Business Continuity Risks Through the Use of Software-As-A-Service: A Descriptive Survey

Denise van Velzen, Marco de Jong, Slinger Jansen

Department of Information and Computing Sciences
Utrecht University

August 12, 2019

Abstract

Due to the positive advantages of Software-as-a-Service (SaaS), such as instantaneous access and low total cost of ownership, more organizations are moving towards SaaS in favor of traditional shrink-wrapped or on-premise software. Little attention goes out to the negative implications of using SaaS. This paper is a descriptive study with the aim of creating more awareness about the risks that come with using SaaS. A survey with 121 respondents showed that about 75% of Dutch small and medium-sized enterprises (SMEs) within the Information Technology (IT) sector are at risk of suffering business interruptions through the use of SaaS. Considering these organizations are working with IT on a daily basis, it is likely that that number increases when looking at SMEs within other sectors. As SMEs represent about 90% of all Dutch organizations, it is important that the sector is informed and aware of these risks. Protection against these risks can be arranged through continuity solutions, such as SaaS escrow and a SaaS Guarantee Fund. If all organizations would adopt such continuity solutions, the steadiness of the sector would increase, positively affecting business in the Netherlands.

1 Introduction

Organizations increasingly depend on information technology (IT) for all facets of their business processes (Cerullo & Cerullo, 2004). The most notable trend of the past decade is the shift towards cloud computing. Cloud computing is defined by the National Institute of Standards and Technology as *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance, 2011). As can be derived from the definition, using cloud computing brings certain benefits, such as the ability to access the cloud from any location or device.

With the rise of cloud computing, the software industry has been moving towards a service-oriented approach, with vendors using products to sell as services (Mäkilä, Järvi, Rönkkö & Nissilä, 2010). As of 2018, Software-as-a-Service (SaaS) is the largest segment of the cloud market. Its revenue has been growing each year, with the expectation of it reaching 85.1 billion US dollars in 2019[1].

There are several advantages of choosing SaaS over on-premise software for both software providers and customers. From the perspective of the provider, SaaS products are easier to scale, easier to maintain and there is a large 'available' market (Mäkilä et al., 2010). Focusing on the end-users, choosing SaaS comes with the advantage of being able to use it instantaneously from any location, provided there is an internet connection. Furthermore, there is no need for the end-user to worry about product maintenance, as this is done automatically by the provider. Consequently, the product is always up-to-date which minimizes the security risks that come with using IT in businesses. Finally, the initial cost of implementing a SaaS solution is significantly lower than on-premise software. This lowers the barrier for small-to-medium businesses to acquire such business solutions.

However, choosing SaaS comes with several risks as well. When choosing SaaS, end-users become dependant on the provider for having continued access to the service. Should the provider fail to provide this, the end-users will experience disruptions in their businesses by losing access to a potentially critical component for their business operations and possibly losing their data as well.

Coghead is an example of the risks that come with using SaaS. This was a start-up web application company that offered an online application development platform. Customers included the University of Southern California Marshall School of Business, insurance company Colonial Group International and Taiwan-based freight forwarding company Morrison Express. When Coghead was acquired by SAP, the services for their customers were terminated. Coghead advised their customers to stop developing on their platform and to download their remaining data, as SAP had ceased technical support. All customers had to find a new platform and re-write their applications[2].

In order to prevent such problems for SaaS-customers, business continuity solutions can be implemented. These solutions have been available for on-premise software for many years. One example of this is a Service Level Agreement, which is a legal document where customer and provider agree on the quality of service, by quantifying minimum quality of service (Hiles, 1994). However, according to van de Zande & Jansen (2011), problems such as a SaaS-provider going out of business are often neglected. This is an oversight that could have

[1] Gartner. (2018, September 12). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. Retrieved May 9, 2019, from https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019

[2] Savvas, A. (2009, February 20). Coghead customers left high and dry despite SAP acquisition. Retrieved May 10, 2019, from https://www.computerweekly.com/news/2240088486/Coghead-customers-left-high-and-dry-despite-SAP-acquisition

disastrous consequences for an organization. Continuity solutions for on-premise software do not match the characteristics of SaaS. This should spark a debate about how to guarantee business continuity from this point forward.

In their paper, van de Zande & Jansen (2011) discuss exactly that. By interviewing several organizations they have defined what risks using SaaS bring to the customers and discovered what continuity solutions exist that are specifically geared towards SaaS. This paper should be seen as a revisit or extension of their research. Based on this paper and the fact that almost no literature on the subject can be found, business continuity for SaaS seemingly is a subject that has not received much attention. The goal of this paper is to give a report on how (and if) the Dutch SME (Small and Medium Enterprises) IT industry perceive SaaS and its risks to business continuity. The research question to be answered is: *What is the current state of the Dutch SME IT sector regarding SaaS continuity?* Furthermore, if it is found that this is indeed something that most organizations are not aware of, this paper can be used to create awareness about the topic.

The rest of the paper is built up as follows:

- Section 2 describes the methods that will be used to answer the research question and defines several sub questions to do so. This includes a survey that will be distributed within the Dutch SME IT sector.
- Section 3 provides the results of the literature study that has been conducted. It discusses SaaS in more detail, including the risks and threats that come with it as well as some continuity solutions. Furthermore, the survey results are presented.
- Section 4 will provide an analysis of the literature study and survey results and will answer the sub questions that have been defined in section 2.
- In section 5 the paper itself as well as recommendations for future work will be discussed. Section 6 will conclude the paper.

2 Research Methods

As stated in the previous section the main question this paper will attempt to answer is *What is the current state of the Dutch SME IT sector regarding SaaS continuity?* In an attempt to keep the scope of this research as small as possible, the focus is put on the Dutch SME IT sector. This specific sector is chosen for multiple reasons, the first one being that, as this research is performed in the Netherlands, Dutch organizations are the easiest to recruit. The choice to focus on Dutch organizations was therefore mostly out of convenience. However, this is not true for the second part of the scope: SMEs. After some preliminary work by de Jong (2019), it became apparent that large organizations often do have some type of continuity solution in place. Large organizations are more likely to have personnel that are specialized in SaaS and/or risk management and therefore know of and act on the risks of SaaS. As SMEs have less personnel

Research Question	Method
RQ1	Literature study, Survey
RQ2	Literature study, Survey
RQ3	Literature study, Survey
RQ4	Survey
RQ5	Survey
RQ6	Survey

Table 1. Research questions and the method chosen to answer them

in general, it is less likely that they are aware of the risks. Therefore, SMEs have become part of the focus of this research. Lastly, the IT sector is involved. This is done both out of convenience and curiosity. As the research involves a survey about SaaS, it is more convenient to have respondents who work in the field of IT. These people are more likely to understand the content of the survey and the technical terms in it, making the answers to the questions more valid and reliable. Furthermore, it would be interesting to see if the IT sector, who are involved with IT on a daily basis, are aware of the risks of SaaS and what their perception of this is. If the results show that they are not aware of it what would that say about Dutch SMEs in general, who are likely to have less knowledge about IT?

Though the the main research question has a small scope in terms of its target audience, the question itself is still broad and multifaceted. In order to answer the question, the following sub questions have been defined:

RQ1: What risks does SaaS pose to business continuity?

RQ2: How likely is it that a SaaS provider is unable to deliver its services?

RQ3: What are current solutions to tackle the business continuity problems posed by SaaS?

RQ4: Are the problems with regards to SaaS continuity known within the Dutch SME IT sector and are these considered to be a risk?

RQ5: What is currently being done within the Dutch SME IT sector to tackle the business continuity problems posed by SaaS?

RQ6: What is the main reason for an organization within the Dutch SME IT sector to (not) adopt a continuity solution?

These research questions all highlight different facets of the main research question. In order to answer these questions, two research methods will be used. Table 1 has been set up showing the method that will be used to answer each individual research question.

2.1 Literature Study

While the introduction to this paper provided some background to the research content, a literature study is necessary to, first of all, define the terms that are used in the research. This ensures a common background when reading the rest of the paper. Second, a literature study will be used to answer some of the research questions. As can be seen in table 1, the literature study will attempt to answer RQ1 *(What risks does SaaS pose to business continuity?)*, RQ2 *(How likely is it that a SaaS provider is unable to deliver its services?)*, and RQ3 *(What are current solutions to tackle the business continuity problems posed by SaaS?)*.

