

UTRECHT UNIVERSITY

BACHELOR'S THESIS

---

Critical Applications Should Come With Critical Questions:  
Business Continuity Solution Adoption  
at Dutch SaaS-Providers

---

*Author:*

**MARCO DE JONG**

5704367

*Supervisor:*

**Dr. R.L. JANSEN**

**Dr. S.J. OVERBEEK**

*A thesis submitted in fulfilment of the requirements  
for the Bachelor of Science*

*in the*

**Bachelor's Programme Information Science  
Department of Information and Computing Sciences**

August 1, 2019

## Abstract

When it comes to business-critical processes, organizations are increasingly adopting SaaS-solutions in favour of traditional on-premise solutions. This paper addresses business continuity solutions at SaaS-providers, by investigating how SaaS-providers perceive business continuity solutions for business-critical applications. The scope of this research is on Dutch SaaS-providers with small-to-medium enterprises as their customers. The goal of this research is to expose choices, motives and opinions towards business continuity solutions, as well as discovering the most effective tool to raise awareness for the risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud. Interviews were held with SaaS-providers, SaaS business continuity solution providers and IT interest groups. The conclusions are that large enterprises, with their own IT-department, are demanding continuity guarantees from their provider, but smaller companies do not due to lack of knowledge; making them extra vulnerable. All respondents agreed unanimously there should be more attention for business continuity solutions, and that a certification mark could help raising awareness for the continuity risk SaaS-applications come with.

## Preface

Before you lies the bachelor thesis “Critical Applications Should Come With Critical Questions: Business Continuity Solution Adoption At Dutch SaaS-Providers”. It has been written to fulfil the graduation requirements of the bachelor’s degree in Information Sciences at Utrecht University. The thesis has been written in the period between March and August 2019.

The project has evolved from ACC ICT’s interest in independent research into the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-providers, and the interest in the development of an effective tool to raise awareness for the continuity risk a SaaS-application comes with. The research questions were formulated together with supervisor Dr. R.L. Jansen, co-worker Denise van Velzen, and Paul Bijleveld and Ronald Kers from ACC ICT. I am happy to say that the research has been executed according to plan. The research questions have been answered by conducting a qualitative research.

I would like to thank Dr. R.L. Jansen, Denise van Velzen, Paul Bijleveld and Ronald Kers for their guidance and valuable input throughout the project. Additionally, I would like to thank all respondents for their cooperation. And last but not least, I would like to thank my girlfriend Lisa, my parents Gerard and Ellie and our dogs Boris and Bruno for their everlasting support and trust.

I hope you enjoy your reading.

Marco de Jong



Utrecht, August 1, 2019

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>Research Approach</b>	<b>6</b>
2.1	Research Questions	6
2.2	Literature Study	7
2.3	Expert Interviews	7
2.3.1	Aligning Interview Questions with Research Questions	9
2.3.2	Constructing an Inquiry-Based Conversation	10
2.3.3	Receiving Feedback on the Interview Protocol	11
2.3.4	Piloting the Interview Protocol	12
2.4	Analysis	13
2.4.1	SaaS-Provider Interview Statements	13
2.4.2	Sparring Sessions	13
<b>3</b>	<b>Results</b>	<b>13</b>
3.1	Literature Study	14
3.1.1	Business Critical Cloud Computing	14
3.1.2	SaaS Business Continuity Threats	15
3.1.3	SaaS Business Continuity Solutions	15
3.2	Interview Results	18
3.2.1	SaaS-Provider Interviews	21
3.2.2	SaaS Business Continuity Solution Providers	25
3.2.3	IT Interest Groups	27
<b>4</b>	<b>Discussion</b>	<b>29</b>
4.1	Limitations	30
4.1.1	Expert Quality	30
4.1.2	Providers' Perspective	30
4.1.3	Customers' Perspective	31
4.2	Opportunities	31
4.2.1	Awareness	31
4.2.2	Revenue Model	31
4.3	Future Research	32
4.3.1	SaaS Business Continuity at Dutch SaaS-Customers	32
4.3.2	Certification Mark	32
4.3.3	Customer Loyalty	32

---

**5 Conclusion..... 33**

**Appendices..... 35**

- A Interview Consent Form..... 35
- B Interview Protocols ..... 36
  - B.1 Interview Protocol for SaaS-Providers.....36
  - B.2 Interview Protocol for SaaS Business Continuity Solution Providers.....39
  - B.3 Interview Protocol for IT Interest Groups .....41
- C Interview Protocol Matrixes..... 43
  - C.1 Interview Protocol Matrix for SaaS-Providers .....43
  - C.2 Interview Protocol Matrix for SaaS Business Continuity Solution Providers .....48
  - C.3 Interview Protocol Matrix for IT Interest Groups .....52

# 1 Introduction

Over the past decade, the software industry has evolved into a service economy, where software products have a Software-as-a-Service (SaaS) business model. SaaS is a form of software deployment, that delivers software on a subscription basis through the internet (Van De Zande & Jansen, 2011). SaaS enables end-users to rent storage for their software products and its corresponding data, instead of having to purchase and establish their own IT-department. Pricing models can vary, but generally customers pay on a subscription-basis or on a usage volume-basis (Abdat, Spruit & Bos, 2010). During the rise of the SaaS-popularity, especially the advantages of such solutions were seen, and the possible business continuity risks were neglected. Not on purpose though, but because the SaaS-industry had not gone through a full lifecycle yet, the possible risks when adopting a SaaS-solution had not yet come to light (Daly, 2017). The coming of SaaS brought new risks which were not present until then; mainly because on-premise software products did not depend as much on third parties as a SaaS-solution does. In the meantime, multiple SaaS-providers faced bankruptcy, leaving the customer to fate. During the process of forming Service Level Agreements (SLA), assumptions were made which did not seem to turn out positively. SLAs are legal documents where customer and provider agree on the quality of service, by quantifying minimum quality of service (Hiles, 1994). Disaster recovery service and business continuity guarantees in case of a human or non-human disaster were left aside when making these agreements. This is mainly because customers assumed the SaaS-provider would include these services, while it did not. On the other hand, SaaS-providers did not feel the need to include those (expensive) services, because SaaS-customers rarely ever asked for them (Van De Zande & Jansen, 2011).

Whereas SaaS-customers previously did not demand business continuity solutions and just assumed SaaS-providers included such solution in their services, these days more and more large SaaS-customers are looking deep into the continuity risks of SaaS-solutions, because of disappointing disaster recovery results from the past. Large companies have an IT-department at their disposal, which is familiar with the risks SaaS-solutions bring and the measures needed to be able to guarantee business continuity. Nowadays, bankruptcy and even natural disasters should be risks SaaS-customers take into account when choosing the right SaaS-provider for their business-critical software systems (Daly, 2017). Although large customers are seeing the need for business continuity arrangements, it is unsure if SaaS-providers realise the needs for such offerings to this very moment. Only a small part of the Dutch SaaS-providers offers its customers a business continuity solution. As long as SaaS-providers do not realise the needs for continuity guaranteeing solutions, we may assume small-to-medium enterprises (SMEs) do neither if they have no experience in IT. As the results from the interviews with SaaS-providers show, most of them believe initiative for the use of a business continuity solutions should come from the end-users, because they are the party running the real risk. But as long as (small) customers do not realise the need for some kind of business continuity solution, the situation remains as it currently is, and we are all waiting for a disaster to happen before measures will be taken. Bankruptcy of a SaaS-provider could have disastrous consequences, which go further than business continuity disruption for the end-user of the application.

This paper addresses SaaS business continuity solutions by mapping experts' visions towards this topic. In other words, the research question to be answered is: *How do Dutch SaaS-providers perceive business continuity solutions for business-critical application?*

To give an answer to this question, an explorative research has been conducted. Several semi-structured interviews have been held with Dutch (experience) experts. Each expert has been interviewed with a personalized interview protocol, to cover and capture every step in their choices, motives or opinions towards SaaS business continuity solutions. These interview protocols are drawn up with the use of a four-phase interview protocol refinement framework (Castillo-Montoya, 2016). This ensured all research questions being covered correctly and all data collected could be transformed into statements to which Dutch SaaS-providers who made a substantiated choice towards the adoption of SaaS business continuity solutions were valued. Another goal of this research was to discover the most effective tool to raise awareness for the continuity risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud. Although multiple ideas for possible tools came up and were discussed during the interviews, all respondents agreed unanimously a certification mark could help raising awareness for the continuity risk SaaS-applications come with.

The paper is built up as follows; Section 2 describes the research approach. This contains the research questions, the literature study, the interview protocols and the analysis of the interview data. Section 3 describes the results of the literature study and the results of the interviews. It shows a table in which the way how Dutch SaaS-providers perceive business continuity solutions for business-critical applications is presented, and it presents the choices, motives and opinions of SaaS business continuity solution providers and IT interest groups towards this topic. It describes and discusses the necessity and incorporation of business continuity solutions for SaaS. Also, two possible tools for raising awareness and improving the quality of SaaS business continuity solutions will be presented and discussed. Section 4 discusses the limitations of this research, possibilities of this research and possible future research. In section 5 the paper will be concluded.

## 2 Research Approach

This research has an explorative nature. This means the main goal of the research is to expose choices, motives and opinions towards business continuity solutions for end-users of business-critical SaaS-applications, to be able to contribute to general publicity of this subject. In order to do so, a literature study has been performed and several interviews were held with SaaS business continuity (experience) experts. This resulted in qualitative data (Baarda, Van Der Hulst & De Goede, 2012). Who these experts are, and why they were invited to contribute to this research, will be further explained in section 3.2: Expert Interviews. First, the research questions will be described, consisting of one main question and four sub-questions. Next, the structure of the literature study will be given. After that, the three expert groups, interview protocols and analysis of those interviews will be described.

### 2.1 Research Questions

This paper addresses SaaS business continuity solutions at Dutch SaaS-providers, by investigating to what extent Dutch SaaS-providers have incorporated these solutions in their business model. Another goal of this research is to discover the most effective tool to raise awareness for the risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud. The research's scope is on Dutch SaaS-providers with small-to-medium enterprises using business-critical SaaS ERPs as their customers.

The main research question to be answered is:

*“How do Dutch SaaS-providers perceive business continuity solutions for business-critical applications?”*

This qualitative main question asks for both researching the context, the practice and the possibilities. In order to answer the main research question, the following sub-questions have been defined:

SQ1: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*

SQ2: *“To what extent do Dutch SaaS-providers feel responsible for their customers' business continuity?”*

SQ3: *“Which solutions can Dutch SaaS-providers offer their customers in order to guarantee business continuity?”*

SQ4: *“What would be the most effective tool to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-solution comes with?”*

These questions were answered by performing a literature study and by conducting nine interviews with SaaS business continuity (experience) experts.

## 2.2 Literature Study

A literature study on the subjects of business continuity, cloud computing, SaaS business continuity threats and SaaS business continuity solutions has been conducted. Various search terms related to business continuity and cloud computing have been executed on the following search engines:

- Google Scholar
- ACM Digital Library
- Google

Different search queries with keywords concerning business continuity, cloud computing and various combinations of those keywords were used in finding the literature. Based on the abstracts, an initial selection was made. All literature with relevant abstracts were added to Mendeley to be further investigated.

It soon became apparent that search queries on business continuity and cloud computing were successful, but combining the keywords led to few results. Almost all results gave no new information about this topic and they generally referred back to one paper: Business Continuity Solutions for SaaS Customers (Van De Zande & Jansen, 2011) Therefore, two additional search methods were used during the literature study. These methods are:

- Snowballing
- Forward reference searching

With snowballing, the reference list of a paper or the citations to a paper are used to identify additional papers (Wohlin, 2014). According to Wohlin (2014), one of the main advantages of snowballing is that it starts from relevant papers and then uses these to drive the further study. This is particularly useful in the case of this paper, as the topic is one that has not been explored much yet. Snowballing led to three additional sources. Forward reference searching also led to three additional papers. Modern bibliographic databases allow to identify and report the citations of a publication (Hinde & Spackman, 2015). This relatively limited result, again, concludes little research on this topic has been conducted in the past. This means, the focus of this research is on the expert interviews.

## 2.3 Expert Interviews

To obtain an answer to the main research question and the various sub-questions, a qualitative research was performed. Based on the literature study and meetings with ACC ICT, with which this research was conducted in collaboration, a list of interview questions was devised. A total of nine interviews have been conducted with Dutch SaaS business continuity (experience) experts. For this research, a total of sixteen companies were approached and invited to take part in the research. These companies were selected by the authors of this paper and were all within the acquaintance of ACC ICT. The interviewee selection process threatens the validity of the research, in that the participants were selected based on availability and willingness to participate. Nine out of the sixteen selected organisations responded positively and were willing to be interviewed. However, due to the method used to find participants the researcher dares to say with some certainty that the interviewees' responses were relevant, on-topic, and addressed the topic with sufficient experience and insight.

All interviewees signed a consent form, as stated in Appendix A. The individual consent forms are in hands of this paper's authors. This consent form allowed the researcher to record the interview using an audio recorder and to quote some of the interviewees.

The experts can be separated into three groups. Table 1 provides an overview of all organisations that were interviewed, along with the role of the interviewee and the expert group to which the organisation belongs. These groups are:

- A. SaaS-providers that either do or do not offer their end-users a business continuity solution, but at least have thought about the subject and made a substantiated decision.
- B. Companies that offer business continuity solutions for SaaS-providers and their end-users.
- C. Interest groups in the field of IT.

The reasons for selecting these specific groups of experts can be found in the goals of the research as well as validity and reliability of the research. The main purpose of this research is to map out the current state of affairs concerning business continuity solution for business-critical applications at SaaS-providers. For expert group “A” (SaaS-providers) the decision has been made, in consultation with ACC ICT, to only interview SaaS-providers that have made a substantiated decision in adopting SaaS business continuity solutions for their customers. This way, when concluding this paper, judgements towards SaaS business continuity solution adoption at SaaS-providers can be made with respect to the group of SaaS-providers which has actively thought about this subject. Therefore, this paper describes the current state of affairs from the point of view of SaaS-providers who have arranged business continuity best for their customers. Future research could conduct a national survey among SaaS-providers and -customers to get a more representative view of the current state of affairs. Due to the other goal of this research, namely discovering the most effective tool to raise awareness for the continuity risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud, the risk of collecting insufficient and unsound information during the SaaS-provider interviews, was too large. Experts in the field of SaaS business continuity were required in order to debate and substantiate the properties of a possible, to be developed, tool. To ensure validity and reliability of the research, multi-source triangulation has been applied (Baarda, De Goede & Teunissen, 2001). Multi-source triangulation means multiple sources were used to elicit information. During this research three groups of SaaS business continuity experts were interviewed, as described above, with every group consisting of two or more respondents. These three groups allowed to collect and compare data from multiple perspectives. Motives, opinions, needs, interests and visions can heavily differ between groups (Baarda, De Goede & Teunissen, 2001).

Research ID	Organisation	Role of Interviewee	Expert Group
A1	AllSolutions	Team Leader Developers	A
A2	De Voorkant	Co-Owner	A
A3	ICT Group	Intern Manager	A
A4	Innovixion	Owner	A
A5	TimeTell	Owner(s)	A
B1	ACC ICT	Director	B
B2	Escrow4All	Director	B
C1	DHPA	Director	C
C2	NederlandICT	Jurist	C

**Table 1.** Organizations, role of interviewee and expert group.

Expert interviews can be described as “information gathering meetings” used primarily for collecting facts and knowledge from domain related experts. (Bogner & Menz, 2009). The interviews were set-up to be in-depth interviews, meaning they were semi-structured with open-ended questions, used to seek understanding and interpretation of domain related concepts (Guion & McDonald, 2011). In order to insure interaction during the interviews and understanding of the companies’ daily activities, all interviews were held at the interviewees’ office buildings.

