What information about security and privacy standards is needed from the literature to develop a framework for the main problem?* The description of these security and privacy standards will help companies to apply these standards on the framework. This is possible, because these standards consist of multiple internal control measures. Only a small amount of the available standards is described. These are the most relevant standards for companies within the scope.

A description of Enterprise Risk Management, importance of internal control, and importance of stakeholders are the answers on research question 6: *What information about Enterprise Risk Management is needed from the literature to develop a framework for the main problem?* Enterprise Risk Management shows the importance of internal control. By implementing internal control measures correctly, the first step of ERM is already done.

Design of the framework and how to validate the framework is the answer on research question 7: *How can a proper framework be designed and validated for the main problem?* The design and validation method are designed by means of the literature gathered in chapter 2. The designed framework will show how the procedures of internal control must be designed in an Agile business while complying with the needs of their stakeholders. The design is shown in chapter 3.

The implementation plan is the answer on research question 8: *How should companies implement the framework within their business?* The implementation plan describes how companies can implement the framework within their organisation. Every step that must be executed is described, which helps using the framework. The implementation plan is shown in chapter 4.

Implementing the framework at CAPE Groep is the answer on research question 9: *How is the framework implemented and validated at CAPE Groep?* All steps of the implementation plan are executed during the implementation of the framework. The implementation succeeded at CAPE Groep so the framework could be validated.

Validating and evaluating the experience at CAPE Groep is the answer on research question 10: *How is the framework experienced by CAPE Groep?* The validation interviews and the questionnaire show that the users of the framework experience the framework as usable at CAPE Groep. It also shows that the framework will achieve its goal. On the other side, some stakeholders do not see the applications of the framework. This is described in chapter 5 and chapter 6.

7.3 Goal of the framework

The goal of the framework is to give Agile businesses insights in the procedures of internal control while they comply with the needs of their stakeholders. This is done by combing different internal control categories (Financial, IT and data) with the steps of an Agile production process, while considering the needs of all stakeholders. The framework shows the difference between all the combinations of categories, steps of an Agile process and the needs of the stakeholders. Internal control measures can be put in the framework to show which stakeholders are involved at a specific internal control measure and if this internal control fits within the needs of these stakeholders.

So, this framework must combine the different perspectives of all stakeholders of a company. The stakeholders have different needs from different perspectives. For example, applying an internal control measure can be a good idea for employees looking from the IT perspective, but it can have negative effects for employees looking from a financial perspective. Even the same stakeholder can

have different needs between different categories. The framework must give insights into these differences.

If a company wants to implement an internal control measure, while it can be obstructive for some needs, they can easily show that other needs are pleased by this internal control. This can be the reason to still implement this internal control measure. Hopefully, this will create more understanding for the people who experience the obstructions.

Another goal of the framework is to create an overview of all the different aspects which must be considered when implementing a new internal control measure. This framework ensures that every important aspect (all stakeholders' needs, all possible internal control categories, and the correct process step(s)) is considered.

7.4 Performance of the framework

During the validation, most of the interviewees did not see direct applications of the framework for their jobs. Nevertheless, the opinion of most of the interviewees is still that the framework will be useable within CAPE Groep. They see how other employees can make use of the framework, and how it can benefit them.

As can be seen in section 6.2, some of the employees think that it can be hard to implement and use the framework in practice. This is not an unexpected result of this research. The framework is mainly designed for employees who are in the Management Team and/or having a function where internal control measures and protecting all stakeholders' interests are important. When the framework is implemented, more internal control measures are used on the framework. Hopefully, this will show the importance of the framework for all the doubting stakeholders.

All stakeholders see valuables within the framework. It gives a clear overview of all aspects that must be considered when an internal control measure is implemented. It shows that all needs will be considered, which means that a stakeholder knows that also his needs are considered. And the framework can also create an understanding of why an internal control measure is implemented.

An Agile business gets insights in the procedures of internal control while they comply with the needs of their stakeholders shows that the goal of the framework and this research is realised. Not all employees will get the insights immediately due to the high level of abstractness. However, the important stakeholder who must use the framework get the insights, namely the Business Controller (and other members of the Management Team).

7.5 Limitations and further research

This section includes the limitations of this research and information for further research on the framework.