The search for relevant literature started by using search terms related to business continuity and SaaS in the search engines Google Scholar, ACM Digital Library and Google. The following terms were used, either individually or combined (in alphabetical order):

- Business continuity
- Cloud
- Cloud bankruptcy
- Cloud computing
- Continuity solutions
- IT disaster recovery
- SaaS
- SaaS adoption
- SaaS bankruptcy
- SaaS escrow
- SaaS guarantee fund
- SaaS risks
- SaaS trends
- Source-code escrow

Unfortunately, almost none of these searches led to papers that were completely relevant to this research. Most papers highlight only a small part of it. Therefore, another method was used to find more literature: snowballing. This method uses the reference list of a paper or the citations to the paper 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. As stated above finding relevant literature is difficult, so using snowballing once relevant literature has been found is a useful method to find more. The snowballing method was used on all papers that had been found through the search engine searches.

Again, only papers that highlight a certain part of the scope of this research were found. However, this result was already expected. Referring to table 1 again, the plan for this research is to answer research questions one through three with a literature study. The literature that was found was suitable to do so.

2.2 Survey

In order to answer research questions four through six and support the literature study for research questions one through three a survey is created (Table 1). The contents of the survey have been created with the research questions in mind and are partially based on an interview protocol by de Jong (2019) on the same topic. Some research questions have a direct link to certain survey questions, others are addressed by a combination of survey questions. The survey contains 31 questions in total, of which 18 questions are relevant for the research questions. The other 13 are either used to determine whether a respondent belongs to the target audience (SQ 1-3), provide a general background to the research (SQ 22-27) or are questions related to additional personal information and preferences (SQ 28-31). Table 2 indicates which research question each question from the survey is geared towards.

When creating the questions, excerpts from Iarossi (2006) were used to ensure good survey design. Iarossi (2006) states questions should be brief, objective, simple, and specific (or BOSS). The questions in the survey were checked on these criteria. In order to create a general understanding and common ground, definitions of 'SaaS', 'Traditional "shrink-wrapped"/on-premise software', and 'Continuity solution' are given at every page that contains questions related to one or more of these terms. This is in line with the guidelines for technical terms that was provided by Iarossi (2006).

This is a semi-structured survey which will therefore produce quantitative- as well as qualitative data. Descriptive statistics will be used to analyze the results, as almost all of the questions contain categorical data. The survey was distributed in Dutch, as the target group is people who work in the Dutch SME IT sector. However, an English translation of the survey can be found in appendix A. Furthermore, appendix B contains the Dutch survey.

The survey was public and distributed via the following channels:

- WhatsApp groups
- Facebook pages
- LinkedIn pages
- LinkedIn connection requests

Most responses came through the use of a tool which automatically approaches people within your target group by sending them a connection request through LinkedIn. In total, 1113 requests were sent out through this tool. The request was accepted 336 times and the survey was filled in through this channel 127 times. This means that in total the response rate for this distribution method is 11.4%. In total, 147 responses were collected, of which 121 could be used for the research.

SQ	General	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6
1 - 3	X						
4					X		
5		X					
6 - 7					X		
8			X		X		
9			X				
10 - 14						X	
15				X			
16						X	
17				X		X	
18							X
19					X		
20 - 21					X		X
22 - 31	X						
Total	**13**	**1**	**2**	**2**	**7**	**7**	**3**

Table 2. Indication of which research questions are targeted by the survey

3 Results

3.1 Literature Study

This chapter describes the results of the literature study that was conducted towards research questions one through three (Table 1). First, some definitions are provided. Then, the risks and threats of using SaaS are discussed. Next, an overview of continuity solutions is presented.

3.1.1 Software-as-a-Service

The cloud has become indispensable in current society, being our entertainment network (YouTube, Netflix), our social network (Facebook, Instagram), our virtual library (Google), our workbench (Basecamp, Adobe Creative Cloud), and a development network (GitHub, GitLab). The same is true for organizations, as more organizations are increasingly adopting SaaS-solutions in favour of traditional on-premise solutions (Spiotto & Spiotto, 2003).

Mäkilä et al. (2010) provided a study towards a definition of SaaS. From this, a list of five distinctive characteristics that are typically associated with SaaS was created:

1. Product is used through a web browser.
2. Product is not tailor made for each customer.
3. The product does not include software that needs to be installed at the customer's location.
4. The product does not require special integration and installation work.

5. The pricing of the product is based on actual usage of the software.

In order to have a common ground while reading the rest of this paper, these characteristics are what will be used as a definition for SaaS.

There are three major cloud system types: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) (Bibi, Katsaros & Bozanis, 2012). SaaS is a software deployment model that has become well known and popular in the mid 2000s. With SaaS, the software is provided to customers over the internet, which differentiates it from traditional on-premise software (Mäkilä et al., 2010).

However, SaaS is not the first internet based deployment model. An example of a more traditional internet based deployment model is Application Service Provider (ASP), which uses the internet or other wide area networks to provide online application services on a rental basis (Tao, 2001). A distinction between SaaS and ASP can be made on the basis of customization. With ASP a new instance of the software is created for each customer, whereas with SaaS the software is standardized for all customers (Mäkilä et al., 2010).

When an organization opts for SaaS in favor of on-premise software, that organization becomes part of a cloud environment. The typical SaaS-model contains four parties: customers, the SaaS-provider, a hosting party and a data center. The actual hardware where the software and data resides is out of the customer's reach and control. Some SaaS-solutions contain content from third-parties, which expands the model. Customers typically are unaware of the network behind a SaaS-solution, as they only deal with the SaaS-provider. The customer pays the SaaS-provider who in turn pays the different parties involved to deliver its service (van de Zande & Jansen, 2011). A basic SaaS-setup can be found in figure 1a.

Business critical SaaS-solutions, such as an enterprise resource planning system, are particularly interesting for SMEs. These are applications which traditionally come with high upfront costs and long installation times. With SaaS, however, customers only pay a (relatively) low monthly price or pay for what they actually use. As the solution itself is not hosted locally at the customer's organization, the costs of ownership and maintenance can be transferred to the SaaS-provider (Lewandowski, Salako & Garcia-Perez, 2013). Furthermore, little expertise is needed to run these solutions, as updates and maintenance are carried out automatically by the SaaS-provider. Overall, this allows SMEs to be able to experiment with business solutions that could improve the robustness of their sector.

3.1.2 Business Continuity

Aside from this positive outlook on the characteristics of SaaS, there are downsides to these as well. Not hosting an application locally means there is a dependence on other parties to be able to access the application and data. There are several aspects that would disrupt business continuity if these were to be compromised. Looking at the research questions posed in the previous chapter,

the first one is *"What risks does SaaS pose to business continuity?"*. According to van de Zande & Jansen (2011) the risks that using SaaS pose to business continuity include (in order of importance):

R1: Losing access to data

R2: Losing access to the application itself

R3: Losing support and maintenance

Data is the most important asset a company could lose. Depending on the type of SaaS-solution that is in place, losing data could mean losing all information about its customers, finances, personnel, orders: information that is critical for business continuity. Therefore, losing data has a high impact on business continuity. Even if the solution itself would become unavailable, access to the data would allow an organization to continue to operate (albeit slower and less efficient) and migrate their data to a different solution.

The latter comes with its own problems, however, as it is not likely that two different solutions will have the same way of dealing with data. Therefore, the next risk is losing access to the application itself. Having to migrate to a different solution not only entails having to transfer data in the right way (if the data was still available), but learning to operate in and with a new environment as well. This can be a difficult and time-consuming process, which negatively impacts business continuity. Lewandowski et al. (2013) conducted interviews with several SMEs about the adoption of a certain SaaS solution. One of the findings was that 20% was concerned about vendor lock in: the difficulty of switching to other solutions. Overall, losing access to the application itself has an impact on business continuity, but not as much as losing data.

Lastly, there is the risk of losing support and maintenance. In some scenarios, such as the bankruptcy of a SaaS-provider, a choice is made to keep the core services running but to cut other departments and/or services. In this case, customers would still be able to use a solution, but without having access to support or having the assurance that the solution will always be up to date. The latter comes with risks in and of itself, such as being vulnerable to (new) security threats. Losing support and maintenance is inconvenient and negatively impacts business continuity, but less so than losing access to the application itself or the data in it. These risks can be a deal-breaker when faced with the decision to migrate to the cloud or not. Offering some form of insurance can help persuade organizations that doubt the reliability of SaaS to make the switch.

The availability of SaaS applications relies on the robustness of the SaaS-provider and its underlying parties. With every additional party there are more places the network could "break". These external parties are one of the reasons using SaaS increases the chance of business interruptions, thus posing a threat to customers' business continuity. Research question two is *"How likely is it that a SaaS provider is unable to deliver its services?"*. There are two parts to this question: temporary unavailability and permanent unavailability. For the former, one should investigate the complete supply chain of a SaaS solution.