After identifying expert groups and selecting them the next part of this qualitative research consisted of drafting an interview protocol. Especially since there are three groups of experts, each expert has been interviewed with a personalized interview protocol, to cover and capture every step in their choices, motives and opinions towards SaaS business continuity solutions. These interview protocols can be found in Appendix B. The creation

of the various interview protocols will be described in the next four sections. Since the interviews, which were conducted during this research, had to deliver information needed to compose survey questions in future research, the construction and substantiation of the interviews were of importance. If these interviews did not deliver unbiased, trustworthy and sufficient information, the whole research could have failed. The specification of the planned future research will be presented in section 4.3.1: SaaS Business Continuity at Dutch SaaS Customers.

To assure all aspects of the researchable topic would be covered correctly and sufficiently, the four-phase interview protocol refinement (IPR) framework of Castillo-Montoya (2016) has been applied. This framework is a guide for systematically developing and refining an interview protocol. The four-phase process includes: (1) ensuring interview questions align with research questions, (2) constructing an inquiry-based conversation, (3) receiving feedback on interview protocols, and (4) piloting the interview protocol (Castillo-Montoya, 2016). Each phase helps taking one step further toward developing a research instrument appropriate for the participants and congruent with the aims of the research (Jones et al., 2014). The IPR framework is a guide for such protocol and therefore highly flexible (Castillo-Montoya, 2016).

### 2.3.1 Aligning Interview Questions with Research Questions

In the case of this research, the interviews are used to elicit thoughts, opinions and background information about SaaS business continuity solutions in the business to business (B2B) SaaS-sector. The questions help participants tell their stories one layer at a time, but also need to stay aligned with the purpose of the study. To check the alignment of questions, a matrix has been created to map interview questions onto research questions (Castillo-Montoya, 2016). Table 2 offers a brief overview of the matrix, related to interviews with SaaS-providers, with interview question numbers listed in rows and research question numbers in columns. As Neumann (2018) suggested, the cells in which a particular interview question had the potential to elicit information relevant to a particular research question were marked with an “X”. The full interview protocol matrix of the SaaS-providers and those of the other two expert groups can be found in Appendix C.

The process of creating these matrixes exposed several gaps in what was being asked. Interview questions were assessed, adjusted and added to ensure every research question was going to be answered satisfactory during the interviews. The creating of the matrixes also helped to observe the exact moment questions had to be asked (e.g. beginning, middle, end). Ideally, the researcher asks the questions most connected to the study’s purpose in the middle of the interview after building rapport (Rubin & Rubin, 2012). Once it was clear which interview questions were most likely to address which research questions, they were marked in the final interview protocol as key questions to ask during the interview (Castillo-Montoya, 2016).

Interview Question	Background Information	RQsub1	RQsub2	RQsub3	RQsub4
1.	X				
2.	X				
3.	X				
4.	X				
5.	X				
6.	X				
7.		X	X	X	
8.		X	X	X	
9.		X	X	X	X
10.		X	X	X	X
11.		X	X	X	
12.		X			
13.		X			
14.		X	X	X	
15.		X		X	
16.		X	X	X	
17.		X	X	X	
18.		X	X	X	
19.		X	X		
20.		X	X	X	
21.	X	X	X	X	X
22.					

**Table 2.** Interview Protocol Matrix of SaaS-Providers.

### 2.3.2 Constructing an Inquiry-Based Conversation

The interview protocol enables both asking questions for specific information related to the aims of the study as well as conversating about a particular topic (Patton, 2015). Castillo-Montoya (2016) refers to this balance between inquiry and conversation as an inquiry-based conversation. This phase of constructing the interview protocols used for this research entails the researcher with: a) interview questions written differently from the research questions; b) an organisation following social rules of ordinary conversation; c) a variety of questions; d) a script with likely follow-up and prompt questions. As described in section 2.3.1: Aligning Interview Questions with Research Questions, research questions are different from interview questions. Brinkmann and Kvale (2015) stated, “The researcher questions are usually formulated in a theoretical language, whereas the interview questions should be expressed in the everyday language of the interviewees” (p. 158). As such, the researcher should consider terms used by participants and ask one question at a time (Merriam, 2009). Clarifying questions were added to the protocols in case the answer given by the interviewee could possibly not satisfy the researcher’s intention. Also, questions from the position of why were avoided. An interview participant may perceive “why”-questions as judgmental (Rubin & Rubin, 2012).

The interview protocols were composed based on four types of questions: (1) introductory questions, (2) transition questions, (3) key questions and (4) closing questions. With these types of questions, the conversational and inquiry goals of the research were preserved (Creswell, 2007; Krueger & Casey, 2009; Merriam, 2009; Rubin & Rubin, 2012). The introductory questions served to begin the interview and get to know some facts about the interviewee and the organisation. In order to insure interaction during the interviews and understanding of the companies’ daily activities, all interviews were held at the interviewees’ office buildings. This start of the interview helped to set the tone of a conversation, but also distinguished the interview as a form of inquiry

(Castillo-Montoya, 2016). The transition questions moved the interview towards the key questions (Krueger & Casey, 2009) and keep the conversational tone of the interview. In between sections and topics, expressions of gratitude were added to clarify the transition towards another topic. Key questions, also referred to as main questions, tend to solicit the most valuable information (Krueger & Casey, 2009; Rubin & Rubin, 2012). The interviewees' answers to the series of key questions were instrumental to the researcher's learning of their awareness and knowledge of SaaS business continuity solutions, and led to insights of how SaaS business continuity solutions work, where the demand for such solutions come from and why those solutions are necessary. The questions allowed to form statements and analyse those statements to arrive at a finding about the differences and similarities in interviewees' choices, motives and opinions. These statements can be found in section 2.4.1: SaaS-Provider Interview Statements. At the end of the interviews, participants were provided the opportunity to raise any issues not addressed. The questions in this section provided the participants an opportunity to insert information and reflect, but also signalled a conclusion (Castillo-Montoya, 2016). The overall organisation of questions (beginning, transitional, key, and closing questions) shaped the interview protocols towards an inquiry-based conversation.

### 2.3.3 Receiving Feedback on the Interview Protocol

The questions in the interview protocol matrix are developed both to be "conversational and likely to elicit information related to the study's research questions" (Castillo-Montoya, 2016, p. 16). Receiving feedback on the developed interview protocol belongs to the next phase of the IPR framework. According to Castillo-Montoya (2016), "the purpose of obtaining feedback on the interview protocol is to enhance its reliability - its trustworthiness - as a research instrument" (p. 16). Feedback can provide the researcher with information about how well participants understand the interview questions and whether their understanding is close to what the researcher intends or expects (Patton, 2015).

Table 3 shows a checklist for proofing the interview protocols. Checking has been done for structure, length, writing style, and comprehension. The person doing the close read of the interview protocol checked that the interview questions "promote a positive interaction, keep the flow of the conversation going, and stimulate the subjects to talk about their experiences and feelings. They should be easy to understand, short, and devoid of academic language" (Brinkmann & Kvale, 2015, p. 157). The person doing the close read should put themselves in the place of the interviewee in order to anticipate how they may understand the interview questions and respond to them (Maxwell, 2013).

Close reading has been performed by two fellow researchers and two employees of ACC ICT. With the use of the feedback checklist below, the interview protocols were refined until all questions were accessible and understandable. By refining the interview protocols, their quality and trustworthiness were enhanced (Castillo-Montoya, 2016).

<b>Aspects of an Interview Protocol</b>	<b>Yes</b>	<b>No</b>
<b><i>Interview Protocol Structure</i></b>		
Beginning questions are factual in nature.		
Key questions are majority of the questions and are placed between beginning and ending questions.		
Questions at the end of interview protocol are reflective and provide participant an opportunity to share closing comments.		
A brief script throughout the interview protocol provides smooth transitions between topic areas.		
Interviewer closes with expressed gratitude and any intents to stay connected or follow up.		
Overall, interview is organized to promote conversational flow.		
<b><i>Writing of Interview Questions &amp; Statements</i></b>		
Questions/statements are free from spelling error(s).		
Only one question asked at a time.		
Most questions ask participants to describe experiences and feelings.		
Questions are mostly open ended.		
Questions are written in a non-judgmental manner.		
<b><i>Length of Interview Protocol</i></b>		
All questions are needed.		
Questions/statements are concise.		
<b><i>Comprehension</i></b>		
Questions/statements are devoid of academic language.		
Questions/statements are easy to understand.		

**Table 3.** Activity Checklist for Close Reading of Interview Protocol.

#### 2.3.4 Piloting the Interview Protocol

Since the IPR Framework serves as a guide, it is highly flexible (Castillo-Montoya, 2016). For this research, phase four has been edited to fit the limitations and possibilities of it. Phase four is meant to pilot the refined interview protocol with people who mirror the characteristics of the sample to be interviewed for the actual study (Maxwell, 2013). Merriam (2009) pointed out that the “best way to tell whether the order of your questions works or not is to try it out in a pilot interview” (p. 104). A limitation of this research is that it had a very specific and hard to find group of participants. Therefore, the interview protocol has not been tested on people who mirror the characteristics of the domain experts. Castillo-Montoya (2016) stated that “some researchers may not have the time, money, or access to participants to engage in a piloting phase. In that case, phase 3 (feedback) becomes even more crucial to refining the interview protocol” (p. 19).

As described in the previous section, multiple feedback sessions have taken place with various experts and fellow researchers in the field of SaaS business continuity. First, the SaaS-providers interview protocol had been composed by the researcher and has been reviewed by the experts. The interview protocol has been refined various times and has been tested at ACC ICT after that. As an alternative to piloting the interview protocol with people that mirror the characteristics of the sample to be interviewed, the first, and most accessible, group of experts has been used to pilot the interview protocol and to try out the research instrument. Although gathering information was successful and no changes were made during or after the period of interviewing SaaS-providers, the lack of a true piloting phase may have negatively influenced the interview results. Possibly, the interview protocol would have been further refined if a pilot group could have been used. The other two interview protocols have been derived from the SaaS-providers’ interview protocol after all interviews with that group of experts were completed. The results of the interviews with SaaS-providers helped to improve the interview protocols of the SaaS business continuity solution providers and the IT interest groups. Especially the last questions, which provided the participants an opportunity to speak freely about future developments and insert information, helped improving the interview protocols of the other two expert groups.

## 2.4 Analysis

### 2.4.1 SaaS-Provider Interview Statements

As explained in section 2.3.1: *Aligning Interview Questions with Research Questions*, the research questions have been mapped into interview questions, with the use of the interview protocol matrixes. The interviewees' answers to the series of key questions were instrumental to the researcher's learning of their awareness and knowledge of SaaS business continuity solutions, and led to insights of how SaaS business continuity solutions work, where the demand for such solutions come from and why those solutions are necessary. The interview protocol encouraged respondents to talk freely about choices, motives and opinions, but at the same time it offered the opportunity to judge SaaS-providers based on statements. The questions allowed to form statements concerning business continuity solutions at SaaS-providers and analyse those statements to arrive at a finding about the differences and similarities in interviewees' choices, motives and opinions. Transcribing and coding this part of the SaaS-providers' interviews would have costed much more time and effort, while it probably would have delivered the same results. During the interviews, notes were taken which could later be transformed into answering the statements. Also, the interviews were recorded using an audio recorder, so that interesting parts of the interviews could still be transcribed and quotes could be used to describe and substantiate one's choices, motives or opinions. The statements will be introduced in section 3.2: *Interview Results*.

### 2.4.2 Sparring Sessions

During the interviews with various parties, in the closing part, there was room to spar about the future possibilities of business continuity solutions, responsibilities at SaaS-providers and end-users, and possible regulations from the government towards the General Data Protection Regulation (GDPR). The main goal of these sparring sessions was to discover the most effective tool to raise awareness for the risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud. As described in section 2.3.2: *Constructing an Inquiry-Based Conversation*, all interviews were held at the interviewees' office buildings to insure interaction during the interviews. Especially during this part of the interview, this helped immensely in keeping the conversation going and in keeping the ideas coming up. The interviews were recorded using an audio recorder, so that interesting parts of the interviews could still be transcribed and quotes could be used to describe and substantiate one's choices, motives or opinions.

## 3 Results

This chapter describes the results of the literature study and the expert interviews. First, the results of the literature study will be described, starting by explaining what business continuity means. Business continuity goes hand in hand with business interruptions. These terms do not just relate to IT, but apply to every company. Business critical cloud computing will be described, starting with what cloud computing – in specific SaaS – is and to what extent companies are depending on it. In the following section, SaaS business continuity threats will be described. The last section of the literature study focusses on the SaaS business continuity solutions which can be demanded by end-users and be adopted by SaaS-providers.

Right after, the interview results will be discussed. The SaaS-providers' interviews discussed themes such as customer demand for business continuity solutions, use of business continuity solutions, what business continuity solution SaaS-providers (would) use and why, what would happen to their customers if their company unexpectedly disappears, and what problems they would face and what data the end-user would lose. First off, the SaaS-providers will be graded on the interview statements. Additionally, their visions towards SaaS business continuity solutions will be described. Finally, the grading on the statements will be reflected on their visions and

opinions, and their visions towards the development of the most effective tool to raise awareness at Dutch SaaS-providers and end-users who did not think of this subject yet will be documented.

The chapter continues with the interview results of the SaaS business continuity solution providers. The interviews with the SaaS business continuity solutions providers were conducted to gather detailed information about how their continuity solution works, why they offer such solution, how many experience they have in interfering in case of bankruptcy at SaaS-providers' level, how their customer acquisition works, how they try to raise awareness themselves and what their vision is on how awareness could be raised in the most effective manner. Lastly, the results of the interviews with IT interest groups will be discussed. They were asked for their vision towards the need, supply and demand for SaaS business continuity solutions, which SaaS business continuity solution they would prefer for their members and why, and what they have arranged for their members with respect to these solutions.

## 3.1 Literature Study

### 3.1.1 Business Critical Cloud Computing

The SaaS-model is fundamentally different from the traditional software-licensing model. The difference is that the customer does not possess the object-code on-premises but, instead, accesses the application on a remote server, using the internet. This remote server is managed by the SaaS-provider, either on-site or by using a hosting-provider. The actual hardware where the software and data reside is out of the customer's reach and control. Some SaaS-solutions even include content from third-party content providers in their SaaS-solution. A customer does not have anything to do with all those external parties, and commonly they do not even know that external parties are being employed. The customer pays its SaaS-provider for access to the software and the SaaS-provider in his turn pays the different parties involved to deliver its service. Figure 1 describes a simplified version of a standard SaaS-application.

This research focusses on business-critical SaaS-application. Enterprise Resource Planning (ERP) software is business-critical software. In the core, this software is meant to support business processes, but in practice customers often fully rely their business operation on such system. An ERP program usually consists of small sub-programs (modules) that all support a specific task. Where previously companies used different programs to support their business activities, a number of processes (departments) can be accommodated in an ERP program. A consequence of such an ERP system is that data from, for example, customers and products only needs to be entered once within the organization, because a single database is used for all business activities. In addition to reducing the chance of inconsistent and redundant data, an ERP system can offer many other benefits such as a more efficient way of working, better communication and possibly cost reduction.