Limitations

The main limitation of this research is the chosen research design. Within this research design, only one company is considered for the validation, and not all stakeholders, not the whole Agile process and not all internal control categories are considered. Also, some of the considered stakeholders are represented by employees of CAPE Groep.

The framework is only tested at one company, CAPE Groep. Within this research design, there was no time to implement the framework at another company. However, as all companies differ, it is hard to predict how this framework will work for other companies. It is predicted that companies that can be

compared with CAPE Groep by size and characteristics will act alike, but to be sure the framework must be tested at more (similar) companies.

The next limitation is that only a part of the framework is validated. Only 4 of the 7 stakeholders, 2 of the 6 steps of an Agile production process, and 2 of the 3 internal control categories are considered in this validation. Validating the whole framework would take longer than time is available within this research design. Validating the whole framework will also ask more time and dedication from the stakeholders. It was wise to validate a small part of the framework first, before investing a lot of time without knowing the value of the framework.

Besides, because of the chosen research design, the framework is not validated by all stakeholders. The customers and the government are not interviewed, but employees from CAPE Groep who are experienced with these stakeholders took their place. These stakeholders are not accessible for relatively small research like this one.

Further research

There are a lot of different employees within a company like CAPE Groep, and all the employees have different interests. It can be relevant for the framework to split the stakeholder 'Employees' in: 'Executing personnel' and 'Management personnel', because the biggest differences in interests appeared at these stakeholders. It can also be useful to split the Executing personnel furthermore. This category can be split into: 'Programme Manager', 'Team Lead', 'Consultant', and 'Customer Support'. All these employees have different interests and it is hard to put all their needs together. Implementing an internal control measure will sometimes fulfil a need or requirement of the consultant, while it can be obstructive for Customer Support. Splitting the stakeholder 'Employees' will automatically lead to even more cells in the framework.

Splitting the stakeholders and adding a category is possible due to the modularity of the framework. The modularity of the framework gives even more options for further research. A possible option is to examine if the framework can perform with another type of process instead of the Agile production process. The framework itself can also be extended at the internal control category part. As can be concluded from the interviews, the methodology can also be seen as a control category. So, the methodology can be added as an internal control category. Using the framework in a different industry, will probably lead to the need for different internal control categories. Adding, deleting or replacing is possible due to the modularity of the framework.

The framework is only validated at one company. It must be researched how the framework will perform at other companies. These companies must be in the scope of the research, because the framework is designed for IT companies which can be classified as SME.

Only a small part of the framework is validated, only 16 cells of the total 126 cells. A logical next step would be to involve more stakeholders, considering the third internal control category or considering more steps of the Agile production process. These possible steps should not be done at the same time, but step by step because each process will be time consuming and therefore will be burdensome for some stakeholders. This validation is needed if the whole framework must be implemented within a company.

With the current VUCA world, large changes can happen every day. This can affect the framework. These effects are minimized because a solution for VUCA is already part of the framework. So, the framework needs no big changes in the near future. Changes only occur if companies are using the modularity of the framework.

Reference list

Abu Saleem, K. S., Zraqat, O. M., & Okour, S. M. (2019). The Effect of Internal Audit Quality (IAQ) on Enterprise Risk Management (ERM) in Accordance to COSO Framework. *European Journal of Scientific Research*, 177–188. https://doi.org/10.13140/RG.2.2.22520.08962

agile adjective - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com. (n.d.). Retrieved July 11, 2019, from https://www.oxfordlearnersdictionaries.com/definition/english/agile

AICPA Assurance Services Executive Committee. (2017). *Trust Services Criteria*. New York: American Institute of Certified Public Accountants, Inc.