There are multiple places where the service could be interrupted, either at one of the parties within the network (SaaS-provider, hosting-provider, data center, a third party) or outside of the network (internet provider, electricity provider, landlords or mortgage holders for one of the parties). Because there are a lot of parties involved, there is a high chance of temporary unavailability of a service. Ernst & Young (2002) conducted a survey which showed that critical business systems were increasingly interrupted: more than 75 percent of organizations worldwide experienced unexpected unavailability (as cited in (Cerullo & Cerullo, 2004). The impact of these moments of unavailability depends on the duration, though it is clear that the longer the unavailability lasts, the greater the impact on the customer's organization will be. One possible way for organizations to protect themselves against this threat is to ensure there is a fallback option: having two internet providers, for example. That way, if one should fail, there is the possibility to continue with the other. An analysis should be done to pinpoint where organizations should set-up such fallback options.

Looking at permanent unavailability, there are a few possible scenarios. These include (in order of importance):

S1: SaaS-provider going out of business

S2: Hosting-provider going out of business

S3: Data center going out of business

S4: Third-party content providers going out of business

Going out of business can have different reasons. These include natural disasters, choosing to cease business out of free will, being taken over by another company and bankruptcy.

One of the characteristics of SaaS is the subscription-based payment model. Consequently, the revenue of a SaaS-provider is steady and predictable. Because of this, the chances of a SaaS-provider going bankrupt is small. Furthermore, if a bankruptcy were to happen, it is more in the interest of a Bankruptcy Trustee to keep this constant stream of revenue flowing because it can be used to pay off creditors. In order to do so, the SaaS application must be kept online. Should this happen, even though the service will be stopped eventually, it will not happen instantly, giving the customers some breathing room. Even though this is a logical assumption, a Bankruptcy Trustee is not obliged to keep the service running. Furthermore, a SaaS-provider may decide to simply cease operations and sell their assets instead of filing for bankruptcy. Next, even though there is a constant revenue stream, it should be highlighted that this is not a guarantee for a strong financial situation. If a SaaS-provider has a low number of customers, the impact of one customer leaving its service is high, possibly putting the provider in a difficult financial situation. Because of the different uncertainties mentioned in this section, although it is not likely to happen, bankruptcy is still a viable threat (Caplan, 2010).

3.1.3 Continuity Solutions

In order to protect themselves against the risks mentioned earlier, SaaS customers can opt for a continuity solution. There are several continuity solutions available, all differentiating in terms of costs, completeness, and what parties are involved. According to van de Zande & Jansen (2011) the following are the components that make up a complete SaaS business continuity solution (in order of importance):

C1: **Own Back-up:** 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.

These components tie in with the risks that were defined previously in section 3.2.1. Any solution containing these components should be able to effectively protect customers of a SaaS-provider when it goes bankrupt or otherwise out of business. However, not all continuity solutions will be complete.

3.1.4 External data back-ups

As stated, the first and most important component of a continuity solution is a back-up. This ties in with R1: *Lose access to data* and can be realized in three ways: receiving back-ups from the SaaS-provider, being able to back-up the data yourself or a combination of both. This solution is called *External data back-ups*. It is the most basic continuity solution which mostly lies in the hands of the SaaS-provider: they should design their SaaS solutions in such a way that it is possible - and, preferably, easy - to create back-ups. A simplified view of a SaaS-setup that is extended with the possibility to back-up data can be found in figure 1b.

3.1.5 Source-code escrow and SaaS-escrow

For the next continuity solution, the term 'escrow' must be considered. The definition of escrow according to Cambridge Dictionary is: *"an agreement between two people or organizations in which money or property is kept by a third person or organization until a particular condition is met"* [3]. In terms of software,

[3]Escrow. (n.d.) In Cambridge Business English Dictionary. Retrieved from https://dictionary.cambridge.org/dictionary/english/escrow

there are two kinds of escrow that are interesting for this research: *source-code escrow* and *SaaS-escrow*. As for shrink wrapped software, one way customers can protect themselves against the consequences of software developers going out of business is source-code escrow (Freeman, 2004). With this, the source code of the application is stored with a third party, the escrow agent. Should the developer go out of business or otherwise fail to deliver his support and maintenance obligations, customers can request the escrow agent to release the source-code. The source-code transfer will go through if the escrow agent can confirm that a valid release condition has been met (van de Zande & Jansen, 2011).

Even though this continuity solution works for shrink wrapped software, it would not be sufficient for SaaS software. If an organization uses shrink wrapped software, they must have the tools to run this software in-house. With SaaS, however, because the software is hosted off-premise, organizations generally do not possess these tools. Source-code escrow does not contain any of the components defined above for a SaaS business continuity solution, therefore making it an unsuitable solution for SaaS. Fortunately, with the rising popularity of SaaS, most escrow agents have added a SaaS-escrow service to their product portfolio. This is a modified version of source-code escrow, generally consisting of the addition of a data back-up. Furthermore, more complete SaaS-escrow solutions provide continuation of hosting as well, where an agreement with the hosting provider is arranged. In this case, the escrow-agent will take over the financial obligation towards the hosting provider if the SaaS provider is unable to fulfill its payments. In return, the hosting provider ensures that it will continue hosting the SaaS application and data under any circumstance (van de Zande & Jansen, 2011). A simplified view of a SaaS-setup extended with SaaS-escrow can be found in figure 1c. This version of SaaS-escrow contains components 1 (own back-ups) and 2 (hosting insurance). Some escrow-agents offer extra services such as delivering support and maintenance of the escrow application when the escrow is released (van de Zande & Jansen, 2011). In that case, the fourth component is also included, making it an almost complete SaaS business continuity solution.

SaaS-escrow solutions can be arranged either through a three-party arrangement between the SaaS-provider, the SaaS-customer and the escrow agent or with a 'master-contract'. The former is suitable when only one customer demands an escrow-arrangement, as with this arrangement only the customer that is involved in it is able to access the application when the escrow is released. However, when multiple customers demand an escrow-arrangement, a master-contract is more suitable. This is a two-party arrangement between the SaaS-provider and the escrow-agent, with which there is no limit on how many customers can benefit from the arrangement. Depending on if a customer wants to pay for this continuity solution or not, they will be able to benefit from it. Initially, a master-contract arrangement is more expensive than a three-party arrangement, but the costs can be spread over all the participating customers (van de Zande & Jansen, 2011). Therefore, after a certain threshold is exceeded, a master-contract will be the least expensive option.

When comparing source-code escrow with SaaS-escrow, the former can be described as a storage facility for sensitive information while the latter acts more like an insurance company for hosting costs. SaaS-escrow creates a possible risk for the escrow-company itself, as hosting an application becomes more costly when a SaaS-provider grows in size. Therefore, taking over hosting-costs could become too expensive for the escrow-company if a big SaaS-provider goes bankrupt. Another possible problem is that most SaaS-escrow solutions do not contain the third component defined above: arrangements with third-party content providers (van de Zande & Jansen, 2011). If content from third-parties are an important aspect of a SaaS application, this would mean that customers would still not be able to fully use the application when a SaaS-provider goes out of business.

3.1.6 SaaS Guarantee Fund

From the interviews that were conducted by van de Zande & Jansen (2011) for their research, another business continuity solution was defined: a *SaaS Guarantee Fund*. The idea behind this is that a SaaS-provider will set up a fund with a budget that is large enough to cover their expenses for a set period of time. All third-parties involved in running their SaaS applications should be taken into account when determining the budget. As SaaS-providers have a clear image of their financial situation, this budget is easily determined. The fund would then set up agreements with these third-parties to continue their services under any circumstance. The reason for using a fund is that this is a different legal entity than the provider itself. Therefore, if the provider has financial problems or faces bankruptcy, it would not be affected. During these financial problems or after a bankruptcy, the fund can take over the financial obligation towards the third-parties for the predetermined time frame. This allows the SaaS provider some time to make a restart, or provides customers a bit of breathing room for migrating their data to a new solution. A simplified view of a SaaS-setup extended with a SaaS Guarantee Fund can be found in figure 1c.

According to van de Zande & Jansen (2011) some organizations have set up a SaaS guarantee fund for their solution. However, there are no known SaaS guarantee funds with multiple participants. Such a fund would lower costs, depending on the amount of participants. As it is unlikely that multiple providers would be troubled at the same time, the required deposit per provider would be lower than with a guarantee fund that is tailored towards one specific solution. This is where the downside lies as well, as the fund is less customizable. Another problem lies in actually setting up a fund for multiple participants: who will take the initiative? Doing so requires time and money, while it does not seem to have any extra benefits for the provider who will initiate the fund. The most suitable party to set up and manage such a fund would be a (software) trade association.