When it comes to business-critical processes, organizations are increasingly adopting SaaS-solutions in favour of traditional on-premise solutions. The rise of Software-as-a-Service brought advantages in terms of cost reduction, maintenance time, mobility and scalability. Yet, running business-critical processes in the cloud, in the form of an ERP for example, brings new risks. If the SaaS-provider disappears, the payment towards the hosting-provider stops and the hosting-provider will discontinue hosting the application and data. As a result, the customer does not have access to either of these any longer. Some companies see these risks as an ultimate downside for outsourcing their IT to an external service provider, and use it as an argument to stick to the traditional on-premise software (Spiotto & Spiotto, 2003).

### 3.1.2 SaaS Business Continuity Threats

The availability of business-critical applications, such as ERPs, relies on the robustness of the SaaS-provider and its underlying parties. The business continuity disruption situations include (in order of importance):

- S1.* SaaS-provider going out of business
- S2.* Hosting-provider going out of business
- S3.* Datacentre going out of business

Since SaaS-providers can be found on every corner of the street these days, the most probable situation that could occur is a SaaS-provider going bankrupt or going out of business. Most SaaS-providers chosen by SMEs do not have more than one or two software developers. Sometimes, SaaS-providers even hire third parties to build the web interfaces of the SaaS ERP solution, because they do not have the expertise or capability themselves. Most hosting-providers have lots of both business and private customers, and have a continuous and predictable flow of income. Although the chance of such hosting-provider going bankrupt is small, the impact may be large. Just a step higher, at datacentre level, the chances of bankruptcy will be smaller, but because of its scale consequences will be even larger.

These underlying parties are businesses SMEs will probably never be in touch with. They have contracts and SLAs with SaaS-providers, hosting services and even with companies at their own level. That is because hosting parties, for example, demand their datacentre to have agreements with other datacentres as a backup in case of emergency. As SaaS-providers demand their host to offer such guarantees, and hosting parties demand their datacentres to offer such guarantees, the question why end users do not demand their SaaS-provider these guarantees, raises.

Unexpected bankruptcy of a SaaS-provider can lead to loss of data or catastrophic downtime (Lucassen, Van Rooij, & Jansen, 2013). If a company is using mission-critical software that is hosted off-premises, it could get into big problems when the SaaS-provider decides to pull the plug. The business continuity risks include (in order of importance) (Van De Zande & Jansen, 2011):

- R1.* Lose access to data
- R2.* Lose access to the application
- R3.* Lose support and maintenance

The impact and consequences of these risks should be discussed and reported in a Service License Agreement (SLA). SLAs are legal documents where customer and provider agree on the quality of service, by quantifying minimum quality of service (Hiles, 1994). For SaaS, these mostly discuss availability and response time. Although these two factors are part of business continuity, they do not cover continuity risks as a whole. Worst case disaster scenario's, like a SaaS-provider going out of business because of bankruptcy for example, were left aside. This is mainly because customers assumed the SLA would include these scenarios, while it did not. On the other hand, SaaS-providers did not feel the need to include those (expensive) services, because SaaS-customers rarely ever asked for them (Van De Zande & Jansen, 2011).

### 3.1.3 SaaS Business Continuity Solutions

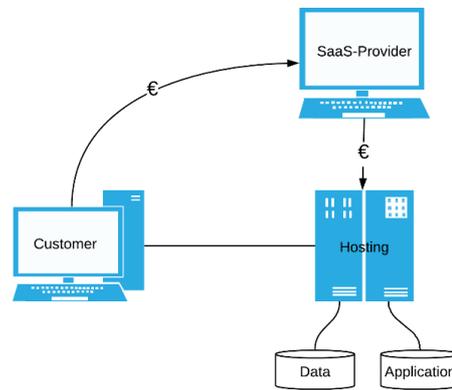
The main goal with a business continuity arrangement is the assurance that the customer continues to have access to his SaaS-application and data, even if the SaaS-provider disappears. To make the continuation of access and data work, several key elements should be covered. In this section, business continuity solutions are discussed and compared with the requirements for a successful business continuity guarantee. According to Van De Zande & Jansen (2011) required components for a complete SaaS business continuity solution are (in order of importance):

- 
- C1. Own Backup:** Every SaaS-customer should be able to download all of its data.
  - C2. Hosting Insurance:** A third party should create an arrangement with the hosting-provider to continue hosting even if the SaaS-provider fails.
  - C3. Arrangement with content providers:** If the SaaS-application contains (paid) content from third parties, they should also continue providing the content.
  - C4. Support and maintenance for the application:** If the SaaS-provider disappears, the customer also loses support. A third party could try to continue support for the application.

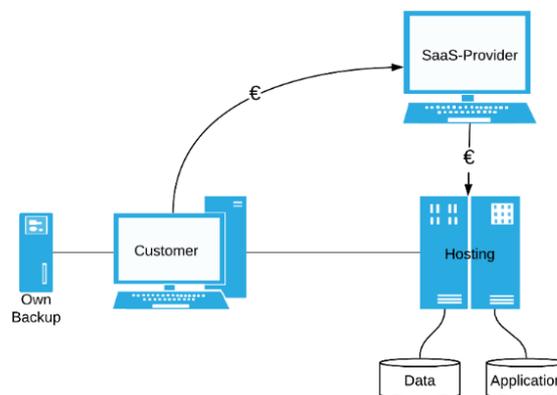
As stated in component 1, the first and most important step towards better business continuity would be to receive, or at least be able to acquire, regular backups of the data. This would preferably be in a common form like XML or CSV. Figure 2 describes such solution. For some SaaS-customers, this would be enough to satisfy their business continuity concerns, because they do not depend on the SaaS-application that much and could relatively easily function without it for a couple of days or even weeks.

Several companies offer business continuity solutions for SaaS-providers and/or their customers. These companies can either be a SaaS-escrow provider or a hosting-provider with a continuity guarantee plan. SaaS-escrow providers often operated as a source-code escrow for traditional on-premise software. Most escrow-providers have added a 'SaaS-escrow' service to their product portfolio (Van De Zande & Jansen, 2011). With SaaS-escrow, as opposed to traditional escrow services, the initial purpose of storing the source-code and releasing it to the customer on certain release-events is less important than the continuation of application access. Figure 3 describes this next step towards a more complete SaaS business continuity solution. Most SaaS-customers would not have any use for the source-code, because they probably do not have the hardware and infrastructure to deploy the software application on-premises. As an added value, the escrow company can offer support and maintenance for the SaaS-application, by storing documentation and remaining in contact with key-persons involved with the software-maintenance at the SaaS-provider. So, with SaaS-escrow, the escrow-provider acts more like an insurance company for hosting costs than a storage facility for sensitive information. An alternative for SaaS-escrow providers can be found in innovative hosting-providers. Certain hosting-providers are starting to realise they can distinguish themselves from competing colleagues by setting up a business continuity guaranteeing solution as an alternative for a SaaS-escrow solution. This hosting continuity is a kind of insurance that will guarantee continuation of SaaS-applications and its data for a predetermined amount of time, after the SaaS-provider concerned faced bankruptcy. In case of the hosting-provider being the business continuity solution provider at the same time, a SaaS-provider usually pays its hosting-provider a pre-agreed percentage for the business continuity solution. So, the price of the business continuity solution is an additional percentage of the monthly or annual payment for hiring hardware and software at the hosting-provider. For hosting-providers, it could be a logical step to introduce such insurance, because they already take care and responsibility of hosting the software and data, providing that they guarantee excellent service and uptime guarantees in the first place. The ambition to arrange everything to the last detail results in datacentre independent infrastructures, extreme uptime guarantees and thus high responsibilities and accountabilities, which allow hosting-providers to offer continuity guarantees and naturally bring additional costs. Hosting-providers with an insufficient foundation, focussing on quantity instead of quality, are unable to guarantee continuation of services in case of bankruptcy because of small margins. Though, the insurance naturally becomes more effective and cheaper with every additional SaaS-provider and its customers, because the chance that all of the SaaS-providers fail at the same time is lower than the chance that one of them fails.

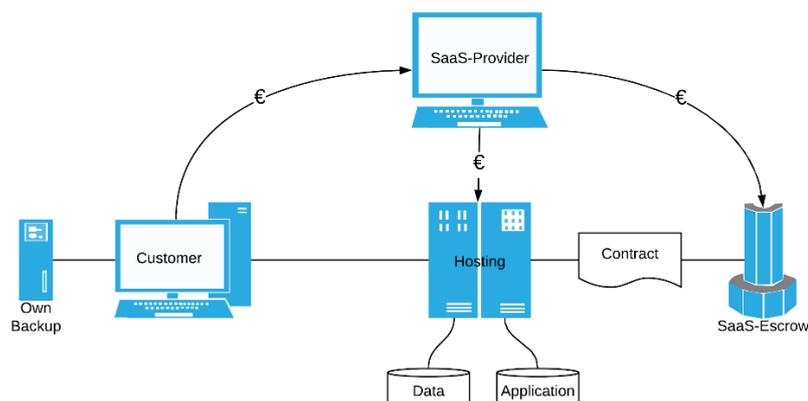
SaaS-providers that build business-critical applications which use a lot of third-party content in their application could think of funding their own business continuity foundation. Typical escrow solutions do not offer support for SaaS-applications which use a lot of third-party content, because they only cover continuation of payment towards the hosting-provider, but not the payment towards third-party content-providers. The same applies to SaaS-providers who use a lot of different hosting-providers to host their application, for example to provide better reliability and speed for customers around the world. The escrow-provider then should sign a contract with every single one of those content- and hosting-providers to be able to assure full continuation of the SaaS-application.



**Fig. 1.** A simplified SaaS-setup. The customer does not possess the object-code on-premises but, instead, accesses the application on a remote server, using the internet. This remote server is managed by the SaaS-provider, either on-site or by using a hosting-provider. The actual hardware where the software and data reside is out of the customer's reach and control. The customer pays its SaaS-provider for access to the software and the SaaS-provider in his turn pays the different parties involved to deliver its service.



**Fig. 2.** A diagram showing the first step towards better business continuity; a backup of data residing with the customer. The most important step towards better business continuity would be to receive, or at least be able to acquire, regular backups of the data. This would preferably be in a common form like XML or CSV. For some SaaS-customers, this would be enough to satisfy their business continuity concerns, because they do not depend on the SaaS-application that much and could relatively easy function without it for a couple of days or even weeks.



**Fig. 3.** The second step towards a more complete business continuity solution. A separate legal entity with an arrangement with the hosting-provider. Several companies offer business continuity solutions for SaaS-providers and/or their customers. SaaS-escrow providers often operated as a source-code escrow for traditional on-premise software. Most escrow-providers have added a 'SaaS-escrow' service to their product portfolio. With SaaS-escrow, as opposed to traditional escrow services, the initial purpose of storing the source-code and releasing it to the customer on certain release-events is less important than the continuation of application access.

## 3.2 Interview Results

The interviews were held in May, June and July 2019. As described in section 2.3.4: Piloting the Interview Protocol, the most accessible group of experts was interviewed first. This group consists of SaaS-providers who made a substantiated choice towards offering a business continuity solution for their customers. Interviews with this group helped drawing up and improving the interview protocols for SaaS business continuity solution providers and IT interest groups, by sparring on the subject. After the interviews with the SaaS-providers were completed and processed, the interviews with the other two groups of experts started.

As described before in section 2.4.1: SaaS-Provider Interview Statements, a large part of the interviews is processed with the use of statements. The interview protocol encouraged respondents to talk freely about choices, motives and opinions, but at the same time it offered the opportunity to judge SaaS-providers based on statements. These statements describe facts, choices, and motives, and can be answered with yes or no. Some statements are used to describe a SaaS-provider's business and provide context. Others play a key role in answering the research sub-questions. Below, all interview questions have been transformed into fifteen statements.

*Statement 1: SaaS-providers build business-critical software.*

Enterprise Resource Planning (ERP) software is a perfect example of business-critical software. In the core, this software is meant to support business processes, but in practice customers often fully rely their business operation on such system. An ERP-program usually consists of small sub-programs, also known as modules, that all support a specific task. Where previously companies used different programs to support their business activities, a very large number of processes (departments) can be accommodated in an ERP program. A consequence of such an ERP system is that data from, for example, customers and products only needs to be entered once within the organization, because a single database is used. In addition to reducing the chance of inconsistent data, an ERP-system can offer many other benefits such as a more efficient way of working, better communication and possibly cost reduction. Yet, running business-critical processes in the cloud brings new risks. If the SaaS-provider disappears, the payment towards the hosting-provider stops and the hosting-provider will discontinue hosting the application and data. As a result, the customer does not have access to either of these any longer. Some companies see these risks as an ultimate downside for outsourcing their IT to an external service provider, and use it as an argument to stick to the traditional on-premise software (Spiotto & Spiotto, 2003). Therefore, business continuity solutions are considered to be more important and valuable for ERPs than for example for an Application Programming Interface (API), which are “defined interfaces through which interactions happen between an enterprise and applications that use its assets” (Rudrakshi et al., 2014). These applications are often used to facilitate retrievable information from other organisations, like address data. Although those supporting APIs are helpful, they can be lived without.

*Statement 2: SaaS-providers made a substantiated choice towards business continuity solutions.*

Regardless of whether a SaaS-provider has a business continuity solution for its customers or not, all SaaS-providers interviewed during this research made a substantiated choice towards adopting business continuity solutions. Some providers chose to not introduce a business continuity solution after investigating the benefits and costs for both themselves and their customers. Others chose to guarantee limited business continuity, by guaranteeing business continuity in case they go bankrupt themselves or by guaranteeing business continuity for their customers in case the hosting-provider faces bankruptcy. The remaining group of SaaS-providers offer the full business continuity solution package concerning bankruptcy.

*Statement 3: Motivation for looking into business continuity solutions was a demand or requirement from a (potential) customer.*

The motivation to investigate the possibilities, necessity, benefits and costs of a business continuity solution must come from somewhere. In general, the direct cause for a SaaS-provider looking into business continuity solutions can be two things. Either the SaaS-providers feels responsible for its customers' business continuity and wants to proactively investigate the risks and possibilities regarding business continuity, or a (potential) customer demands for guaranteed business continuity in case of bankruptcy of underlying parties and the SaaS-provider

behaved reactive. This statement is a key statement concerning the answering of sub-question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 4: SaaS-providers offer their customers a business continuity solution.*

Statement 4 indicates whether a SaaS-provider chose to adopt a business continuity solution, after investigating the benefits and costs. As can be derived from Statement 3, benefits and costs could relate to acquiring or losing (potential) customers, if a customer demands a continuity solution. This statement is a key statement concerning the answering of sub-question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 5: SaaS-providers developed their own business continuity solution.*

There are multiple solutions to guarantee continuity of SaaS-applications. One of those solutions is a measure developed by the SaaS-provider itself. This can, for example, be a user group or a guarantee fund. These solutions will be discussed in section 3.1.3: SaaS Business Continuity Solutions. This statement is a key statement concerning the answering of sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*, and sub-question three: *“Which solutions can Dutch SaaS-providers offer their customers in order to guarantee business continuity?”*.