AICPA. (2014). *The importance of internal control in financial reporting and safeguarding plan assets*. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/employeebenefitplanauditquality/resources/planadvisories/downloadabledocuments/plan-advisoryinternalcontrol-hires.pdf

Archer, G. R. (2006). Six Good Reasons to Include Competitors as Stakeholders. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1437117

AuditConnect. (n.d.). SOC 1, 2 & 3. Retrieved 9 October 2019, from https://www.auditconnect.nl/nl/it-audits/SOC-1--2---3/

Beck, K. (2018, December 12). Agile Manifesto for Software Development | Agile Alliance. Retrieved July 9, 2019, from https://www.agilealliance.org/agile101/the-agile-manifesto/

Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons*, *57*(3), 311–317. https://doi.org/10.1016/j.bushor.2014.01.001

Bonner, T. (2020, January 6). Explaining the Different Types of Stakeholders in Project Management. Retrieved from https://www.brighthubpm.com/project-planning/93262-stakeholders-in-project-management/

Bragg, S. (2018). Internal control. Retrieved August 19, 2019, from https://www.accountingtools.com/articles/internal-control.html

Brink, H. I. L. (1993). Validity and reliability in qualitative research. Presented at the SA Society of Nurse Researchers' Workshop, Rau.

Bryson, J. M. (1995). *Strategic Planning for Public and Nonprofit Organizations Revised Edition*. San Francisco: Jossey-Bass.

Bryson, J. M. (2004). What to do when stakeholders matter - A guide to stakeholder identification and analysis techniques. *Public Management Review*.

BusinessDictionary. (2019). Framework definition and meaning. Retrieved 26 September 2019, from http://www.businessdictionary.com/definition/framework.html

Byatt, G. (2017, April 20). 5 Steps to Enable Agile Enterprise Risk Management. Retrieved 11 October 2019, from https://enablon.com/blog/5-steps-to-enable-agile-enterprise-risk-management/

Casadesús, M., & Giménez, G. (2000). The benefits of the implementation of the ISO 9000 standard: empirical research in 288 Spanish companies. *The TQM Magazine*, *12*(6), 432–441. https://doi.org/10.1108/09544780010351751

Certified B Corporation. (2019). B Resource Guide: Implementing Financial Controls. Retrieved August 20, 2019, from https://bimpactassessment.net/sites/all/themes/bcorp_impact/pdfs/B+Resources+-+Implementing+Financial+Controls.pdf

Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information & Management*, *51*(2), 187–205. https://doi.org/10.1016/j.im.2013.11.002

CollabNet, & VersionOne. (2019, May 7). 13th Annual State of Agile Survey. Retrieved March 26, 2020, from https://www.stateofagile.com/#ufh-i-521251909-13th-annual-state-of-agile-report/473508

Conboy, K., & Fitzgerald, B. (2004). Toward a Conceptual Framework of Agile Methods. *Lecture Notes in Computer Science*, 105–116. https://doi.org/10.1007/978-3-540-27777-4_11

COSO. (2013a). Internal Control - Integrated Framework Executive Summary. *COSO*. Retrieved from https://www.coso.org/Pages/ic.aspx

COSO. (2013b). Internal Control Guidance and Thought Papers. Retrieved August 21, 2019, from https://www.coso.org/Pages/ic.aspx

COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance. *COSO*. Retrieved from https://www.coso.org/Pages/erm.aspx

DeBenedetti, J. (n.d.). Why are internal controls important in financial statements. Retrieved March 19, 2020, from https://smallbusiness.chron.com/internal-controls-important-financial-statements-80211.html

Dunkelberger, D. (2019, March 4). Understand the Difference Between SOC 1 Type 1 & 2 Reports. Retrieved 9 October 2019, from https://www.ispartnersllc.com/blog/understand-the-difference-soc-1-type-1-2-reports/

Freeman, R. E. (2010). *Strategic Management: A Stakeholder Approach*. Cambridge: Cambridge University Press.

Gallagher, B. (2019, September 27). SOC 1 vs. SOC 2 Reports. Retrieved 9 October 2019, from https://www.ispartnersllc.com/blog/soc-1-soc-2-reports-difference/

Gonçalves, A., Correia, A., & Cavique, L. (2019). An Approach to GDPR Based on Object Role Modeling. *Advances in Intelligent Systems and Computing*, 595–602. https://doi.org/10.1007/978-3-030-16181-1_56

Hofisi, C., Hofisi, M., & Mago, S. (2014). Critiquing Interviewing as a Data Collection Method. *Mediterranean Journal of Social Sciences*. https://doi.org/10.5901/mjss.2014.v5n16p60