Looking at the components of a complete SaaS business continuity solution defined in section 3.3, a SaaS guarantee fund could potentially contain all of

them. This depends on how the fund is set up. Therefore, it can be considered a complete SaaS business continuity solution.

3.1.7 Comparison

In this section, four continuity solutions have been defined. All differ in completeness, cost, set-up and the effects on the customer. These are the continuity solutions that were mentioned (in order of appearance):

1. External data back-ups
2. Source-code escrow
3. SaaS-escrow
4. SaaS guarantee fund

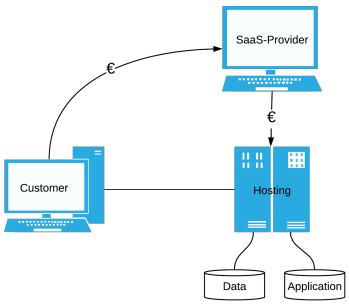
When considering these solutions and the list of components that was defined in section 3.3, it is apparent that two of the solutions contain too little components to be considered a complete enough continuity solution. External data back-ups take away the greatest risk associated with SaaS, losing your data, but the customers' business will still be interrupted, as without the application there is likely no easy or quick way to continue their business operations. This depends on how critical the SaaS application is to an organization. As for source-code escrow, it is likely that organizations who use SaaS will not have the tools or capacity to be able to host the application themselves. Therefore, it is not a sufficient continuity solution for SaaS software. Removing external data back-ups and source-code escrow from the list, the continuity solutions that are left are:

CS1: SaaS-escrow

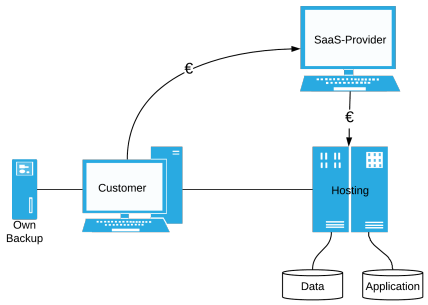
CS2: SaaS guarantee fund

These two continuity solutions are both able to satisfy all components defined in section 3.1.3, depending on how the arrangements are set-up. A comparison between the two has been made by van de Zande & Jansen (2011), which can be seen in table 3. These differences should be taken into account when investigating what continuity solution would work best for an organization.

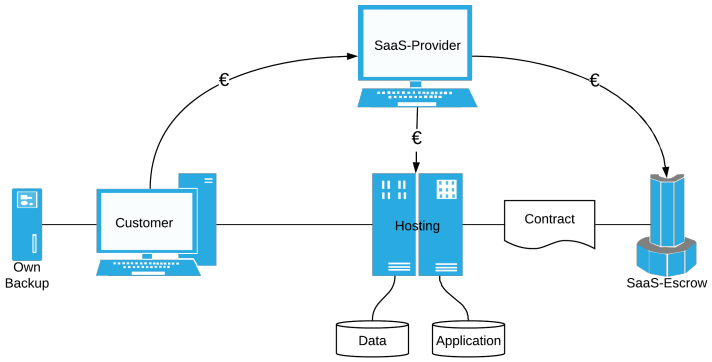
Having looked at the risks, threats, likeliness and continuity solutions, the question remains whether or not an organization should invest in a continuity solution or not. While it is not likely that a SaaS provider will go out of business, the threat remains present. Organizations should investigate for themselves whether or not a continuity solution is necessary. This can be done by performing a risk analysis. External data back-ups is a basic solution that is easy to implement and low in cost. Therefore, this is something SaaS customers should always demand. Depending on the determined risk, they can demand a more complete continuity solution (SaaS-escrow or a SaaS Guarantee Fund) as well.



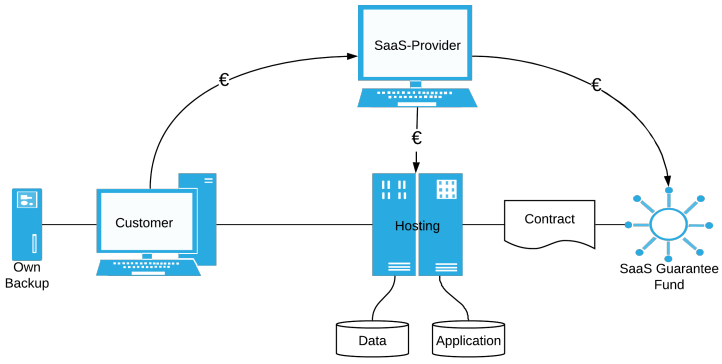
(a) A basic SaaS-setup



(b) SaaS-setup with back-ups



(c) SaaS-setup with SaaS-escrow continuity solution



(d) SaaS-setup with SaaS Guarantee Fund continuity solution

Figure 1. Schematic representation of different SaaS-setups.
Note: Reprinted from "Critical Applications Should Come With Critical Questions: Business Continuity Solution Adoption at Dutch SaaS-Providers", by M. de Jong, 2019, *Unpublished*, p. 17.

	SaaS-escrow	SaaS Guarantee Fund
Advantages	Easy to arrange	Complete control
	Legal knowledge	Customizable for specific solution
	Clear costs	(Expected) lower costs
	Experience	
Disadvantages	Expensive	Requires more effort from provider
	External party	Responsibility stays with the provider
		No prior experience

Table 3. Advantages and disadvantages of the different continuity solutions
Note: Adapted from "Business Continuity Solutions for SaaS Customers", by T. van de Zande and S. Jansen, 2011, *International Conference of Software Business*, p. 17-31.

3.2 Survey Results

In this section the results from the survey are presented. The survey was filled in by 147 people. Of these responses 26 have been removed due to the respondents not fitting into the target audience, which means there are 121 useful responses in total. The responses were collected between July 10th and August 1st, 2019. Using the research questions posed earlier as a structure, the results will now be presented.

3.2.1 Research Questions 1-3

The first research question to be answered is *"What risks does SaaS pose to business continuity?"*. This question was mostly answered by the literature study that was presented earlier in this chapter. However, as the respondents work with SaaS on a daily basis, there might be additional risks they have experienced that are not written about in literature. Therefore, survey questions 4 and 5 were added to the survey in order to potentially discover these. Survey question 4 asked the respondents if they think there are risks attached to using SaaS. Next, if respondents answered 'yes', question 5 asked what they believe these risks are. For question 4, 99 respondents said they do believe there are risks attached to using SaaS and 95 of these answered survey question 5, stating one or more risks. The answers to this question have been summarized and are shown in table 4. The percentages in the table are relative to the entire population of 121 respondents.

Second is the research question *"How likely is it that a SaaS provider is unable to deliver its services?"*. The same principle goes for this research question as the first one: the survey results are meant as an addition to the results of the literature study. Two survey questions were geared towards this research question: questions 8 and 9. The former asked respondents to rate the likeliness of three situations playing out, namely the bankruptcy of a SaaS provider, a hosting party, and a data center. Figure 5 displays the respondents' answers to this question. For all three situations, the majority of the respondents think the chance of it taking place is low. Next, survey question 9 asked respondents to

Risk	Count	Percentage
Dependence on/power of SaaS-provider	46	38.02%
Availability	44	36.36%
Security	36	29.75%
Privacy	27	22.31%
Software continuity	19	15.70%
Costs of employee training	2	1.65%

Table 4. Risks of using SaaS suggested by respondents (SQ5, 95 responses)

Scenario	Low	Medium	High
SaaS provider going bankrupt	66.94%	23.97%	9.09%
Hosting party going bankrupt	64.46%	31.40%	4.13%
Data center going bankrupt	76.86%	18.18%	4.96%

Table 5. "For the following scenarios, please indicate how likely you think these are to happen". Matrix question with the respondents being able to choose one column (low, medium, high) for each row (scenario). Each row therefore adds up to 100 percent. (SQ8, 121 responses)

indicate whether or not the SaaS solutions they use have ever been unavailable. The results can be found in table 9. A slight majority, 54,9%, states that their SaaS solution(s) have ever been unavailable.

The third research question is *"What are current solutions to tackle the business continuity problems posed by SaaS?"*. In addition to the literature study towards this question, survey questions 15 and 17 offer the possibility to discover more solutions. Here, respondents were asked to answer questions about the continuity solutions that were previously found in the literature study but were offered the opportunity to suggest other continuity solutions as well. Of the 121 respondents, 38 answered SQ 15 and/or SQ 17. Table 6 provides a summary of all the answers that have been given to these questions.