*Statement 6: SaaS-providers use a third-party business continuity solution.*

SaaS-providers often consist of a team that is highly specialised in the technical side of SaaS, or IT in general. Business continuity solutions, on the other hand, are legal agreements. A third party can be approached to take care of this problem. This legal entity can either be an escrow-provider or the hosting-provider. Such a separate entity can also provide some additional services next to simply continuing hosting (and providing the funds to do so). They could also offer (temporarily) support for the application when the SaaS-provider fails to do so, and help in the search for a new SaaS-provider to take over activities. This statement is a key statement concerning the answering of sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*, and sub-question three: *“Which solutions can Dutch SaaS-providers offer their customers in order to guarantee business continuity?”*.

*Statement 7: SaaS-providers guarantee business continuity for end-users in case of themselves going bankrupt.*

Business continuity solutions can be divided into at least two layers. The first layer of business continuity solutions consists of SaaS-providers. Unexpected bankruptcy of a SaaS-provider can lead to loss of data or catastrophic downtime (Lucassen, Van Rooij, & Jansen, 2013). If a company is using business-critical software that is hosted off-premise, it could get into big problems when the SaaS-provider decides to pull the plug. To prevent loss of data or catastrophic downtime issues, SaaS-providers can offer guaranteed continuity of these business-critical information system and its data, by making agreements with their hosting-provider. This statement is a key statement concerning the answering of sub-question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 8: SaaS-providers guarantee business continuity for end-users in case of the hosting-provider going bankrupt.*

As Statement 7 describes, bankruptcy can occur in multiple layers throughout the software and data supply chain. The second layer is the hosting-provider running the possibility of facing bankruptcy. If a hosting-provider faces bankruptcy, SaaS-providers and end-users of their software are left to fate, if no continuity guaranteeing agreements have been made between the SaaS-provider and the hosting-provider. By making such agreements, SaaS-providers are assured of continuity of their own DTAP-environment and continuity of the software and data their end-user needs to run business processes. This statement is a key statement concerning the answering of sub-

question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 9: SaaS-providers guarantee business continuity for end-users in case of data encryption by mal- and ransomware.*

In fact, business continuity risks for SaaS go further than just bankruptcy in the software supply chain. A full disaster recovery service for end-users also covers disasters related to data encryption by mal- and ransomware (Daly, 2017). This statement is a key statement concerning the answering of sub-question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 10: Use of business continuity solution is initiated by the end-user.*

The use of a business continuity solution can be either the initiative of the end-user or a suggestion by the SaaS-provider. This statement is a key statement concerning the answering of sub-question one: *“To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?”*, and sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 11: Business continuity solution for customers is optional.*

As a business continuity solution is much like an insurance, it logically brings costs to make use of one. As with every insurable risk, a benefits-to-costs-analysis must be conducted to investigate the value of the insurance. It differs from SaaS-provider to -provider if they let the customer choose to make this insurance contract, or if they offer the business continuity solution as a standard service. This statement is a key statement concerning the answering of sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 12: Business continuity solution is part of the SaaS-providers’ business model.*

Offering a business continuity solution for end-users could be part of the SaaS-provider’s business model. It could make a provider more attractive related to competitors who do not offer such solution. SaaS-providers could use this extra service or possibility as part of the sales pitch when acquiring new customers or extend contracts with existing customers.

*Statement 13: SaaS-providers feel more attractive towards new customers by offering a business continuity solution.*

Using the extra business continuity service as part of the sales pitch is one thing, but creating appreciation from (potential) customers is another thing. Size of customer and size of SaaS-provider, the type of application, the extent to which continuity is discussed during negotiations and the difference of a “standard extra” or “optional extra”, could have effect on the customer’s appreciation.

*Statement 14: Business continuity solution costs are charged to customers.*

As mentioned in Statement 11, an insurance brings additional costs. These costs can either be paid by the SaaS-provider or be passed on to its customers. Depending on the type of business continuity solution, the costs for a SaaS-provider could be fixed and thus independent on the number of end-users, or the costs could rise with the addition of every customer. This statement is a key statement concerning the answering of sub-question two: *“To what extent do Dutch SaaS-providers feel responsible for their customers’ business continuity?”*.

*Statement 15: Business continuity solution is part of the SaaS-providers’ revenue model.*

Since costs can be passed on to the customer, there is an opportunity for SaaS-providers to make extra money of their customers. It is not unusual for an entrepreneur to profit a few percent on a service or product provided by a third party. As a matter of fact, for some business models, it is the whole revenue model. Logically, the business continuity solution provider charges the SaaS-provider more money for the solution than it costs. For the business

---

continuity solution provider, it is part of its revenue model, and so it could be for the SaaS-provider. The SaaS-provider could charge a customer more money on top of their own product – the SaaS ERP system for example – then the business continuity solution costs.

This chapter describes the interview results per expert group. First, the results of the interviews with SaaS-providers will be described. The adoption of SaaS business continuity solutions at SaaS-providers will be judged with the help of the previously drawn up statements. The interview results will be described around the SaaS-providers' statements. Also, their visions towards the future of business continuity solutions and the most effective manner or tool to raise awareness for the subject are discussed. This chapter continues with a section in which the results of interviews with SaaS business continuity solution providers will be described. Lastly, the results from the IT interest groups' interviews are given. Although the statements above are focussed on SaaS-providers, the interviews with SaaS business continuity solution providers and the IT interest groups will be displayed around the statements.

### 3.2.1 SaaS-Provider Interviews

In the previous section the statements, used to review and analyse SaaS-provider interviews within this research, were drafted up and described. For the sake of convenience, the previously introduced interview statements have been listed again in the table below (Table 4). Since all statements can be answered with yes or no, a large part of the results of the SaaS-provider interviews can be displayed clearly in a table. All statements have been listed in this table, together with all SaaS-providers involved in the research. Table 4 shows to what extent these Dutch SaaS-providers have incorporated business continuity solutions into their business model. To improve readability, the SaaS-providers have been given research IDs. The IDs have been assigned as below:

- A1. AllSolutions
- A2. De Voorkant
- A3. ICT Group
- A4. Innovixion
- A5. TimeTell

As stated before in section 2.4.1: SaaS-Provider Interview Statements, the interview protocol encouraged respondents to talk freely about choices, motives and opinions, but at the same time it offered the opportunity to judge SaaS-providers based on statements because of its semi-structured set-up. The statements can be answered with “yes” (Y) or “no” (N). The last column shows the percentage of interviewed Dutch SaaS-providers that scores positively (Y) on the concerned statement. Some statements were not applicable because of an answer to a previous statement. These excluded statements are filled in with a dash (-) and are neglected in the presented percentage.

<i>Statements</i>	A1	A2	A3	A4	A5	...%
<b>S1:</b> SaaS-providers build business-critical software.	Y	N	N	Y	N	40
<b>S2:</b> SaaS-providers made a substantiated choice towards business continuity solutions.	Y	Y	Y	Y	Y	100
<b>S3:</b> Motivation for looking into business continuity solutions was a demand or requirement from a (potential) customer.	Y	Y	Y	N	Y	80
<b>S4:</b> SaaS-providers offer their customers a business continuity solution.	Y	Y	N	Y	Y	80
<b>S5:</b> SaaS-providers developed their own business continuity solution.	N	N	-	Y	Y	50
<b>S6:</b> SaaS-providers use a third-party business continuity solution.	Y	Y	-	Y	Y	100
<b>S7:</b> SaaS-providers guarantee business continuity for end-users in case of itself going bankrupt.	Y	Y	-	Y	Y	100
<b>S8:</b> SaaS-providers guarantee business continuity for end-users in case of the hosting-provider going bankrupt.	Y	Y	-	Y	Y	100
<b>S9:</b> SaaS-providers guarantee business continuity for end-users in case of data encryption by mal- and ransomware.	N	N	-	N	N	0
<b>S10:</b> Use of business continuity solution is initiated by the end-users.	N	Y	-	N	Y	50
<b>S11:</b> Business continuity solution for customers is optional.	N	Y	-	N	Y	50
<b>S12:</b> Business continuity solution is part of the SaaS-providers' business model.	Y	N	-	Y	Y	75
<b>S13:</b> SaaS-providers feel more attractive towards new customers by offering a business continuity solution.	Y	N	-	Y	Y	75
<b>S14:</b> Business continuity solution costs are charged to customers.	Y	Y	-	Y	Y	100
<b>S15:</b> Business continuity solution is part of the SaaS-providers' revenue model.	N	N	-	N	N	0

**Table 4.** SaaS-providers' business continuity solution adoption table

The interview statements engage with the question how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. All SaaS-providers interviewed for this research have made a substantiated choice towards adopting a SaaS business continuity solution (Statement 2). SaaS-providers were selected on this criterium, which explains the 100 percent "Yes"-score. The SaaS-providers' motivation to investigate business continuity solutions must come from somewhere. For the interviewed SaaS-providers, the motivations for investigating the possibilities, benefits and costs of business continuity solutions were (in order of importance):

- M1.* Demand or requirement from a (potential) customer
- M2.* Sense of responsibility for end-users' business continuity
- M3.* Feeling of being ahead of the competition

80 percent of the SaaS-providers investigated these continuity solutions after the demand of a (large) customer (Statement 3), and therefore are reactive towards the investigation and adoption of such solution. The only proactive SaaS-provider in this research is Innovixion. Innovixion develops and provides business-critical SaaS-applications for various niche-markets. These niche-markets are too small to be attractive for large software developers. Innovixion being a small company itself, with only the director as its employee, Wingelaar understands

the continuity risk his customers run, by choosing Innovixion's ERP for their daily activities, like no other. If a SaaS-provider's target market consists of customers that do not realise the risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud, because of lack of knowledge for example, according to Wingelaar (Innovixion, 3 May 2019) a SaaS-provider should take responsibility of it.

Regardless of the motivation, all SaaS-providers made a substantiated choice towards the adoption of a business continuity solution (Statement 2) after investigating and evaluating both the SaaS-provider's and the SaaS-customers' benefits and costs, and the possible business continuity solutions as described in section 3.4.1: SaaS Business Continuity Solutions. According to the interviewed SaaS-providers, factors in deciding whether a business continuity solution would be adopted include (in order of importance):

- F1. SaaS-customer's feeling of necessity*
- F2. Monthly costs for the SaaS-provider*
- F3. Monthly costs for the SaaS-customer*
- F4. Sunk costs for the SaaS-provider*
- F5. Entering a new target market*
- F6. SaaS-provider's feeling of necessity*

Remarkable is that the SaaS-providers' perceptions of the necessity of a business continuity solution rarely is one of the factors in the decision-making process. If a customer thinks guaranteeing of software continuity is of importance, the SaaS-provider will practically always satisfy that need if fiscally feasible. Costs at various levels form the primary factors in the decision-making process of adopting a SaaS business continuity solution for end-users. Statement 4 shows that every company choose to adopt a business continuity solution after investigating the benefits and costs of such solution, except for ICT Group. ICT Group does not provide their customers true business-critical software (Statement 1), like an ERP, but they provide solutions for technical automation. Though, it has made a substantiated choice towards the adoption of a business continuity solution (Statement 2). ICT Group has investigated possibilities, benefits and costs of business continuity solutions, and decided to build and deliver (slightly) business-critical applications as on-premise solutions. The interviewee mentioned that the additional percentage a hosting-provider would charge for the business continuity solution is not dramatically high, but it becomes too expensive for the end-users of their software because the hosting-providers that offer these solutions are more expensive in the first place. Their specialty distinguishes them from being a dime a dozen. The ambition to arrange everything to the last detail results in datacentre independent infrastructures, extreme uptime guarantees and thus high responsibilities and accountabilities, which naturally bring additional costs. The alternative, namely making the more business-critical applications an on-premise solution, is much cheaper. ICT Group has the manpower to do so, in contrast to smaller software providers who focus on SaaS only. All other SaaS-providers within this research offer business continuity guarantees in case of their own company going bankrupt, and in case of their hosting-provider going bankrupt (Statement 7 & 8). The providing of SaaS-applications consists of a chain of responsibilities. Though, the guaranteeing of business continuity stays limited to bankruptcy. As statement 9 suggests, business continuity risks for SaaS go further than just bankruptcy in the software supply chain. A full disaster recovery service for end-users also covers disasters related to data encryption by mal- and ransomware. None of the interviewed SaaS-providers offers such Disaster Recovery-as-a-Service (DRaaS) for their customers. Reasons for not guaranteeing business continuity in case of data encryption by mal- and ransomware include (in order of importance):

- R1. No such demand from customers*
- R2. Source-code and infrastructure are designed to withstand attacks*
- R3. No such offering from business continuity solution providers*

This statement shows that the continuity guaranteeing market is mostly reactive and solution will only be provided from the moment it is requested by customers. Setting up a sound business continuity solution is serious business and requires a lot of time, money and effort (Wingelaar, R., Innovixion, 3 May 2019). In the end, it is everyone's benefit to arrange agreements between the provider and customer in such manner that the concerning risks are covered correctly. Statement 5 and 6 handle the way the business continuity solutions are arranged.

40 percent of the interviewed SaaS-providers have set-up their own business continuity solution. The reasons for developing an own business continuity solution include (in order of importance):

- R1. Cost reduction
- R2. Sense of involvement
- R3. Addition to user group agreements

Cost reduction is the most important reason for developing an own business continuity solution. These lower costs enable to make business continuity solutions affordable for SME SaaS-customers. Though, as can be derived from table 4, 100 percent of the interviewed Dutch SaaS-providers make use of a third-party business continuity solution (Statement 6). This means that the two SaaS-providers that developed their own business continuity solution also use a third-party solution to guarantee and provide full coverage, for example at hosting-provider level. These software providers use different business continuity solutions for their different product. TimeTell offers end-users of its on-premise products a business continuity solution through their TimeTell user group (Van Der Meer, J., TimeTell, 16 May 2019). For Software-as-a-Service, things seem to be more complicated and less easy to set-up adequately. The reasons for using a third-party business continuity solution include (in order of importance):

- R1. Lack of experience and expertise
- R2. Lack of time
- R3. Specific demand from a (potential) customer
- R4. Short term costs

Setting up a sound business continuity solution is very time consuming (Wingelaar, R., Innovixion, 3 May 2019), but to be able to understand the risks your customers run, involvement is of importance. In the end, it is everyone's benefit to arrange agreements between the provider and customer in such manner that the concerning risks are covered correctly. Sometimes, large (potential) customers demand a specific business continuity solution from a business continuity solution provider selected by them (Bruinenberg, M., De Voorkant, 8 May 2019). At government level, guidelines have been drawn up that describe that (semi-)government agencies may demand business continuity guarantees under all circumstances (Van Der Meer, J., TimeTell, 16 May 2019). These agencies almost always follow these guidelines, and often have specific wishes or demand. Furthermore, on the short term, choosing a third-party to arrange business continuity solutions can be cheaper for the SaaS-provider than developing one by its own, because of valuable time and effort that needs to be put in setting up such construction. Also, a SaaS business continuity solution set-up by the SaaS-provider itself often applies to every (new) customer, and is not an option (Statement 11). Costs at a third-party could be lower than the costs of developing an own continuity solution, if only a few customers demand or are willing to pay for continuity guarantees.