Holbrook & Manter. (2018, September 5). Difference Between SOX and SOC Compliance. Retrieved 2 October 2019, from https://www.socauditservices.com/2017/03/28/soc-vs-sox/

Home - CAPE Groep. (2020). Retrieved April 7, 2020, from https://www.capegroep.nl/

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

ISACA. (2012). *COBIT 5 - An Introduction*. Retrieved from http://www.isaca.org/COBIT/Documents/Forms/AllItems.aspx

ISO. (2019a). ISO/IEC 27001 Information security management. Retrieved 25 September 2019, from https://www.iso.org/isoiec-27001-information-security.html

ISO. (2019b, June 11). ISO 9001:2015. Retrieved 25 September 2019, from https://www.iso.org/standard/62085.html

ISO. (2019c, July 1). ISO 31000:2018. Retrieved 30 September 2019, from https://www.iso.org/standard/65694.html

ISO. (2019d, August 6). ISO/IEC 27001:2013. Retrieved 25 September 2019, from https://www.iso.org/standard/54534.html

ISO. (2019e, August 6). ISO/IEC 27701:2019. Retrieved 30 September 2019, from https://www.iso.org/standard/71670.html

IT Governance UK. (2019). ISO 27001 and the GDPR. Retrieved 23 September 2019, from https://www.itgovernance.co.uk/gdpr-and-iso-27001

Kirkpatrick, J. (2019, June 19). 3 Objectives of COSO. Retrieved August 21, 2019, from https://kirkpatrickprice.com/video/3-objectives-coso/

LeanSixSigma. (2019). Wat is lean? Retrieved 22 October 2019, from https://www.sixsigma.nl/wat-is-lean

Leffingwell, D. et al (2019, May 29). Scaled Agile Framework for Lean Enterprises. Retrieved 17 October 2019, from https://www.scaledagileframework.com/

LeSS. (2005). Large Scale Scrum (LeSS). Retrieved 17 October 2019, from https://less.works/

Lucidchart. (2017, December 1). The Stages of the Agile Software Development Life Cycle. Retrieved 22 October 2019, from https://www.lucidchart.com/blog/agile-software-development-life-cycle

Maxius. (2019, September 24). Burgerlijk Wetboek Boek. Retrieved 7 October 2019, from https://maxius.nl/burgerlijk-wetboek-boek-2/boek2/titel9/

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*.

Melicharova, A. (2018). Standard ISO 9001:2015, most important changes and their impact on supplier complaints management. *Engineering for Rural Development*. https://doi.org/10.22616/ERDev2018.17.N448

Nerur, S., Mahapatra, R., & Mangalaraj, G. (2005). Challenges of Migrating to Agile Methodologies. *Communications of the ACM*, *48*(5). Retrieved from http://www.umsl.edu/~sauterv/analysis/challenges_of_migrating_to_agile_methodologies.pdf

Neuman, E. J. (2005). The impact of the Enron accounting scandal on impressions of managerial control. *Academy of Management 2005 Annual Meeting*, *1*. Retrieved from http://ww.ericneuman.com/Papers/post-enron-attributions_aom_2005.pdf

Osterwalder, A., Pigneur, Y., & Clark, T. (2010). *Business Model Generation*. Hoboken, NJ, United States: Wiley.

OTAVA. (2019, August 30). SOC 1, SOC 2 & SOC 3 Report Comparison. Retrieved 9 October 2019, from https://www.otava.com/blog/soc-1-soc-2-soc-3-report-comparison/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Informations Systems*, *24*(s).

Pfister, J. A. (2009). *Managing Organizational Culture for Effective Internal Control: From Practice to Theory*. Heidelberg: Physica-Verlag HD.

Porter, M. E. (1985). *Competitive Advantage*. New York: Free Press.

Ralph, P. (2016). Software engineering process theory: A multi-method comparison of Sensemaking–Coevolution–Implementation Theory and Function–Behavior–Structure Theory. *Information and Software Technology*, *70*, 232–250. https://doi.org/10.1016/j.infsof.2015.06.010

Reifer, D. J., Maurer, F., & Erdogmus, H. (2003). Scaling Agile Methods. *IEEE Computer Society*. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1207448

Rubin, K. S. (2012). *Essential Scrum*. Boston, United States: Addison-Wesley.