Contintuity Solution	Count	Percentage
Multi-cloud strategy	11	9.09%
SaaS-provider that is "too big to fail"	4	3.31%
Ensuring SaaS-provider uses industry standards	3	2.48%
Transferring the server after bankruptcy	2	1.65%
Managing the system yourself	1	0.83%
Multi-cloud including on-premise for data	1	0.83%
Customized continuity contract	1	0.83%
Invest/become stakeholder in the SaaS company	1	0.83%

Table 6. Continuity solutions suggested by respondents (SQ15 and SQ17, 37 responses)

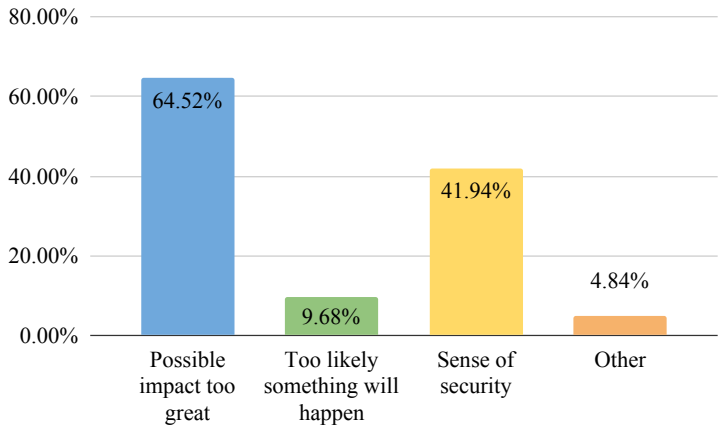


Figure 2. Why would you adopt a continuity solution? (SQ20, 62 responses)

3.2.2 Research Question 4

Next is the fourth research question: *"Are the problems with regards to SaaS continuity known within the Dutch SME IT sector and are these considered to be a risk?"*. There are five survey questions related to this research question, the first one asking respondents if they think there are risks attached to using SaaS withing an organization (SQ4). To this, just under a fifth of the respondents answered 'No'. Two questions later, the respondents are told about the risks of losing access to the application, data, support and maintenance and are asked if they are aware of these risks (SQ6). Almost all of the respondents answered that they are indeed aware of these risks: over 95%. The results of survey questions 4 and 6 can be found in table 9.

Near the end of the survey there are three questions (SQ19-21) which ask the respondents to indicate whether they would adopt a continuity solution or not if they were in the position to do so. Next, they are asked why they would or would not do so. The results show that a slight majority would adopt a continuity solution (51,24%) (Table 9). Of these people (62), 64,52% state they would do so because the possible impact is too high (Fig. 2). Of the people that would not adopt a continuity solution, 48,76% or 59 people, 52,54% would not do so because they believe the risk is too low (Fig. 3). This means that in total a little over a quarter of all 121 respondents (25,62%) thinks the risks attached to using SaaS are too little to adopt a continuity solution.

3.2.3 Research Question 5

The next results are geared towards research question five: *"What is currently being done within the Dutch SME IT sector to tackle the business continuity problems posed by SaaS?"*. There are seven survey questions in total which

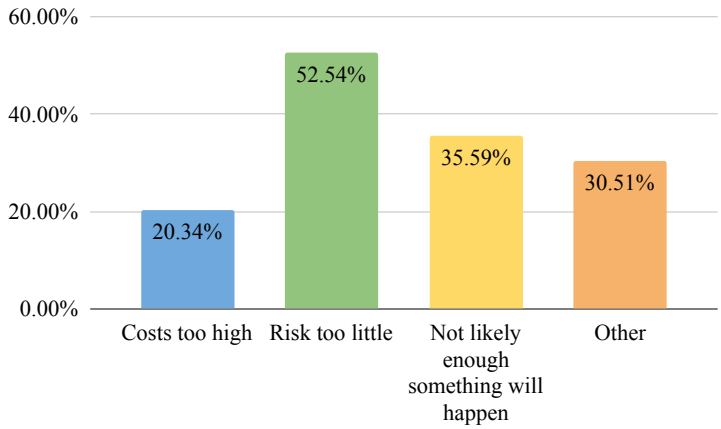


Figure 3. Why would you not adopt a continuity solution? (SQ21, 59 responses)

focus on this research question. The first five of these questions (SQ10-14) test the respondents' awareness of the continuity solutions that were found in the literature study. A little under 30% of the respondents is not aware of the existence of continuity solutions. The results of these survey questions can be found in table 9.

Next, the last two survey questions (SQ16 and SQ17) ask respondents whether the organization they work for uses a continuity solution and if so which one that is. The results show that the majority of the organizations respondents work for do use a continuity solution (Fig. 4) and that the most used continuity solution is external data back-ups (Fig. 5). The percentages shown in figure 5 are relative to the respondents who indicated their organizations use continuity solutions. However, four of them did not fill in this question, leaving 67 responses. The percentages in figure 5 add up to more than 100, because some organizations use more than one continuity solution. There are fifteen different combinations of continuity solutions that are used. A complete overview of exactly which and how many continuity solutions are being used per organization is given in table 7.

3.2.4 Research Question 6

Last is the research question *"What is the main reason for an organization within the Dutch SME IT sector to (not) adopt a continuity solution?"*. Three survey questions relate to this research question (SQ18, 20, 21) and all ask the respondents why either the organization they work for or themselves would or would not adopt a continuity solution. Of the people whose organization do not use a continuity solution, 60% thinks this is because they were never offered one (Fig. 6). The results of survey questions 20 and 21 can be found in figure 2 and

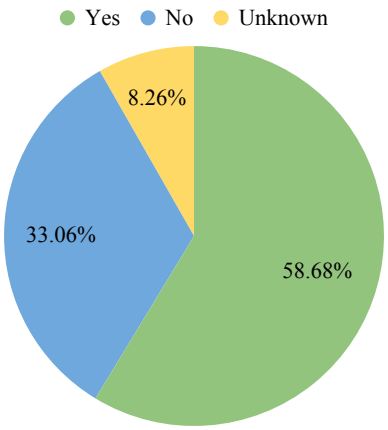


Figure 4. Does your organization use some sort of continuity solution? (SQ16, 121 responses)

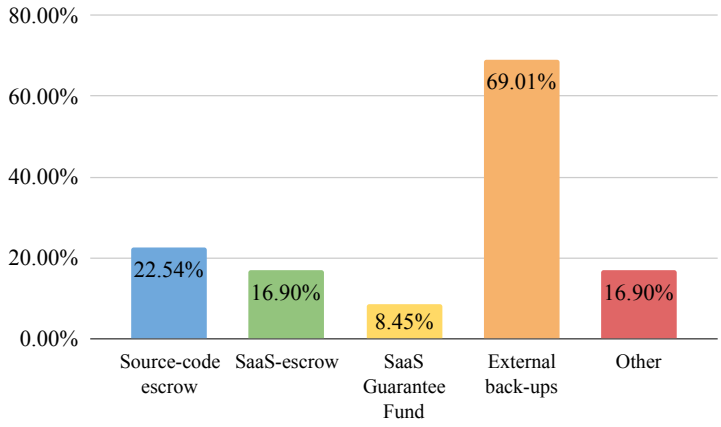


Figure 5. What continuity solution(s) does your organization use? (SQ17, 67 responses)

Continuity solution(s) in use	**Count**	**Percentage**
1 Solution	*47*	*38.84%*
Source-code escrow	6	4.96%
SaaS-escrow	1	0.83%
SaaS Guarantee Fund	2	1.65%
External data back-up	31	25.62%
Other	7	5.79%
2 Solutions	*13*	*10.74%*
Source-code escrow + External data back-up	3	2.48%
Source-code escrow + SaaS escrow	1	0.83%
SaaS-escrow + External data back-up	4	3.31%
SaaS Guarantee Fund + External data back-up	1	0.83%
Other + External data back-up	4	3.31%
3 Solutions	*6*	*4.96%*
Source-code escrow + SaaS-escrow + External data back-up	3	2.48%
Source-code escrow + External data back-up + Other	1	0.83%
Source-code escrow + SaaS-escrow + SaaS Guarantee Fund	1	0.83%
SaaS-escrow + SaaS Guarantee Fund + External data back-up	1	0.83%
4 Solutions	*1*	*0.83%*
Source-code escrow + SaaS-escrow + SaaS Guarantee Fund + External data back-up	1	0.83%
Total	**67**	**55.37%**

Table 7. Complete overview of continuity solutions used by the respondents' organizations (SQ17, 67 responses)

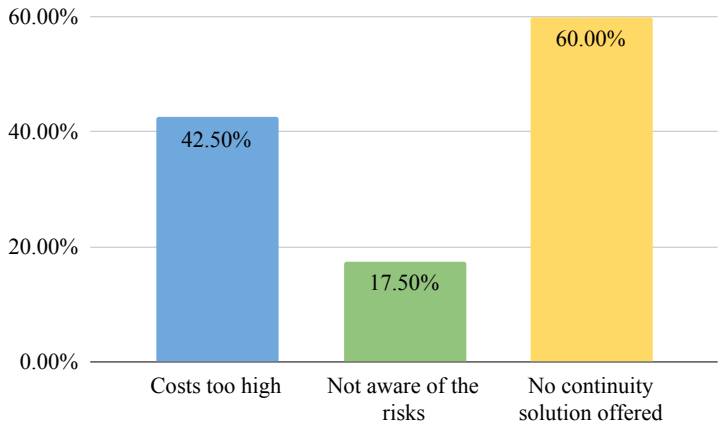


Figure 6. What do you think the main reason is for your organization to not adopt a continuity solution? (SQ18, 40 responses)

figure 3, respectively. These show that 64.52% of people who would adopt a continuity solution would do so because they believe the possible impact is too great. For the 52.54% who would not adopt one, the risk is too little. Table 8 provides a summary of the additional reasons respondents gave to (not) adopt a continuity solution.