The initiative of using a SaaS business continuity solution has also to do with this (Statement 10). A large enterprise customer will always have thought about this subject before negotiations, and will therefore rarely ever agree on applying such solution when a SaaS-provider suggests the use of it, if they have already determined they are not in need of one (Bruinenberg, M., De Voorkant, 8 May 2019). As the respondents of this research said, many small businesses do not ask SaaS-providers about SaaS business continuity solutions, because they neither know about the risks nor the existence of such solutions. Secondly, when informed about these risks and possibilities during negotiations, it seems to be a far-flung event that does not weigh against higher annual costs of the SaaS-application. Therefore, De Voorkant does not initiate the use of a business continuity solution anymore, but still offers it as an option (Statement 10 & 11). Depending on the type and the daily dependencies of the application, costs play a significant role while choosing the right SaaS-provider for the job. Wingelaar (Innovixion, 3 May 2019) stated that potential customers would prefer his company when he (silently) includes the business continuity solution costs in the standard service, instead of stating it as an explicit extra (Statement 11). This means small customers, without knowledge of IT or knowledge about business continuity risks, do not want to pay for business continuity solutions, but they agree to pay a higher price if the service is a "matter of course". Van Der Meer (TimeTell, 16 May 2019) told the same during this interview. On one hand, customers accept a business continuity solution in the standard package and may prefer a SaaS-provider who provides a business continuity

solution above one that does not; even if it costs more money. On the other hand, if the business continuity solution is optional, and thus brings additional costs on the quotation during negotiations, customers rarely ever want the continuity solution. Appreciation from SME-customers seems to exist, but only as long as the business continuity solutions is “free” (Statement 13). Improved appreciation and attractiveness are covered by interview statement 13. The interview with De Voorkant revealed some interesting thoughts customers seem to have. Although De Voorkant offers their customers a business continuity solution (Statement 4), it does not feel more attractive because of it (Statements 12 & 13). Sometimes, it even feels like a threat for new businesses. Bruinenberg (De Voorkant, 8 May 2019) stated that the offering of the business continuity solution to cover the bankruptcy of his company made multiple, in particular smaller, potential customers insecure about the financial health of De Voorkant. That, of course, is not the emotion that should be created at end-users, when a SaaS-provider shows its best side. SaaS business continuity guarantees should increase trust in a provider’s competence, involvement, responsibility and its services (Wingelaar, R., Innovixion, 3 May). Therefore, De Voorkant does not mention the opportunity of using a business continuity solution, unless the (potential) customer takes initiative for it (Statements 10, 11 & 12).

Yet, as the results of statements 12 and 13 show, most SaaS-providers feel more attractive towards new customers by offering a business continuity solution, and they have implemented the business continuity solution into their business model. Once such solution construction is set-up, a new target market opens and brings advantages compared to the competitor. Since the offering of business continuity solutions can lead to more customers and projects, some SaaS-providers choose to split the costs of the business continuity solution between them and their customers (Van Der Meer, J., TimeTell, 16 May 2019), while others pass the costs on to the customer entirely (Statement 14). Though, none of the interviewed SaaS-providers stated that the offering of the business continuity solution was part of their revenue model (Statement 15). Business continuity solutions are considered to be rather expensive for the risk they cover, since the chances of bankruptcy are generally nil. If SaaS-providers would profit a few percent on the business continuity solution, it would become even more expensive, and chances are potential customers will pick a different SaaS-provider for the job (Kuindersma, Y., AllSolutions, 11 June 2019).

### 3.2.2 SaaS Business Continuity Solution Providers

Two SaaS business continuity solution providers have been interviewed during this research. Business continuity solution providers are companies which offer business continuity solutions for SaaS-applications. This offering can either be their core business, which in case of Escrow4All applies (Kui, H., Escrow4All, 24 May 2019), or a side activity, which applies to ACC ICT (Bijleveld, P., ACC ICT, 7 June 2019). Escrow4All offers a variety of escrow-services including SaaS-escrow. This SaaS-escrow ensures business continuity for end-users of online software in case their SaaS-provider faces bankruptcy. In this construction, the escrow-provider is a third party which gets paid by the SaaS-provider and draws up a contract with the hosting-provider to ensure continuity of SaaS-applications when the SaaS-provider fails to pay the hosting-provider. The other business continuity solution provider that was interviewed, ACC ICT, offers SaaS business continuity solutions as a side activity. It offers the business continuity solution in addition to their hosting services. ACC ICT is specialised in the hosting of business-critical SaaS-applications. As described before in section 3.1.3: SaaS Business Continuity Solutions, this hosting continuity is a kind of insurance that will guarantee continuation of SaaS-applications and its data for a predetermined amount of time, immediately after the SaaS-provider in dispute faces bankruptcy. SaaS-providers pay an additional percentage on top off the monthly payment towards the hosting-provider. For hosting-providers, it could be a logical step to introduce such insurance, because they already take care and responsibility of hosting the software and data, providing that they guarantee excellent service and uptime guarantees in the first place. The ambition to arrange everything to the last detail results in datacentre independent infrastructures, extreme uptime guarantees and thus high responsibilities and accountabilities, which allow hosting-providers to offer continuity guarantees and naturally bring additional costs. Hosting-providers with an insufficient foundation, focussing on quantity instead of quality, are unable to guarantee continuation of services in case of bankruptcy because of small margins. Though, the insurance naturally becomes more effective and cheaper with every additional SaaS-provider

and its customers, because the chance that all of the SaaS-providers fail at the same time is lower than the chance that one of them fails (Kui, H., 24 May 2019).

Both companies see a growing line in SaaS-providers adopting business continuity solutions for their end-users, but the average type of continuity demanding end-user is conspicuous. In the previous section, the results from the SaaS-providers show that only large companies, with their own IT-department, demand guarantees of continuity to prevent interruptions in their business processes because of bankruptcy in the software supply chain. Both SaaS business continuity solution providers endorse this. Large organisations such as governmental institutions, banks and insurance companies demand continuity guarantees. Sometimes, they even contact the business continuity solution provider directly instead of via the SaaS-provider. They want to make sure continuity guarantees are arranged in the way they want it to be (Kui, H., 24 May 2019). Micro-businesses and SMEs, especially those that are highly dependent on their SaaS-application, should be aware of continuity risks and think about the extent to which they need continuity guarantees from their software provider. It is a challenge though, because they often do not have the expertise and capacity to realise and evaluate risks, chances and consequences of SaaS continuity interruptions (Bijleveld, P., ACC ICT, 7 June 2019). Besides that, for small companies, costs play a huge role in selecting the right SaaS-provider. Entrepreneurs often see the business-critical software as supporting software. They do not realise how much interaction they have with this software, and to which extent they do rely on it (Kui, H., Escrow4All, 24 May 2019). As mentioned before, the core objective of ERPs is to support daily activities, but as it seems companies highly rely on it and cannot operate without (Wingelaar, R., Innovixion, 3 May 2019). ERP-software for micro-businesses and SMEs is normally no tailor-made software, and often consists of modules which can be turned on or off by the SaaS-provider (Kuindersma, Y., AllSolutions, 11 June 2019). This makes the ERP-software relatively cheap, and the additional costs of a business continuity solution would become a substantial part of the monthly payment.

To facilitate business continuity guarantees for micro-businesses and SMEs in a cost-saving manner, some providers choose to develop their own business continuity solution. Kui, director of Escrow4All, doubts the effectiveness and trustworthiness of these constructions. SaaS-providers could pretend to have a sound business continuity solution while in reality all they have arranged is a guarantee fund controlled by themselves. This could lead to a conflict of interest, still leaving the customer stand empty-handed in a worst-case scenario (Kui, H., Escrow4All, 24 May 2019). In the context of *“let the cobbler stick to his last”*, SaaS-providers and end-users should seek salvation in a third, independent party to take care of the business continuity solution. Setting up a business continuity solution is serious business and should not be done hasty and not only to please customers. According to both SaaS business continuity solutions providers, end-users should play a significant role in the commissioning of a business continuity solution for their SaaS-application. Bijleveld, director of ACC ICT, mentioned this would avoid sham security and improve SaaS business continuity solutions' quality. With the results of previous research in this field in his mind, Bijleveld is pleased to see that some SaaS-providers are being proactive towards adopting business continuity solutions and taking responsibility of their customers' business continuity, but critical applications should always come with critical questions from the end-user (Bijleveld, P., ACC ICT, 7 June 2019). The responsibility for making a business continuity solution agreement is not just the responsibility of the SaaS-provider nor the end-user of the online software. It is the cooperation between the two, or three when a solution provider gets involved, that matters. As the results from the interviews with SaaS-providers show, most of them believe initiative for the use of a business continuity solutions should come from the end-users, because they are the party running the real risk. But as long as (small) customers do not realise the need for some kind of business continuity solution, the situation remains as it currently is, and we are all waiting for a disaster to happen before measures will be taken. The bankruptcy of a SaaS-provider could cause disastrous consequences, which go further than business continuity disruption of the end-user of the application. Currently, in the unhoped-for event of a hosting-provider going bankrupt, if the bankruptcy trustee receives the servers, it is unsure what will happen with the, potential privacy sensitive, data stored on those machines. It would be in everyone's benefit if agreements were made about these servers with the use of, for example, a business continuity solution (Kui, H., Escrow4All, 24 May 2019). A bankruptcy trustee is not obliged to keep the service running, and could decide to liquidate all assets instead.

As in all interviews, during the interviews with the SaaS business continuity solution providers there was room for a discussion between the interviewee and the researcher towards the development of the most effective tool to increase awareness for SaaS business continuity risks and the solutions to cover those risks at both SaaS-providers and their customers. As described in the previous section, during the interviews with SaaS-providers two

possible measures or tools came to mind. Both measures should be able to change all parties involved from being reactive into being proactive. The first one, probably being the most effective but hardest to realise measure, is to legally require business continuity solutions for SaaS-applications. At least for SaaS-applications that manage and edit privacy sensitive information, this could be recorded in the recently updated General Data Protection Regulation (GDPR). With the GDPR, “the EU aims at regaining the people’s trust in the responsible treatment of their personal data in order to boost digital economy across the EU-internal market” (Voigt & Von Dem Bussche, 2017). Although both respondents think this is a very effective manner of guaranteeing SaaS business continuity, the measure might be too drastic. Not all types of SaaS-applications require (expensive) business continuity solutions, and forcing SaaS-providers to guarantee continuation of their software by law might destroy competitiveness in the market (Kui, H., 24 May 2019). Simple applications might become too expensive, because of additional (mandatory) costs. By making SaaS business continuity solutions a legal obligation the possibilities during negotiation diminish, and companies will go search for loopholes (Bijleveld, P., 7 June 2019). Besides, with the power of law, this burden is entirely placed on the shoulders of SaaS-providers, while the customers are the only real beneficiaries (Kui, H., 24 May 2019). Both SaaS business continuity solution providers believe there has to be a faster, easier and more appropriate way to success. Both the SaaS-provider and the SaaS-customer should be stimulated to investigate and appreciate business continuity risks, possibilities and needs for solutions. If the awareness for continuity risks businesses run by transferring their business-critical software to the cloud could be raised at SaaS-customers, the demand for such solutions will grow as a result and SaaS-providers will respond adequately, depending on their services and products, in order to be attractive and competitive (Bijleveld, P., 7 June 2019). And so, the other conception that came up during the interviews is the establishment of a (new) independent party that issues a certification mark towards SaaS-providers. Bijleveld told that ACC ICT has briefly investigated the possibilities, challenges and requirements for such certification mark in the past. He was positively surprised to hear that also some SaaS-providers see possible salvation in a medium that values SaaS-providers on the business continuity guarantees they offer their software’s end-users. A certification mark fits perfectly in the way ACC ICT sees the responsibility of SaaS-customers towards choosing the right SaaS-provider for their project. Until this very moment, there is little know-how about SaaS – or IT in general – and its possibilities, shortcomings and risks at micro-businesses and SMEs. Therefore, they cannot be blamed for not asking their SaaS-provider critical questions during negotiations. A certification mark could remedy and change this. Nowadays, for almost everything a consumer can buy, one can value a product’s quality, origin and safety using certification marks. In every sector, independent of IT, it is not just the responsibility of the vendor or producer to operate in a (socially) responsible manner, but also the responsibility and choice of the (business) customer to balance benefits and costs, and purchase the right product (Bijleveld, P., ACC ICT, 7 June 2019). According to Bijleveld, a certification mark for SaaS-providers should suffice. In principle, the SaaS-provider is the only party within the software supply chain a customer has contact with. The who, what, where, when and how does not matter in the customer’s eyes, as long as the organisation behind the certification mark investigates, evaluates and judges SaaS-providers in a structured and consistent manner, and issues the appropriate level of certification. This way, on one hand, both large and small (potential) customers can easily and effortlessly assess and compare SaaS-providers’ products and services without knowledge about the underlying technical constructions (Bijleveld, P., ACC ICT, 7 June 2019). SaaS-providers, on the other hand, can show their level of competence, involvement, and feeling of responsibility for their customers’ business continuity to increase customers’ trust in their products and services. Exactly what SaaS business continuity solutions are meant for.

### 3.2.3 IT Interest Groups

In July 2019, the last two interviews were held with IT interest groups. The purpose of these interviews was to discover their visions and opinions towards the behaviour of SaaS business continuity solution providers, SaaS hosting-providers, SaaS-providers and SaaS-customers with respect to SaaS business continuity solutions. Also, their daily activities and involvement in the topic were investigated. The two interviewed IT interest groups were NederlandICT and DHPA. NederlandICT is an interest group that represents over 600 companies in the digital sector, which include SaaS-providers and -developers. These members range from sole proprietors to listed companies. DHPA is the abbreviation for Dutch Hosting Provider Association. As the name suggests, DHPA

represents the interests of various market-leading Dutch hosting-providers. Interest groups deal with topics and problems that are relevant to their members. They try to relieve their members and arrange as much as possible as a collective (Tempelman, I., NederlandICT, 11 July 2019). Companies join IT interest groups for the following reasons (in order of importance):

- R1. Joining forces and having a say
- R2. Using of and getting discount on services and products IT interest groups offer
- R3. Projecting quality and professionalism
- R4. Staying abreast of the most recent developments in the sector
- R5. Learning from competing colleagues
- R6. Participating in workshops and networking meetings

The more members an interest group has, the more power and influence the interest group can exert. Joining forces and having a say is the most important reason to join an interest group for any business (Tempelman, I., NederlandICT, 11 July 2019). Furthermore, it is a great advantage to centrally arrange standard matters, in such manner that companies do not have to reinvent the wheel and companies can focus on the product or service they want to deliver (Tempelman, I., NederlandICT, 11 July 2019). According to Tempelman, using of and getting discount on services and products NederlandICT offers, is also one of the main reasons why both small and large companies join NederlandICT. For members of DHPA, the most important reasons for joining are joining forces, having a say, the projecting of quality and professionalism and staying abreast of the most recent developments in the sector (Alaerds, R., DHPA, 19 July 2019). In the scope of this research, these reasons and motivations can all be reflected on the arrangement of a business continuity solution for SaaS-providers and their end-users by these interest groups. Though, neither of these interest groups have arranged or developed their own business continuity solution for their members yet. While NederlandICT is not planning on doing so, because of limited demands (Tempelman, I., NederlandICT, 11 July 2019), DHPA is currently in the process of developing a business continuity solution for its members (Alaerds, R., DHPA, 19 July 2019). According to Alaerds, this is a very long-term project which has been going slow but steady for over two years. The Dutch Hosting Provider Association has conducted a survey among two-thirds of its members to discover the requirements for a collective SaaS business continuity solution for SaaS infrastructure-providers. In the meantime, the agreement has been made with various datacentres to continue hosting of software and data for one month in case a member of DHPA faces bankruptcy. This agreement could be realised because of the requirements that are set for (potential) members of DHPA. Members of DHPA are inspected before they can join the organisation. According to the IT interest groups, a sound business continuity solution includes the following aspects (in order of importance):

- A1. The risk that will be mitigated by the business continuity solution
- A2. The party that takes care of continuing hosting of application and data
- A3. The party that bears the costs of the transitional period
- A4. The duration of the transitional period
- A5. The consequences of a possible restart of the original supplier's business

Although DHPA is in the process of developing a business continuity solution for its members, it is not their top priority either (Alaerds, R., DHPA, 19 July 2019). Interest groups deal with topics and problems that are relevant to their members. They try to relieve their members and arrange as much as possible as a collective (Tempelman, I., NederlandICT, 11 July 2019). NederlandICT deals with solving (legal) issues concerning SaaS-applications on a daily basis. The given that business continuity for SaaS-applications has no priority at this moment, comes from the fact that it has no priority for SaaS-providers and other parties involved in the software supply chain. Everything runs on supply and demand. As soon as more members desire a centrally regulated continuity solution for SaaS-applications, the interest groups can focus on this. At both interest groups the capacity is too limited to address issues that have little or no priority for their members (Tempelman, I., NederlandICT, 11 July 2019). NederlandICT currently refers to a SaaS business continuity solution provider when the request for advice or possibilities rises from a member. For the SaaS-providers and -customers that need these guarantees for their business-critical applications, the current offer meets the requirements. For small companies that want such continuity guarantees for their business-critical SaaS-applications, there is currently no cost-effective solution

available, and there might be room for the interest groups there (Tempelman, I., NederlandICT, 11 July 2019). Both interest groups indicate that they are willing to participate as a stakeholder in thinking about workable, cost-effective business continuity solutions. Tempelman mentioned that properly arranging and being able to provide affordable continuity guarantees is something that the members of NederlandICT all would like to do, but currently there are insufficient opportunities in the market.