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, *10*(3), 21–45. Retrieved from http://www.proso.com/dl/Samonas.pdf

Shaffril, H. A. M. et al. (2012). Measuring ICT Usage among West Coast Fishermen: Pre-Test Results from Port Dickson, Negeri Sembilan . *American Journal of Agricultural and Biological Sciences*, 21–27.

Simons, R. (1995). Control in an Age of Empowerment. *Harvard Business Review*, *95211*, 80–88.

Smartsheet. (2019). Understanding the Agile Software Development Lifecycle and Process Workflow. Retrieved 22 October 2019, from https://www.smartsheet.com/understanding-agile-software-development-lifecycle-and-process-workflow

Sousa, P., Tereso, A., Alves, A., & Gomes, L. (2018). Implementation of project management and lean production practices in a SME Portuguese innovation company. *Procedia Computer Science*, *138*, 867–874. https://doi.org/10.1016/j.procs.2018.10.113

Sowa, J. F., & Zachman, J. A. (1992). Extending and formalizing the framework for information systems architecture. *IBM Systems Journal*.

Stoel, M. D., & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems*, *12*(4), 280–304. https://doi.org/10.1016/j.accinf.2011.06.001

strongDM. (2019, June 4). SOC 2 Type 1 Guide | Everything You Need To Know. Retrieved 9 October 2019, from https://www.strongdm.com/what-is-soc-2-type-1/

Sutherland, J., & Schwaber, K. (2011). *The Scrum Papers: Nut, Bolts, and Origins of an Agile Framework*. Boston, United States: Scrum, Inc.

Terry, J. (2019). *Benefits of Agile Development* [Photograph]. Retrieved from https://www.planview.com/resources/articles/benefits-of-agile-development/

Thummadi, B. V., Shiv, O., & Lyytinen, K. (2011). Enacted Routines in Agile and Waterfall Processes. *2011 AGILE Conference*. https://doi.org/10.1109/AGILE.2011.29

Uwadiae, O. (2015, May 22). COSO - An Approach to Internal Control Framework. Retrieved August 21, 2019, from https://www2.deloitte.com/ng/en/pages/audit/articles/financial-reporting/coso-an-approach-to-internal-control-framework.html