3.2.5 Context

To conclude the results section there are four survey questions that do not relate to a research question directly but offer context to the research. First is question 23, which asks respondents how much they would be willing to pay for a continuity solution. This question has not been asked in direct numbers, but rather a percentage of the regular price they pay for their SaaS solutions. The results in figure 7 show that none of the respondents would pay more than 50% of their SaaS solutions' price for a continuity solution, with the largest group willing to pay between 1 and 4 percent. Next, the respondents were asked if they would prefer to have the price for a continuity solution included in the package price of a SaaS solution or to have this as an optional service. To this, a little over 60% stated they would prefer continuity solutions to be an optional service (Fig. 8).

Finally, the last survey questions that will be discussed here are about the aim of this research: awareness of the subject. The survey forced the respondents to think about the risks SaaS can pose to an organization and the continuity solutions that can lessen the impact of these. When asked if the survey had made the respondents more aware of this subject, 43.8% said that was the case. Furthermore, 40.5% of the respondents stated they are planning on looking into the subject. These results can be found in table 9.

Reason	Count	Percentage
Why adopt a continuity solution (SQ20)		
Everything will stop eventually	1	0.83%
Business continuity	1	0.83%
Simplification and security of development pipeline	1	0.83%
Why not to adopt a continuity solution (SQ21)		
Own possibilities are enough	3	2.48%
SaaS-provider is "too big to fail"	3	2.48%
Non-business critical SaaS applications	2	1.65%
Should be standard / handled by provider	2	1.65%
Protection through interest of the bank	1	0.83%
Wanting to switch as soon as possible, so no use	1	0.83%
It is a business risk	1	0.83%

Table 8. Other reasons given to the question why one would or would not adopt a continuity solution (SQ20, 3 responses; SQ21, 18 responses). Percentages relative to total number of respondents (121).

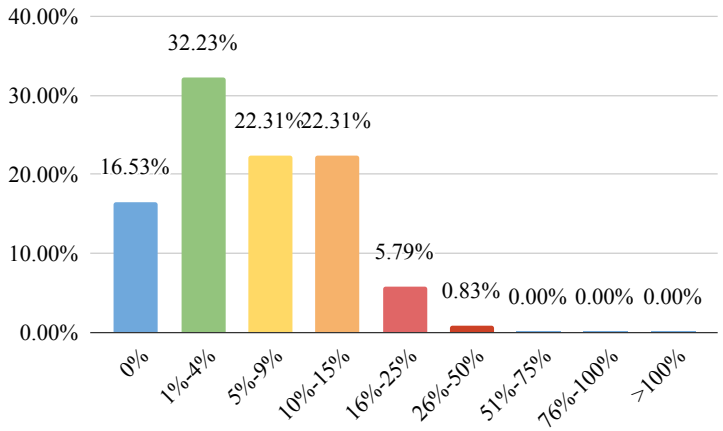


Figure 7. How much would you be willing to pay to guarantee business continuity when using SaaS? A maximum of ...% on top of the monthly SaaS package price. (SQ23, 121 responses)

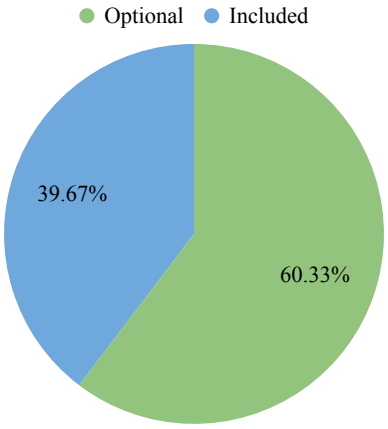


Figure 8. Would you prefer a continuity solution to be directly included in the price of a SaaS package or to have this be an optional service? (SQ24, 121 responses)

RQ	SQ	Question	Yes	No
RQ2	SQ9	Has/have the SaaS application(s) used by your organization ever been unavailable?	55.37%	44.63%
RQ4	SQ4	Do you think there are risks attached to using SaaS within an organization?	81.82%	18.18%
RQ4	SQ6	Were you aware of the possible risks of losing access to data, the application, support, and/or maintenance?	95.87%	4.13%
RQ4	SQ19	If you had the opportunity to do so, would you adopt a continuity solution when using SaaS?	51.24%	48.76%
RQ5	SQ10	Are you aware of the existence of "continuity solutions"?	70.25%	29.75%
RQ5	SQ11	Had you heard of "source-code escrow" before this survey?	78.51%	21.49%
RQ5	SQ12	Had you heard of "SaaS-escrow" before this survey?	48.76%	51.24%
RQ5	SQ13	Had you heard of "SaaS Guarantee Fund" before this survey?	23.14%	76.86%
RQ5	SQ14	Had you heard of using external data back-ups as a continuity solution before this survey?	89.26%	10.74%
-	SQ25	Has this survey made you more aware of the possible risks of using SaaS?	43.80%	56.20%
-	SQ26	Are you planning on looking into the possible risks and solutions when using SaaS?	40.50%	59.50%

Table 9. Results of all survey questions with the answer possibilities yes and no. All questions received 121 responses.

4 Analysis

Using the results from the literature study and survey, the research questions will be answered in this chapter. This will be done systematically, starting with the first research question: *"What risks does SaaS pose to business continuity?"*. Through the literature study three risks have been identified:

R1: Losing access to data

R2: Losing access to the application itself

R3: Losing support and maintenance

Within the survey there was an opportunity to suggest other risks as well. However, there were no risks mentioned that either are not already present in the list above or were focused on the topic at hand: business continuity. Therefore, the answer to research question one is: when using SaaS within an organization, the risks that could threaten business continuity are losing access to data, losing access to the application itself, and losing support and maintenance.

The second research question is *"How likely is it that a SaaS provider is unable to deliver its services?*. From the literature study it became apparent that there are two kinds of unavailability: temporary and permanent. As there are many factors and parties that come into play when attempting to access a SaaS application, it is likely that the application will be temporarily unavailable at some point in time. The survey results mirrored this conclusion: 55.37% of the respondents said their SaaS applications have been unavailable in the past. Looking at permanent unavailability, that chance seems to be lower because of the nature of the SaaS payment model. First, this payment model enables SaaS providers to have a clear overview of their financial situation, as there is a constant stream of income because of the monthly payment system. Second, it is in the interest of a Bankruptcy Trustee to keep a SaaS application running for this same reason. The constant stream of income can be used to pay off any debts the SaaS provider might have. Looking at the survey results, the respondents seem to mirror this train of thought: they think the chances of a SaaS provider, hosting party or data center going bankrupt is low (66.94%, 64.46%, and 76.86%, respectively). Taking all of this into account, the answer to the second research question is: while it is likely that a SaaS application will be temporarily unavailable at some point in time, the chance of it becoming permanently unavailable is low. However, it is not impossible. Consequently, there are still risks involved in using SaaS for business critical processes.

Next, the third research question is: *"What are current solutions to tackle the business continuity problems posed by SaaS?"*. The continuity solutions that have been found through the literature study are:

CS1: SaaS-escrow

CS2: SaaS Guarantee Fund

Two other solutions were found (external back-ups and source-code escrow), but these were insufficient when looking at the list of components a complete SaaS continuity solution should have, previously defined in section 3.1.3. The respondents of the survey have suggested eight additional continuity solutions (Table 6). However, none of these satisfy all components that a complete SaaS continuity solution should have. Therefore, the answer to the research question is: currently, there are two continuity solutions that are complete for SaaS applications. These are 'SaaS-escrow' and 'SaaS Guarantee Fund'.