Both organisations doubt the actual need for business continuity solutions. Although no actual numbers on SaaS-provider bankruptcies were available during the interviews, both organisations consider chances of bankruptcy in this sector rather small. The chance may seem small, but the impact may be large, depending on the type and size of the application. In the event that things go wrong with the developer or supplier of the software, the end-user could have a major problem; especially if the business operations highly depend on it (Alaerds, R., DHPA, 19 July 2019). The data can probably still be retrieved via the curator if nothing has been arranged between customer and supplier concerning business continuity, provided that the buyer of the software is willing to pay a fee so that the estate is not disadvantaged. Given that the provision of the data has no adverse consequences for estate creditors, the data can be released by the curator against payment (Tempelman, I., NederlandICT, 11 July 2019). The making of clear agreements and using a business continuity solution is certainly useful, but end-users may insure themselves against something that they will – hopefully – never have to use. If it concerns a business-critical application for the customer, the customer will be more willing to bear the costs of a business continuity solution. Currently, continuity solutions for SaaS-applications often are simply too expensive for small end-users to consider such insurance worthwhile (Tempelman, I., NederlandICT, 11 July 2019). In order to make these insurances accessible for micro-businesses and SMEs, the first steps should be taken by SaaS business continuity solution providers. Guaranteeing of business continuity is their business and those firms are the experts. They should be the parties taking the initiative in raising awareness for SaaS continuity risks at parties that do not have the knowledge or experience (Tempelman, I., NederlandICT, 11 July 2019). Raising awareness of business continuity risks is important in general, so that so that the endangered parties can make the substantiated decision to cover themselves against the risk or not (Alaerds, R., DHPA, 19 July 2019).

As all other interviewed SaaS-experts during this interview did, both IT interest groups see potential in a certification mark, provided that it is addressed correctly and thoroughly. According to Tempelman, this responsibility, or burden, of guaranteeing continuity of business-critical SaaS-applications in case of bankruptcy in the supply chain should not be placed on shoulders of the SaaS-providers. Support is the most important factor in creating a fundamentally strong and responsible certification mark. One should start at the bottom of the software supply chain, being the business continuity solution providers. From the moment business continuity solutions are cost-effective for every kind and size of software-dependent business, logos on SaaS-providers' websites can be used to evaluate and indicate the level of continuity guarantees (Tempelman, I., NederlandICT, 11 July 2019). The other tool discussed in various interviewed to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-solutions comes with, being the legal obligation of business continuity solutions, was found not to be suitable according to these IT interest groups. Alaerds stated that there are no to very few cases known in which things had gone drastically wrong. The existence of an insurance policy does not mean that it is necessary by definition. It is not such a big problem yet that strict measures are needed (Tempelman, I., NederlandICT, 11 July 2019). It is much better to let the market figure out how things should be arranged than for the government to get involved.

## 4 Discussion

In February 2019, the start of the empirical research has been made after completion of the literature study. The process of choosing a topic for the bachelor thesis was relatively easy since the researcher was approached to take part in this research. The actual start was an introductory meeting with the other researchers and ACC ICT in Nieuwegein, to get to know each other and to establish the research purposes.

The research was carried out step by step and can generally be divided into seven phases, being the elaboration of the approach and scope, conducting the literature study, selecting (experience) experts in various groups, drafting of the interview protocols, followed by the execution of the research, analysis and processing of the results, and completion of the thesis. Until the execution of the research, the researcher has had approximately

biweekly coordination with the supervisor. This coordination was mainly substantive in nature and has served as a monitoring function: is the research still going in the direction as it should? Quick responses and useful feedback from the supervisor and co-worker of the research has contributed to keep some pace in the research process. Despite the regular coordination, the researcher has never had the feeling of not being for 100 percent in charge of the research.

The execution of the research has started in May 2019, which means the first phases of the research took more time than planned. Life does not stand still during a graduation period, and a large part of Q2 has disappeared due to personal circumstances in which it was not possible to work on the research. Besides that, it proved to be difficult and time-consuming to select and find the right respondents for the research. The time of waiting for responses and making appointments for on-location interviews contained various moments of reflection. In conclusion, it can be stated that the “safe” way of first completing one part of the research and interviews completely before proceeding with the next part, has not been ideal with respect to the needed time to do so.

Besides a personal reflection, this chapter also discusses the research limitations, opportunities and possibilities for future research.

## 4.1 Limitations

The following limitations might have influenced the validity of the performed research. Part of these limitations are serving as inspiration for future research as described in section 4.3: Future Research.

### 4.1.1 Expert Quality

SaaS business continuity solutions are considered to be at the start of its rise (Bijleveld, P., ACC ICT, 7 June 2019). This causes the amount of experienced domain experts to be relatively low. Most of the experts interviewed were SaaS-providers or SaaS business continuity solution providers which logically have business interest in this field of work. Even IT interest groups have some sort of business interest. Since independent SaaS business continuity experts in the Netherlands are scarce, the previously mentioned parties had to be the experts during this research. The interviewee selection process threatens the validity of the research, in that the participants were selected based on availability and willingness to participate. Besides that, they were all selected from within the acquaintance of ACC ICT. Also, none of the SaaS-providers had any experience with a real worst-case scenario in which one of their (supply) chain parties faced bankruptcy, and only one of the SaaS business continuity solution providers has had to intervene several times – approximately twice a year – due to bankruptcy of a SaaS-provider. This low amount of experience might negatively influence the expert quality. However, due to the method used to find participants the researcher dares say with some certainty that the interviewees’ responses were relevant, on-topic, and addressed the topic with sufficient experience and insight. This should be kept in mind, when assessing the quality of the conducted expert interviews. The quality and validity of this research would possibly have been improved if both SaaS-customers who have experienced long lasting unavailability of their SaaS-application due to their provider’s bankruptcy, and SaaS-customers who have experienced the successful inception of the SaaS business continuity provider were included as experts in the research. Also, (ex) SaaS-providers who faced bankruptcy could possibly have provided valuable information and visions towards the urgency of this topic, although they would probably have been very hard to find due to being out of business.

### 4.1.2 Providers’ Perspective

The research was performed with the exploration of the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-providers as its main purpose. As described before in section 2.3: Expert Interviews, a very specific group of SaaS-providers was selected to contribute to the research. Solely SaaS-providers that made a substantiated choice towards the adoption of SaaS business continuity solutions were selected and interviewed. One of the reasons for making this decision can be found in time-limiting factors.

Due to the length of this research, the researcher was unable to search, find and select a representative group of Dutch SaaS-providers to interview and to describe the current state of affairs with. The current state of affairs at SaaS-providers within this topic has been described from the perspective of some of the best SaaS-providers with respect to business continuity solution adoption. Every provider that has not arranged any form of SaaS business continuity solution for their end-customers would score worse in the overview table given in section 3.2.1: SaaS-Provider Interviews. A second reason for this decision can be found in the other goal of this research, namely discovering the most effective tool to raise awareness for the continuity risk businesses run in case their SaaS-provider goes bankrupt by transferring business-critical applications to the cloud. The risk of collecting insufficient and unsound information during the SaaS-provider interviews, was too large if parties who do not have any experience in this topic would have been interviewed.

Furthermore, as can be derived from the same table in section 3.2.1: SaaS-Provider Interviews, not all interviewed SaaS-providers sell business-critical applications. Though, this research focusses on business-critical applications. Business-critical applications form, due to their nature of being business-critical, the group of software for which continuity guarantees are most needed. Since all SaaS-providers within this research within this research made a substantiated choice towards the adoption of business continuity solutions, the researcher dares to say with some certainty that the interviewees' responses were relevant, on-topic, and addressed the topic with sufficient experience and insight.

#### 4.1.3 Customers' Perspective

The research was performed with the exploration of the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-developers as its main purpose. It was out of the scope of this project to research the demand and knowledge of business continuity risks and solutions at customer level. The requirements and needs were therefore based on the literature research and expert interviews. Several requirements resulted in components of which experts assumed they might have value for the customer, without confirming this value by the SaaS-customers as well.

### 4.2 Opportunities

Although the current study has some limitations, there are also some opportunities worth mentioning. Since little research has been done on the combination of business continuity solutions and business-critical SaaS-applications, the current study can be a valuable contribution to the overall body of knowledge for the domains of both business continuity and Software-as-a-Service.

#### 4.2.1 Awareness

This research could increase the awareness of business continuity threats, risks and solutions for end-users of business-critical SaaS-applications, and could change SMEs from being reactive to being proactive concerning business continuity guaranteeing.

#### 4.2.2 Revenue Model

Since costs can be passed on to the customer, there is an opportunity for SaaS-providers to make extra money of their customers. It is not unusual for an entrepreneur to profit a few percent on a service or product provided by a third party. As a matter of fact, for some business models, it is the whole revenue model. Logically, the business continuity solution provider charges the SaaS-provider more money for the solution than it costs. For the business continuity solution provider, it is part of its revenue model, and so it could be for the SaaS-provider. The SaaS-

provider could charge a customer more money on top of their own product – the SaaS ERP system for example – then the business continuity solution costs. As the results of this research show, guaranteeing business continuity is part of some of the SaaS-providers' business models, but none of them sees the business continuity solution as a way to increase profit margins yet.

### 4.3 Future Research

During this research, various topics came to light in which more research could be conducted. Future research could take all the limitations and possibilities of the current study into account.

#### 4.3.1 SaaS Business Continuity at Dutch SaaS-Customers

None of the respondents of this research are customers of Software-as-a-Service applications and chances are that customers of such services could have different visions on the chances, impacts and thus risks of business continuity disruptions than the parties interviewed during this research. Future research could take this into account by conducting a similar research among customers of SaaS-applications. As the results of this research show, SME-customers of Software-as-a-Service providers do not seem to be able to evaluate the risk of their provider going bankrupt. Lacking this information, businesses are effectively putting their critical business services in jeopardy. Though, this conclusion is based on the results of this research, since it was out of the scope of this project to research the demand and knowledge of business continuity risks and solutions at customer level. The requirements and needs were therefore based on the literature research and expert interviews. Several requirements resulted in components of which experts assumed they might have value for the customer, without confirming this value by the SaaS-customers as well.

#### 4.3.2 Certification Mark

Future research could develop a method to evaluate the (supply chain) health of different SaaS-providers. The results could enable businesses and individuals to make an informed decision on what SaaS-providers to do business with (Lucassen, Van Rooij, & Jansen, 2013). In order to prevent redundancy of investigating SaaS-providers by these businesses and individuals, this (to be) developed method to evaluate the health of different SaaS-providers could be done in the form of, for example, a certification mark. The function of a certification mark is to provide impartial third-party endorsement to aid buyers in overcoming some of the problems of product selection (Taylor, 1958). Future research could investigate the demands, needs, requirements, regulation, possibilities and limitations of such certification mark. Although this study has somewhat addressed and discussed various requirements and issues that come with a certification mark, no unequivocal answer has emerged. More research into the correct set-up of a certification mark will have to be performed before it can be concluded that this is the most effective tool to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-application comes with.

#### 4.3.3 Customer Loyalty

SME-customers that see the value of a business continuity solution will probably never choose a SaaS-provider for their business-critical applications that does not offer such solution. This will result in a win-win situation, as a customer will have increased trust in a provider's competence, involvement, responsibility and its services. Future research could investigate if this increased trust in the SaaS-provider would result in increased customer loyalty towards the provider.

---

## 5 Conclusion

During the rise of the SaaS-popularity, especially the advantages of such solutions were seen, and the possible business continuity risks were neglected. Not on purpose though, but because the SaaS-industry had not gone through a full lifecycle yet, the possible risks when adopting a SaaS-solution had not yet come to light. Disaster recovery service and business continuity guarantees in case of a human or non-human disaster were left aside when making these agreements. This is mainly because customers assumed the SaaS-provider would include these services, while it did not. On the other hand, SaaS-providers did not feel the need to include those (expensive) services, because SaaS-customers rarely ever asked for them. Whereas SaaS-customers previously did not demand business continuity solutions and just assumed SaaS-providers included such solution in their services, these days more and more large SaaS-customers are looking deep into the continuity risks of SaaS-solutions, and demand business continuity guarantees from their SaaS-provider, because of disappointing disaster recovery results from the past. Large companies have an IT-department at their disposal, which is familiar with the risks SaaS-solutions bring and the measures needed to be able to guarantee business continuity. Nowadays, bankruptcy and even natural disasters should be risks SaaS-customers take into account when choosing the right SaaS-provider for their business-critical software systems. As the title of this research says, critical applications should come with critical questions. Although large customers are seeing the need for business continuity arrangements, it is unsure if SaaS-providers realise the needs for such offerings to this very moment. Only a small part of the Dutch SaaS-providers offers its customers a business continuity solution and as the results of this research show, the main reason for looking into business continuity solution possibilities is the demand from (potential) customers. As long as SaaS-providers do not realise the needs for continuity guaranteeing solutions, we may assume small-to-medium enterprises (SMEs) do neither if they have no experience in IT. Remarkable is that the SaaS-providers' perceptions of the necessity of a business continuity solution rarely is one of the factors in the decision-making process. If a customer thinks guaranteeing of software continuity is of importance, the SaaS-provider will practically always satisfy that need if fiscally feasible. Costs at various levels form the primary factors in the decision-making process of adopting a SaaS business continuity solution for end-users. As the results from the interviews show, most (experience) experts believe initiative for the use of a business continuity solutions should come from the end-users, because they are the party running the real risk. But as long as (small) customers do not realise the need for some kind of business continuity solution, the situation remains as it currently is, and we are all waiting for a disaster to happen before measures will be taken in the software supply chain.