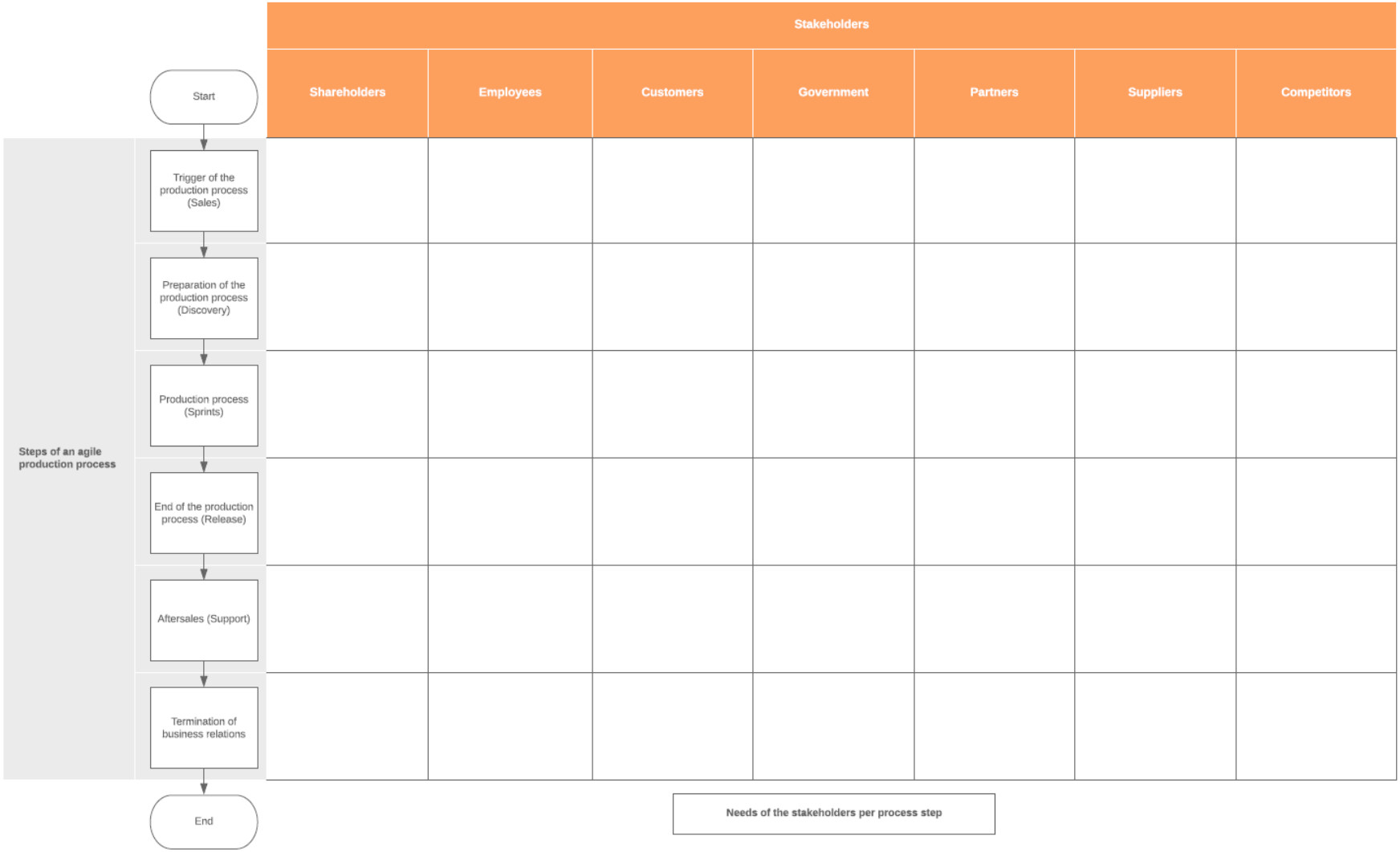
Van Noort Gassler & Co. (2018, December 11). Accountantscontrole is verplicht in Nederland, maar niet voor iedereen. Retrieved 3 September 2019, from https://noortgassler.nl/accountantscontrole-is-verplicht-in-nederland-maar-niet-voor-iedereen/

Venkatesh, V. (2003). *User Acceptance of Information Technology: Toward a Unified View*. Retrieved from https://www.jstor.org/stable/30036540

Visual Paradigm. (2019). What is Zachman Framework? Retrieved 2 September 2019, from https://www.visual-paradigm.com/guide/enterprise-architecture/what-is-zachman-framework/

Zhang, E. (2016, September 23). The Importance of Internal Controls in Accounting - Houston, The Woodlands, Sugar Land. Retrieved March 19, 2020, from http://www.carrtegra.com/2016/06/importance-internal-controls-accounting/

Appendix A – Agile internal control framework design: control category perspective



Appendix B – Results of the questionnaire

PE 1	5	2	3	3	2	2	4	3
PE 2	4	2	3	2	2	1	2	2
PE 3	4	2	3	3	5	1	1	2
PE 4	3	1	1	1	3	1	1	3
EE 1	4	4	3	4	4	2	5	3
EE 2	4	4	3	4	4	3	4	3
EE 3	3	3	3	4	4	4	4	3
EE 4	4	4	3	2	4	2	4	3
FC 1	4	4	3	4	4	4	3	2
FC 2	4	4	4	3	4	3	5	3
FC 3	2	3	1	3	2	3	1	2
FC 4	1	2	4	4	4	5	4	3
SE 1	4	4	3	3	4	1	2	3
SE 2	2	5	2	3	3	4	4	3
SE 3	5	4	2	3	4	3	4	3
SE 4	2	3	3	3	4	5	4	2
BI 1	5	2	2	4	5	4	3	3
BI 2	4	2	2	4	3	2	3	3
BI 3	3	1	2	4	1	3	2	3
AQ 1	Business Controller	MIS	Financial Controller	CEO	Consultant	Teamlead / Consultant	Commercial Manager	Manager Customer Support
AQ 2	3	5	1	5	4	5	5	4
AQ 3	5	4	4	4	2	3	3	3