Moving to the fourth question, *"Are the problems with regards to SaaS continuity known within the Dutch SME IT sector and are these considered to be a risk?"*, this is the first question to solely be answered with the results from the survey. From this, it becomes apparent that the vast majority believes there are risks attached to using SaaS (81.82%). However, a significantly lower percentage would adopt a continuity solution if they had the power to do so (51.24%). Focusing on the respondents that said they do believe there are risks attached to using SaaS, only a slight majority would adopt a continuity solution (53.54%). Of the respondents that would not adopt a continuity solution, 52.54% say they would not do so because the risk is too little. This translates to a little over a quarter (25.62%) of the total number of respondents who believe the risk involved with using SaaS is too little to adopt a continuity solution. Furthermore, 17.35% stated they would not do so because it is not likely enough that something will happen. Of the people that would adopt a continuity solution, 64.52% says they would do so because the possible impact is too great, which translates to 33.07% of the total number of responses. Furthermore, 4.96% of the total number of respondents would adopt a continuity solution because they think it is too likely something will happen. To answer research question four: while the vast majority of people within the Dutch SME IT sector do seem to be aware of the problems with regards to SaaS continuity, only a slight majority would try to insure themselves against these risks. The people that choose not to adopt a continuity solution either do not do this because they think the risk is too little or it is not likely enough that something will happen: 42.97% in total. However, 38.02% think the possible impact is too great and/or that it is too likely something will happen. Therefore, while the problems are mostly known, whether these problems are then considered to be actual risks is divided within the sector.

Fifth is the research question *"What is currently being done within the Dutch SME IT sector to tackle the business continuity problems posed by SaaS?"*. The survey results show that 58.68% of the organizations the respondents work for use continuity solutions. About a third (33.06%) does not and 8.26% of the respondents were unsure about their organizations' situation. Looking at the organizations that use continuity solutions, the vast majority uses external data back-ups (69.01%) and 22.54% use source-code escrow. However, the literature study has determined that both are not complete continuity solutions for SaaS. Furthermore, when analyzing the answers that were given to the 'other' option when indicating what continuity solutions their organization use, another 33.39% uses continuity solutions that are incomplete for SaaS. Translating these

percentages to the entire respondent sample, just under three quarters use some form of incomplete SaaS continuity solution: 73.31%. However, this does not take into account the possibility that an organization might use more than one continuity solution. Previously, fifteen different combinations of continuity solution use were discovered. The most prevalent is the use of one continuity solution (38.84%), with external data back-ups being the most used. About a quarter (25.62%) of all respondents' organizations only use external data back-ups. When taking the mean of the other combinations' prevalence percentages (2.125%) it becomes apparent that the group using this combination of continuity solutions is significantly larger than all other combinations. A little over 10 percent (10.47%) uses two continuity solutions, 4.96% uses three and 0.83% uses four. Aside from the continuity solutions that are actually being used, it is interesting to know how aware the sector is of the continuity solutions themselves. Therefore, there were a few survey questions which asks if the respondents had heard of certain continuity solutions before. Not surprisingly, external back-ups is the most known continuity solution with almost 90 percent (89.26%) stating they had heard of this before. Source-code escrow is a term most respondents knew as well (78.51%). Interestingly, the only two continuity solutions that have been marked as 'complete' in the literature study are the most unknown solutions, with 51.24% having never heard of SaaS-escrow and 76.86% not knowing about SaaS Guarantee Funds. Furthermore, 29.75% was not aware of the existence of continuity solutions at all. It is likely that they had heard of the individual terms, but not that these were a form of continuity solutions, considering the percentages of people having heard of the different continuity solutions before. Reflecting back on the research question, *"What is currently being done within the Dutch SME IT sector to tackle the business continuity problems posed by SaaS?"*, it is difficult to give a straightforward answer. About two-thirds either do not use a continuity solution or use one that is insufficient to protect an organization against the risks that come with SaaS. This is likely because these organization are either not aware of the risks, do not know about the existence of continuity solutions, believe continuity solutions are included within a SaaS package or do not think the risk is high enough to justify the costs of continuity solutions. About one-fifth does seem to aware of the risks and wanting to insure themselves against these, by either using one complete SaaS continuity solution or using at least two continuity solutions. The answer to the research question is therefore: while the majority is not (sufficiently) insured against the risks SaaS pose to organization, there is a small group that do use complete continuity solutions to protect themselves against these risks.

Finally, the sixth research question is *"What is the main reason for an organization within the Dutch SME IT sector to (not) adopt a continuity solution?"*. This question has been addressed in the survey in two different ways: from the perspective of the respondents' organization and from the respondents' own point of view. Precisely 60 percent of respondents' said they believe their organization does not use a continuity solution because they were never offered one. This translates to 19.84% of the total sample. When asking the respondents that would not adopt a continuity solution themselves why they would not do so, the

most prevalent answers are that the risk is too little (52.54%) and that it is not likely enough that something will happen (35.59%). Of the respondents that would adopt a continuity solutions themselves, a large majority (64.52%) would do so because the possible impact is too great. Translating these percentages to the total sample, 25.62% believes the risk is too little, 17.35% believes it is not likely enough something will happen, and 31.46% believes the possible impact is too great not to adopt a continuity solution. Answering the question, the main reason that has been given for not adopting a continuity solution is that the risk is too little. Interestingly, the main reason given to do adopt one is that the possible impact is too great. This goes along with the answer to research question four: the sector seems to be divided over if the problems with regards to SaaS continuity are risks that should be accepted as common business risks or should be insured against.

5 Discussion

This chapter will discuss the limitations of the research that has been conducted. Furthermore, advice for future work around the subject of this research is given.

5.1 Limitations

Two methods were used in order to answer the research questions that were posed at the start of this paper. First, a literature study was conducted to (partially) answer research questions one, two, and three. Finding literature proved to be a difficult task, as this is a subject that has not been explored much in scientific literature. Therefore, only twelve useful sources could be found, one of which is a paper written by my co-author Marco de Jong which was written during the same time this paper was written. Furthermore, the paper written by van de Zande & Jansen (2011) is cited many times throughout this paper. This is because their paper served as an inspiration for this research. It contains the background knowledge needed for this research and was the only paper that could be found that has the same subject as this research. Everything stated in this paragraph might make the literature study of lesser quality.

Next, a survey was used to answer research questions four, five, and six as well as complementing the literature study towards research questions one, two, and three. Though the survey was checked before distribution by multiple people, four respondents stated that some of the survey questions felt suggestive. Question 18 has been pointed out specifically by two of these four respondents. Looking at the survey after the research is finished, the author agrees with this statement. The question was a follow-up to question 16: "Does your organization use some form of continuity solution?". If the respondents answered no, they were led to question 18: "If not, what do you believe the main reasons are for your organization to not adopt a continuity solution?", a multiple choice (checkbox) question with the answer possibilities: 'Costs', 'Not being aware of the risks', and 'Not having been offered a continuity solution'. The possibility

to answer something else, which is present in all other applicable question, was not added here. Though it was present in the paper version of the survey, it was forgotten in the survey that was distributed. Furthermore, there is no option along the lines of 'The possible impact is too low' or 'The chance something might happen is too small'. This is a severe oversight, which makes the results of this question invalid. The results were used to answer research question 6: *"What is the main reason for an organization within the Dutch SME IT sector to (not) adopt a continuity solution?"*. Another limitation to answering this question is that the respondents were only asked to indicate what they believe their organizations' reasons are when they do not use a continuity solution, not when they do use one. Therefore, the only perspective that can be used for this question is that of the respondents themselves on why they would or would not adopt a continuity solution.

Some survey questions have not been used in the research even though they were meant to be. Survey questions 7 and 8 were supposed to be used together to create a risk analysis for every individual respondents' situation, but this proved to be unfeasible. Therefore, the results were not used. Furthermore, due to technical issues, the results for survey question 22 had to be removed as well. Here, the respondents were shown five categories and were asked to rearrange these in order of urgency. However, one respondent pointed out that this question could not be done on a tablet. This was not checked beforehand. Consequently, an additional research question that focused on this subject (how important SaaS continuity is for the Dutch SME IT sector) was removed.

The last limitation is the group of survey respondents. Though all respondents belong to the target group, it is not likely that all of them are the decision makers within their organization when it comes to SaaS applications/risk management. Therefore, the answers to the research questions that have been given before might not be generalizable to the Dutch SME IT sector as a whole.

5.2 Future work

In order to make the conclusions of this research more reliable, the survey should be held again without the flaws that were mentioned before. Furthermore, the target group should be more specific, focusing on the people that make decisions about SaaS applications/risk management within their organization.