In order to enlarge national awareness of guaranteeing business continuity of SaaS-applications and change all concerning parties from being somewhat reactive towards proactive, broadly there are two opportunities that have emerged during this research. All respondents agreed unanimously there should be more attention for business continuity solutions, and that a certification mark could help raising awareness for the continuity risk SaaS-applications come with. Legal obligation of business continuity guarantees would not have the desired effect. Nowadays, for almost everything a consumer can buy, one can value a product's quality, origin and safety using certification marks. In every sector, independent of IT, it is not just the responsibility of the vendor or producer to operate in a (socially) responsible manner, but also the responsibility and choice of the (business) customer to balance benefits and costs, and purchase the right product. In principle, the SaaS-provider is the only party within the software supply chain a customer has contact with. The who, what, where, when and how does not matter in the customer's eyes, as long as the organisation behind the certification mark investigates, evaluates and judges the complete software supply chain in a structured and consistent manner, and issues the appropriate level of certification. This way, on one hand, both large and small (potential) customers can easily and effortlessly assess and compare SaaS-providers' products and services without knowledge about the underlying technical constructions. SaaS-providers, on the other hand, can show their level of competence, involvement, and feeling of responsibility for their customers' business continuity to increase customers' trust in their products and services. Exactly what SaaS business continuity solutions are meant for.

## References

- Abdat, N., Spruit, M., & Bos, M. (2010): Software as a service and the pricing strategy for vendors. In *Strader, T., ed.: Digital Product Management, Technology and Practice: Interdisciplinary Perspectives. Advances in E-Business Research (AEBR) Book Series. IGI Global*, pp. 154-192.
- Baarda, B., De Goede, M., & Teunissen, J. (2001): *Kwalitatief Onderzoek*. Groningen/Houten: Wolters-Noordhoff.
- Baarda, B., Van der Hulst, M., & De Goede, M. (2012): *Basisboek Interviewen*. (3e druk). Groningen/Houten: Wolters-Noordhoff.
- Bogner, A., Littig, B., Menz, W. (2009): *Interviewing Experts*.
- Brinkmann, S., & Kvale, S. (2015): *Interviews: learning the craft of qualitative research interviewing* (3<sup>rd</sup> ed.).
- Castillo-Montoya, M. (2016): Preparing for Interview Research: The Interview Protocol Refinement Framework. *The Qualitative Report 2016 Volume 21, Number 5, How To Article 1*, pp. 811-831.
- Creswell, J. W. (2007): *Qualitative inquiry and research design: Choosing among five approaches* (2<sup>nd</sup> ed.). Thousand Oaks, CA: Sage.
- Daly, I. (2017): Plan B Disaster Recovery Ltd: Ian discusses IT continuity at IP Expo 2017. [www.youtube.com/watch?v=0px6MdfRUxo](http://www.youtube.com/watch?v=0px6MdfRUxo).
- Guion, L. A., Diehl, D. C., McDonald, D. (2011): Conducting an In-depth Interview.
- Hiles, A. (1994): Service Level Agreements: Panacea or Pain? *The TQM Magazine* 6(2), pp. 14-16.
- Hinde, S., & Spackman, E. (2015). Bidirectional citation searching to completion: an exploration of literature searching methods. *PharmacoEconomics*, 33(1), pp. 5-11.
- Jones, S. R., Torres, V., Arminio, J. (2014): Issues in analysis and interpretation. In *Negotiating the complexities of qualitative research in higher education: Fundamental elements and issues* (2<sup>nd</sup> ed.), pp. 157-173. New York, NY: Routledge.
- Krueger, R. A. & Casey, M. A. (2009): Developing a questioning route. In *Focus groups: A practical guide for applied research*, pp. 35-60. Thousand Oaks, CA: Sage.
- Lucassen, G., Van Rooij, K., Jansen, S. (2013): Ecosystem Health of Cloud PaaS Providers. In *International Conference of Software Business*, pp. 183-194. Springer, Berlin, Heidelberg.
- Maxwell, J. (2013): *Qualitative research design: An interactive approach* (3<sup>rd</sup> ed.). Thousand Oaks, CA: Sage.
- Merriam, S. B. (2009): *Qualitative research: A guide to design and implementation*. San Francisco, CA: Jossey-Bass.
- Neumann, A. (2008): *The craft of interview research*. Graduate course at Teachers College, Columbia University, New York, NY.
- Patton, M. Q. (2015): *Qualitative research & evaluation methods* (4<sup>th</sup> ed.). Thousand Oaks, CA: Sage.
- Rubin, H. J., & Rubin I. S. (2012): *Qualitative interviewing: The art of hearing data* (3<sup>rd</sup> ed.). Thousand Oaks, CA: Sage.
- Rudrakshi, C., Varshney, A., Yadla, B., Kanneganti, R., Somalwar, K. (2014): API-Fiction – Core Building Block Of The Digital Enterprise.
- Schut, J. (1990): Insurance: Lessons from Disasters. In *Institutional Investor*, pp. 297.
- Spiotto, A., & Spiotto, J. (2003): Ultimate Downside of Outsourcing: Bankruptcy of the Service Provider. *The American Bankruptcy Institute Law Review* 11.
- Taylor, D. A. (1958): Certification marks—success or failure?. *Journal of Marketing*, 23(1), pp. 39-46.
- Ten Dam, P. (2014): ACC ICT: De OTAP-ontwikkelstraat.
- Van De Zande, T., & Jansen, S. (2011): Business continuity solutions for SaaS customers. In *International Conference of Software Business*, pp. 17-31. Springer, Berlin, Heidelberg.
- Voigt, P., Von Dem Bussche, A. (2017): *The EU General Data Protection Regulation (GDPR). A Practical Guide*.
- Wohlin, C. (2014): Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *proceedings of the 18<sup>th</sup> international conference on evaluation and assessment in software engineering*, pp. 38.

## Appendices

### A Interview Consent Form

#### To be completed by the participant

I have been informed about the goals of this research. I could ask additional questions. My questions have been answered sufficiently. I had enough time to decide if I wanted to participate.	Yes/No*
I know participating is completely voluntary. I know I can decide not to participate at any time. I don't have to give a reason for that.	Yes/No*
I give permission to mention my statements by name in the results of this study. I know I can indicate that I want to answer certain questions anonymously. I don't want to be quoted regarding those questions.	Yes/No*
I give permission to use my data for the purposes stated in the information letter.	Yes/No*
I give permission to keep the collected data for at least 10 years after the end of this investigation.	Yes/No*
I give permission to record this interview with an audio recorder.	Yes/No*
I want to participate in this study.	Yes/No*

\* Delete as appropriate.

Comments:

Name of participant:

Signature:

Date:

#### To be completed by the researcher

I hereby declare that I have fully informed this participant about the aforementioned study.	Yes/No*
If information becomes known during the investigation that could influence the consent of the participant, I will inform him / her in time.	Yes/No*

\* Delete as appropriate.

Comments:

Name of researcher:

Signature:

Date:

## B Interview Protocols

### B.1 Interview Protocol for SaaS-Providers

Script prior to interview:

*I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.*

[Review aspects of consent form]

*You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? \_\_\_Yes \_\_\_No.*

*If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.*

*If no: Thank you for letting me know. I will only take notes of our conversation.*

*Before we begin the interview, do you have any questions? [Discuss questions]*

*If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.*

#### **Background Information**

*To begin the interview, I would like to ask you about some general information about your company.*

1. Could you introduce yourself to me?
2. Could you introduce your company to me?
3. When was your company founded?
  - 3.1. Since when does your company offer SaaS-solutions?
4. In which field does your company specialize?
  - 4.1. Does your company build business-critical software like ERPs?
5. Did your company somewhere in time make the switch from on-premise solutions towards SaaS-solutions?
6. What is the current size of your company? How many employees does your company have?
  - 6.1. How many customers does your company currently have?

#### **SaaS Business Continuity Solutions**

*Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end users of SaaS-solutions.*

7. Since when does your company offer a continuity solution for her customers?
8. What was the direct cause for your company to think about the possibilities regarding guaranteeing continuity of her customers?
9. At the time of thinking about a continuity solution, was there a project team set up within your company, or did your company outsource this to a continuity expert organisation from the very beginning?
 

*If project team was set up:*

  - 9.1. Why did your company decide to develop their own continuity solution?

*If outsourced to continuity expert organisation:*

9.2. Why did your company decide to outsource the continuity solution?

10. Which continuity interruption(s) or threat(s) is/are covered by your company's continuity solution?

10.1. Which agreements does the continuity solution contain?

11. Has your company had requests for continuity guarantee situations not being covered by the current solution? Think about data losses after natural disasters, mal- or ransomware infection, cyber attacks and hardware malfunction.

11.1. Is your company planning to investigate the possibilities of offering a full disaster recovery service?

12. How many of your company's customers did ask for a continuity solution before your company offered such solution?

13. Did your company ever lose a customer or did your company ever not acquire a customer because of the absence of a continuity solution?

14. How many of your company's current potential customers ask for or demands a continuity solution during the initial negotiations?

15. How many of your company's already acquired customers decided to use the continuity solution after introduction?

16. Which party does initiate the use of the continuity solution? Does the customer always demand for it, or does your company also suggest using the continuity solution?

*If your company suggests use:*

16.1. How often does a customer agree with the proposal of using the continuity solution?

17. Does the continuity solution entail additional costs for the customer?

*If yes:*

17.1. Has the continuity solution become part of your company's business model?

18. How much more customers does your company think to have acquired since the introduction of the continuity solution, with regards to SaaS-providers which do not offer such solution?

18.1. Does your company think (potential) customers choose your company over a competitor because of the existence of the continuity solution?

19. Does your company see that increasingly more SaaS-providers offer a continuity solution, or does your company see that barely any SaaS developers offer such solution?

20. Does your company think that SaaS-providers that currently do not have any plans of introducing a continuity solution for their (potential) customers will price themselves out of the market?

### **Sparring Session**

*Thank you. My last questions are more mend as a sparring session to talk about possibilities for raising awareness for SaaS business continuity risks at SaaS-providers and end-users.*

21. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?

22. Do you think business continuity solutions should get more attention?

*If yes:*

22.1. What would be a powerful tool to improve business continuity awareness?

*If no:*

22.2. Why not?

23. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews?

24. Would you like to receive the findings of this research after completion?

## B.2 Interview Protocol for SaaS Business Continuity Solution Providers

*I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.*

[Review aspects of consent form]

*You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? \_\_\_Yes \_\_\_No.*

*If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.*

*If no: Thank you for letting me know. I will only take notes of our conversation.*

*Before we begin the interview, do you have any questions? [Discuss questions]*

*If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.*

### **Background Information**

*To begin the interview, I would like to ask you about some general information about your company.*

1. Could you introduce yourself to me?
2. Could you introduce your company to me?
3. When was your company founded?
4. What was your core business at that time?
5. What is the current size of your company? How many employees does your company have?
  - 5.1. How many customers does your company currently have?
6. What kind of firm is your average client?
  - 6.1. What kind of SaaS-applications do they provide?
7. What is the size of your average client?
  - 7.1. What kind of customers do they have?

### **SaaS Business Continuity Solutions**

*Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end users of SaaS-solutions.*

8. Since when does your company offer a SaaS business continuity solution?
9. What was the direct cause for your company to think about the possibilities regarding guaranteeing continuity of end-users?
10. Which continuity interruption(s) or threat(s) is/are covered by your company's continuity solution?
11. Which new challenges did SaaS business continuity solutions bring compared to traditional source-code escrow?

12. How does your SaaS business continuity solution work?  
12.1. Is it pure legal?
13. For how long do you promise your clients continuation of their SaaS software in case of bankruptcy of the SaaS-provider?
14. How do you handle SaaS-applications with (a lot of) third-party software?
15. Which responsibilities and duties do you promise towards the SaaS-provider and the end-user?
16. Which responsibilities and duties does the SaaS-provider promise towards you and the end-user?
17. Does the SaaS-provider have one contract with you, for all its end-users, or does every end-user have its own contract with you?  
*If only one format:*  
17.1. Why did you choose for this format?  
*If both formats:*  
17.2. Which format gets used the most?
18. What are the costs of this/these solution(s)?
19. How do you make sure your own costs don't get too high when you need to interfere?
20. How does customer acquisition work? Do you lobby at SaaS-providers and end-users to raise awareness for this subject? Do you give lectures? Do SaaS-providers and/or end-users come to you because they need/want a business continuity solution?
21. Do both big and small companies contact you to inform about business continuity solutions?  
*If only one party does:*  
21.1. Why do you think the other party does not contact you?
22. Do you think that SaaS-providers that currently do not have any plans of introducing a continuity solution for their (potential) customers will price themselves out of the market?

### **Sparring Session**

*Thank you. My last questions are more meant as a sparring session to talk about possibilities for raising awareness for SaaS business continuity risks at SaaS-providers and end-users.*

23. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?
24. Do you think business continuity solutions should get more attention?  
*If yes:*  
24.1. What would be a powerful tool to improve business continuity awareness?  
*If no:*  
24.2. Why not?
25. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews?
26. Would you like to receive the findings of this research after completion?

### B.3 Interview Protocol for IT Interest Groups

*I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.*

[Review aspects of consent form]

*You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? \_\_\_Yes \_\_\_No.*

*If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.*

*If no: Thank you for letting me know. I will only take notes of our conversation.*

*Before we begin the interview, do you have any questions? [Discuss questions]*

*If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.*

#### **Background Information**

*To begin the interview, I would like to ask you about some general information about your company.*

1. Could you introduce yourself to me?
2. Could you introduce your company to me?
  - 2.1. How many employees does your company have?
3. Who are the customers, or members, of your company?
  - 3.1. What size are your members in terms of number of employees?
4. Why do companies join an interest group?
  - 4.1. What are the benefits?
  - 4.2. What are the costs?
5. How many members does your company have?
  - 5.1. Is there a noticeable (exponential) increase in companies that join an interest group?
  - 5.2. Is there a noticeable difference with the high time of on-premise solutions?
6. To what extent does your company focus on SaaS?

#### **SaaS Business Continuity Solutions**

*Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end users of SaaS-solutions.*

7. What is your company's opinion towards the continuity risk, or dependency, that SaaS-solutions come with?
8. A risk does always consist of a chance and an impact. How does your company estimate the chance of bankruptcy at the supplier of a SaaS-application, or another party in the supply chain such as the hosting-provider?
  - 8.1. How does your company estimate the impact for end-users in case a SaaS-provider or hosting-providers faces bankruptcy?
  - 8.2. Of what importance do you think a business continuity solution is, for business-critical SaaS-applications?

9. To what extent does your company deal with the recently updated GDPR?
- 9.1. How does the GDPR relate to guaranteeing business continuity according to your company?
10. Which new challenges did SaaS business continuity solutions bring compared to traditional source-code escrow?
11. To what extent does your company deal with business continuity solutions for SaaS?
- 11.1. To what extent does or did your company investigate and evaluate different SaaS-escrow providers and their business continuity solutions?
- 11.2. Which business continuity solutions does your company know?
- 11.3. To what extent does your company advise its members to investigate the possibilities, needs, benefits and costs of a SaaS business continuity solution?
12. How often does your company receive questions about arranging or giving advice for SaaS business continuity solutions?
- 12.1. From which parties do these questions come from? Do they come from the SaaS-providers, or from the end-users of the software?
- 12.2. Do both big and small companies contact you to inform about business continuity solutions?  
*If only one party does:*
- 12.3. Why do you think the other party does not contact you?
- 12.4. To what extent does your company advise and help arranging SaaS business continuity solutions?
- 12.5. Does your company have its own SaaS-escrow solution for its members?
13. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?
14. Which aspects should be covered by a SaaS business continuity solution, according to your company?
15. Which development does your company notice concerning the guaranteeing of business continuity in the complete SaaS-market?
- 15.1. Does this development also apply to the SME-sector?

### **Sparring Session**

*Thank you. My last questions are more meant as a sparring session to talk about possibilities for raising awareness for SaaS business continuity risks at SaaS-providers and end-users.*

16. Does your company think SME end-users of SaaS-applications realise the continuity risks a SaaS-application comes with?
- 16.1. Does your company think more awareness should be raised for the continuity risks a SaaS-application comes with, and the possible solutions to minimize the impact?  
*If yes:*
- 16.2. What would be a powerful tool to improve business continuity awareness?  
*If no:*
- 16.3. Why not?
17. What is your company's vision on the legal obligation of SaaS continuity guarantees?
- 17.1. What is your vision on establishing an independent party that provides a certification mark to indicate the extent to which business continuity is guaranteed?
18. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews?
19. Would you like to receive the findings of this research after completion?

**C Interview Protocol Matrixes**

**C.1 Interview Protocol Matrix for SaaS-Providers**

<p>Script prior to interview:</p> <p><i>I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.</i></p> <p>[Review aspects of consent form]</p> <p><i>You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? ___Yes ___No.</i></p> <p><i>If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.</i></p> <p><i>If no: Thank you for letting me know. I will only take notes of our conversation.</i></p> <p><i>Before we begin the interview, do you have any questions? [Discuss questions]</i></p> <p><i>If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.</i></p>					
<p><i>What is the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-providers?</i></p>	<p>Background Information</p>	<p>To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?</p>	<p>To what extent do Dutch SaaS-providers feel responsible for their customers' business continuity?</p>	<p>Which solutions can SaaS-providers offer their customers in order to guarantee business continuity?</p>	<p>What would be the most powerful tool to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-solution comes with?</p>
<p><b>Background Information</b></p> <p><i>To begin the interview, I would like to ask you about some general information about your company.</i></p>					
<p>1. Could you introduce yourself to me?</p>	X				
<p>2. Could you introduce your company to me?</p>	X				
<p>3. When was your company founded? <i>Follow up:</i> Since when does your company offer SaaS-solutions?</p>	X				
<p>4. In which field does your company specialize? <i>Follow up:</i> Does your company build business-</p>	X				

critical software like ERPs?					
5. Did your company somewhere in time make the switch from on-premise solutions towards SaaS-solutions?	X				
6. What is the current size of your company? How many employees does your company have? <i>Follow up:</i> how many customers does your company currently have?	X				
<b>SaaS Business Continuity Solutions</b>					
<i>Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end users of SaaS-solutions.</i>					
7. Since when does your company offer a continuity solution for her customers?		X	X		
8. What was the direct cause for your company to think about the possibilities regarding guaranteeing continuity for her customers?		X	X		
9. At the time of thinking about a continuity solution, was there a project team set up within your company, or did your company outsource this to a continuity expert organisation from the very beginning? <i>Follow up:</i> Why did your company decide to develop their own continuity solution/Why did your company decide to outsource the continuity solution?	X	X	X	X	
10. Which continuity interruption(s) or threat(s) is/are covered by your company's continuity solution?		X	X	X	

<i>Follow up:</i> Which agreements does the continuity solution contain?					
11. Has your company had requests for continuity guarantee situations not being covered by the current solution? Think about data losses after natural disasters, mal- or ransomware infection, cyber attacks and hardware malfunction. <i>Follow up:</i> Is your company planning to investigate the possibilities of offering a full disaster recovery service?		X	X	X	
12. How many of your company's customers did ask for a continuity solution before your company offered such solution?		X			
13. Did your company ever lose a customer or did your company ever not acquire a customer because of the absence of a continuity solution?		X	X		
14. How many of your company's current potential customers ask for or demands a continuity solution during the initial negotiations?		X			
15. How many of your company's already acquired customers decided to use the continuity solution after introduction?		X			X
16. Which party does initiate the use of the continuity solution? Does the customer always demand for		X	X		X

<p>it, or does your company also suggest using the continuity solution?  <i>If your company suggests use:</i>          How often does a customer agree with the proposal of using the continuity solution?</p>					
<p>17. Does the continuity solution entail additional costs for the customer?  <i>If yes:</i>          Has the continuity solution become part of your company's business model?</p>		X	X		
<p>18. How much more customers does your company think to have acquired since the introduction of the continuity solution, with regards to SaaS-providers which do not offer such solution?  <i>Follow up:</i>          Does your company think (potential) customers choose your company over a competitor because of the existence of the continuity solution?</p>		X	X		X
<p>19. Does your company see that increasingly more SaaS-providers offer a continuity solution, or does your company see that barely any SaaS developers offer such solution?</p>		X	X		
<p>20. Does your company think that SaaS-providers that currently do not have any plans of introducing a continuity solution for their (potential) customers will price</p>		X	X		X

themselves out of the market?					
<b>Sparring Session</b>					
<i>Thank you. My last questions are more mend as a sparring session to talk about possibilities for raising awareness for SaaS business continuity risks at SaaS-providers and end-users.</i>					
21. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?		X	X		X
22. Do you think business continuity solutions should get more attention? <i>If yes:</i> What would be a powerful tool to improve business continuity awareness? <i>If no:</i> Why not?			X		X
23. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews?	X	X	X	X	X
24. Would you like to receive the findings of this research after completion?	X				

C.2 Interview Protocol Matrix for SaaS Business Continuity Solution Providers

<p>Script prior to interview:</p> <p><i>I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.</i></p> <p>[Review aspects of consent form]</p> <p><i>You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? ___Yes ___No.</i></p> <p><i>If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.</i></p> <p><i>If no: Thank you for letting me know. I will only take notes of our conversation.</i></p> <p><i>Before we begin the interview, do you have any questions? [Discuss questions]</i></p> <p><i>If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.</i></p>					
<p><i>What is the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-providers?</i></p>	<p>Background Information</p>	<p>To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?</p>	<p>To what extent do Dutch SaaS-providers feel responsible for their customers' business continuity?</p>	<p>Which solutions can SaaS-providers offer their customers in order to guarantee business continuity?</p>	<p>What would be the most powerful tool to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-solution comes with?</p>
<p><b>Background Information</b></p> <p><i>To begin the interview, I would like to ask you about some general information about your company.</i></p>					
<p>1. Could you introduce yourself to me?</p>	<p>X</p>				
<p>2. Could you introduce your company to me?</p>	<p>X</p>				
<p>3. When was your company founded?</p>	<p>X</p>				
<p>4. What was your core business at that time?</p>	<p>X</p>				
<p>5. What is the current size of your company? How many employees does your company have?</p> <p><i>Follow up:</i> How many customers does your</p>	<p>X</p>				

company currently have?					
6. What kind of firm is your average client? <i>Follow up:</i> What kind of SaaS-applications do they provide?	X				
7. What is the size of your average client? <i>Follow up:</i> What kind of customers do they have?	X				
<b>SaaS Business Continuity Solutions</b> <i>Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end-users of SaaS-solutions.</i>					
8. Since when does your company offer a SaaS business continuity solution?		X	X	X	
9. What was the direct cause for your company to think about the possibilities about guaranteeing continuity for end-users?		X	X	X	
10. Which continuity interruption(s) or threat(s) is/are covered by your company's continuity solution?		X	X	X	
11. Which new challenges did SaaS business continuity solutions bring compared to traditional source-code escrow?		X	X	X	
12. How does your SaaS business continuity solution work? <i>Follow up:</i> Is it pure legal?				X	
13. For how long do you promise your clients continuation of their SaaS software in case of bankruptcy of the SaaS-provider?		X		X	
14. How do you handle SaaS-applications with (a		X	X	X	

lot of) third-party software?					
15. Which responsibilities and duties do you promise towards the SaaS-provider and the end-user?		X		X	
16. Which responsibilities and duties does the SaaS-provider promise towards you and the end-user?			X	X	
17. Does the SaaS-provider have one contract with you, for all its end-users, or does every end-user have its own contract with you? <i>If only one format:</i> Why did you choose for this format? <i>If both formats:</i> Which format gets used the most?		X	X	X	
18. What are the costs of this/these solution(s)?				X	X
19. How do you make sure your own costs don't get too high when you need to interfere?				X	
20. How does customer acquisition work? Do you lobby at SaaS-providers and end-users to raise awareness for this subject? Do you give lectures? Do SaaS-providers and/or end-users come to you because they need/want a business continuity solution?		X	X	X	X
21. Do both big and small companies contact you to inform about business continuity solutions? <i>If only one party does:</i> Why do you think the other party does not contact you?		X			X

22. Do you think that SaaS-providers that currently do not have any plans of introducing a continuity solution for their (potential) customers will price themselves out of the market?		X	X		X
<b>Sparring Session</b> <i>Thank you. My last questions are more mend as a sparring session to talk about possibilities for raising awareness for SaaS business continuity risks at SaaS-providers and end-users.</i>					
23. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?		X	X		X
24. Do you think business continuity solutions should get more attention? <i>If yes:</i> What would be a powerful tool to improve business continuity awareness? <i>If no:</i> Why not?		X	X		X
25. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews?	X	X	X	X	X
26. Would you like to receive the findings of this research after completion?	X				

C.3 Interview Protocol Matrix for IT Interest Groups

<p>Script prior to interview:</p> <p><i>I'd like to thank you once again for being willing to participate in the interview aspect of this study. This study's purpose is to find out how Dutch SaaS-providers perceive business continuity solutions for business-critical applications. Its purpose is also to discover the most effective tool to raise awareness for this subject at both developers and end-users. As your company is an organisation that has clearly thought about this concept, you will fulfil the role of an (experience) expert within this research. Our interview today will last approximately one hour during which I will be asking you about your company and its vision, opinion and choices on SaaS continuity solutions for end users.</i></p> <p>[Review aspects of consent form]</p> <p><i>You completed a consent form indicating that I have your permission (or not) to audio record our conversation. Are you still ok with me recording (or not) our conversation today? ___Yes ___No.</i></p> <p><i>If yes: Thank you. Please let me know if at any point you want me to turn off the recorder or keep something you said off the record.</i></p> <p><i>If no: Thank you for letting me know. I will only take notes of our conversation.</i></p> <p><i>Before we begin the interview, do you have any questions? [Discuss questions]</i></p> <p><i>If any questions (or other comments) arise at any point during this interview, please feel free to ask them at any time. I would be more than happy to answer your questions.</i></p>					
<p><i>What is the current state of affairs concerning business continuity solutions for business-critical applications at Dutch SaaS-providers?</i></p>	<p>Background Information</p>	<p>To what extent are Dutch SaaS-providers under pressure from their customers to guarantee continuity of business-critical software?</p>	<p>To what extent do Dutch SaaS-providers feel responsible for their customers' business continuity?</p>	<p>Which solutions can SaaS-providers offer their customers in order to guarantee business continuity?</p>	<p>What would be the most powerful tool to raise awareness at both Dutch SaaS-providers and their customers for the continuity risk a SaaS-solution comes with?</p>
<p><b>Background Information</b></p> <p><i>To begin the interview, I would like to ask you about some general information about your company.</i></p>					
<p>1. Could you introduce yourself to me?</p>	<p>X</p>				
<p>2. Could you introduce your company to me? <i>Follow up:</i> How many employees does your company have?</p>	<p>X</p>				
<p>3. Who are the customers, or members, of your company? <i>Follow up:</i> What size are your members in terms of number of employees?</p>	<p>X</p>				

4. Why do companies join an interest group? <i>Follow up:</i> What are the benefits? <i>Follow up:</i> What are the costs?	X		X		
5. How many members does your company have? <i>Follow up:</i> Is there a noticeable (exponential) increase in companies that join an interest group? <i>Follow up:</i> Is there a noticeable difference with the high time of on-premise solutions?	X		X		
6. To what extent does your company focus on SaaS?	X				
<b>SaaS Business Continuity Solutions</b> <i>Thank you for your responses. Now, I would like to ask you some questions regarding business continuity solutions for end-users of SaaS-solutions.</i>					
7. What is your company's opinion towards the continuity risk, or dependency, that SaaS-solutions come with?		X	X		
8. A risk does always consist of a chance and an impact. How does your company estimate the chance of bankruptcy at the supplier of a SaaS-application, or another party in the supply chain such as the hosting-provider? <i>Follow up:</i> How does your company estimate the impact for end-users in case a SaaS-provider or hosting-providers faces bankruptcy? <i>Follow up:</i> Of what importance do you think a business continuity		X			X

<p>solution is, for business-critical SaaS-applications?</p>					
<p>9. To what extent does your company deal with the recently updated GDPR? <i>Follow up:</i> How does the GDPR relate to guaranteeing business continuity according to your company?</p>	X	X			X
<p>10. Which new challenges did SaaS business continuity solutions bring compared to traditional source-code escrow?</p>		X	X	X	
<p>11. To what extent does your company deal with business continuity solutions for SaaS? <i>Follow up:</i> To what extent does or did your company investigate and evaluate different SaaS-escrow providers and their business continuity solutions? <i>Follow up:</i> Which business continuity solutions does your company know? <i>Follow up:</i> To what extent does your company advise its members to investigate the possibilities, needs, benefits and costs of a SaaS business continuity solution?</p>		X	X	X	
<p>12. How often does your company receive questions about arranging or giving advise for SaaS business continuity solutions? <i>Follow up:</i> From which parties do these questions</p>	X	X	X	X	

<p>come from? Do they come from the SaaS-providers, or from the end-users of the software?  <i>Follow up:</i>                  Do both big and small companies contact you to inform about business continuity solutions?  <i>If only one party does:</i>                  Why do you think the other party does not contact you?  <i>Follow up:</i>                  To what extent does your company advise and help arranging SaaS business continuity solutions?  <i>Follow up:</i>                  Does your company have its own SaaS-escrow solution for its members?</p>					
<p>13. Whose responsibility do you think it is to initiate the usage of a SaaS business continuity solution? Should this come from the SaaS-provider, because they should take responsibility of the product and service they deliver? Or do you think this should be the responsibility of the end-user, because they are the one running the continuity risk?</p>		X	X		
<p>14. Which aspects should be covered by a SaaS business continuity solution, according to your company?</p>	X	X		X	
<p>15. Which development does your company notice concerning the guaranteeing of business continuity in the complete SaaS-market?</p>		X	X	X	X

<i>Follow up:</i> Does this development also apply to the SME-sector?					
<b>Sparring Session</b> <i>Thank you. My last questions are more mend as a sparring session to talk about possibilities for raising awareness for SaaS business continuity threats at SaaS-providers and end-users.</i>					
16. Does your company think SME end-users of SaaS-applications realise the continuity risks a SaaS-application comes with? <i>Follow up:</i> Do you think business continuity solutions should get more attention? <i>If yes:</i> What would be a powerful tool to improve business continuity awareness? <i>If no:</i> Why not?		X	X	X	X
17. What is your company's vision on the legal obligation of SaaS continuity guarantees? <i>Follow up:</i> What is your vision on establishing an independent party that provides a certification mark to indicate the extent to which business continuity is guaranteed?		X	X	X	X
18. Before closing this interview; Is there any topic about SaaS continuity solutions I did not cover in this interview? Is there anything you would like to address for me to take to the next interviews	X	X	X	X	X
19. Would you like to receive the findings of this research after completion?	X				