Another possibility for future work is to expand this research to other sectors as well. As the research in this paper has been focused on the IT sector, it is to be expected that the awareness about the subject at hand is significantly lower in other sectors. It would be interesting to see if and how organizations in sectors that are not working with IT on a daily business deal with these risks.

6 Conclusion

With this research an attempt was made to map the current state of the Dutch SME IT sector when it comes to the use of SaaS and its risks to business

continuity. This was done through a literature study as well as a survey with a total of 121 responses. With the rise of SaaS, most of the attention went to the advantages it could bring to organizations. However, as became apparent through this research, there are risks attached to using SaaS as well. Starting with the risks that would have the most impact on business continuity, the risks are losing access to: data, the application, support, and maintenance. However, one would not have to insure ones self if there is no chance of it ever happening. Through this research it became clear that it is not likely a SaaS provider, or a hosting party/data center, would go out of business. This is because of the predictable nature of their financial situation. However, going out of business can have other reasons than bankruptcy alone. Therefore, there is always a chance of it happening. Since the impact on organizations could be severe if anything should happen, it is advisable to undertake a risk analysis to decide if an organization should insure itself against these risks or not. There are two continuity solutions which offer complete protection for SaaS applications: SaaS-escrow and a SaaS Guarantee Fund. However, the majority of organizations use either no continuity solution or one that does not offer complete protection. This may be because the likeliness of something happening is low. As the impact remains great, it would be advisable to implement at least some form of continuity solution. This is something SaaS customers should discuss and take into account when looking into subscribing to a SaaS solution.

The main question of this research is *"What is the current state of the Dutch SME IT sector regarding SaaS continuity?"*. It can be stated that while most of the sector does seem to be aware of the risks, awareness about continuity solutions is significantly lower. This is especially true for continuity solutions that offer complete protection (SaaS-escrow, SaaS Guarantee Fund), as opposed to more basic or traditional solutions (source-code escrow, back-ups). There is an opportunity here for new businesses to create more awareness around the subject. This can be especially helpful for organizations within other sectors that are not as familiar with IT.

There is a responsibility for SaaS providers to know these risks as well. Customers have a right to be informed about them and should be able to discuss how they would like to deal with these in accordance with the SaaS provider. Awareness is the first step. From then, each organization can decide for itself whether they would like to implement a continuity solution or not. External data back-ups is a basic solution that is easy to implement and low in cost. Therefore, this is something SaaS customers should always demand. Depending on the determined risk, they can demand a more complete continuity solution (SaaS-escrow or a SaaS Guarantee Fund) as well.

About 75 percent of Dutch SME IT organizations are at risk of suffering business interruptions through SaaS due to not being (sufficiently) protected against the risks that come with using SaaS. Considering the organizations targeted in this research are working with IT on a daily basis, it is likely that that number increases when looking at SMEs in other sectors. As the SME sector represents about 99 percent of all organizations in the Netherlands and

is responsible for 70 percent of the employment opportunities[4], it is important that the sector is informed and aware of these risks and protects themselves against these accordingly. A well-protected sector leads to a strong sector.

[4]MKB Servicedesk. (2019, March 29). Informatie over het MKB (midden- en kleinbedrijf) in Nederland. Retriever August 8, 2019, from https://www.mkbservicedesk.nl/569/informatie-over-midden-kleinbedrijf-nederland.htm

References

Bibi, S., Katsaros, D., & Bozanis, P. (2012). Business application acquisition: on-premise or saas-based solutions? *IEEE software*, *29*(3), 86–93.

Caplan, D. (2010). Bankruptcy in the cloud: effects of bankruptcy by a cloud-services provider. Technical report, Technical report, Law Offices of David S. Caplan, 1289 FordhamBlvd., Suite 345 Chapel Hill, NC 37514, USA.

Cerullo, V. & Cerullo, M. J. (2004). Business continuity planning: a comprehensive approach. *Information Systems Management*, *21*(3), 70–78.

de Jong, M. (2019). Critical applications should come with critical questions: Business continuity solution adoption at dutch saas-providers. Bachelor Thesis.

Freeman, E. H. (2004). Source code escrow. *Information Security Journal*, *13*(1), 8.

Hiles, A. N. (1994). Service level agreements: Panacea or pain? *The TQM Magazine*, *6*(2), 14–16.

Iarossi, G. (2006). *The power of survey design: A user's guide for managing surveys, interpreting results, and influencing respondents*. The World Bank.

Lewandowski, J., Salako, A. O., & Garcia-Perez, A. (2013). Saas enterprise resource planning systems: challenges of their adoption in smes. In *2013 IEEE 10th International Conference on e-Business Engineering*, (pp. 56–61). IEEE.

Mäkilä, T., Järvi, A., Rönkkö, M., & Nissilä, J. (2010). How to define software-as-a-service–an empirical study of finnish saas providers. In *International Conference of Software Business*, (pp. 115–124). Springer.

Mell, P. & Grance, T. (2011). The nist definition of cloud computing. *NIST Special Publication*, *800*, 145.

Spiotto, A. H. & Spiotto, J. E. (2003). The ultimate downside of outsourcing: Bankruptcy of the service provider. *Am. Bankr. Inst. L. Rev.*, *11*, 47.

Tao, L. (2001). Shifting paradigms with the application service provider model. *Computer*, *34*(10), 32–39.

van de Zande, T. & Jansen, S. (2011). Business continuity solutions for saas customers. In *International Conference of Software Business*, (pp. 17–31). Springer.

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, (pp.38). Citeseer.

A Survey English

All of your responses will be treated as confidential. The results of the survey will be used for research purposes.

SaaS : Software-as-a-Service. Software that is accessed through an Internet connection. There is often a subscription payment model. Examples of SaaS solutions are a CRM, ERP, productivity tools (Microsoft Office), online workspaces (Slack) and accounting software.

1. What is the domain of your organization? **Open**
2. Do you work for a small-to-medium enterprise? **Y/N**
3. Does your organization use business critical SaaS applications? **Y/N**
4. Do you think there are risks attached to using SaaS within an organization? **Y/N**
5. If so, what do you think these are? **Open**
6. If a SaaS provider goes bankrupt its customers could lose access to the application as well as the data that is stored in it. Furthermore, customers could lose access to support and/or maintenance. Were you aware that this could happen? **Y/N**
7. Please indicate for the three most important SaaS solutions used in your organization what impact the following continuity risks would have on your organization if these solutions were to be affected. Possible answers are: low, medium, high. *Please fill in at least one row. If your most important SaaS solution is a CRM, you would fill in 'CRM' in the first row in the column 'SaaS solution'. Next, type 'Low', 'Medium', or 'High' in the other four cells in that row, depending on how much impact the risk in that column would have on your organization if your CRM system would be affected.***Matrix with the following items as columns. Low/Medium/High as possible answers. See table 11 below for the design of this question.**
   - SaaS solution
   - Losing access to your data
   - Losing access to the application
   - Losing access to support
   - Losing access to maintenance
8. For the following scenarios, please indicate how likely you think these are to happen. **Low, Medium, High**
   - SaaS provider going bankrupt
   - Hosting party going bankrupt

- Data center going bankrupt

9. Has/have the SaaS solution(s) your organization uses ever been unavailable? **Y/N**

10. Are you aware of the existence of 'continuity solutions'? These provide end-users with some form of guarantee that their business is able to continue should something go wrong with the provider. **Y/N**

11. 'Source-code escrow' is an arrangement between vendor and user that ensures the user will receive the source-code for the application he paid for when the provider is unable to fulfill its obligations towards the customer. Had you heard of 'source-code escrow' before this survey? **Y/N**

12. 'SaaS-escrow' is a modified version of source-code escrow which generally consists of the addition of an external data back-up with the deposit of the source-code and continuation of hosting*. Had you heard of 'SaaS-escrow' before this survey? *This means the escrow agent will take over the financial obligation towards the hosting party, who promises to continue hosting the SaaS application and data.***Y/N**

13. With a 'SaaS guarantee fund' a SaaS provider sets up a fund with enough budget to cover the costs for several months so the application can keep functioning. Because of this, no data will be lost and data leaks can be prevented. Had you heard of 'SaaS guarantee fund' before this survey? **Y/N**

14. Finally, users have the option to create external data back-ups. Had you heard of using external data back-ups as a continuity solution before this survey? **Y/N**

15. Do you know any other continuity solution that has not been mentioned here? **Open**

16. Does your organization use some sort of continuity solution? **Y/N/I do not know**

17. If so, please indicate what continuity solution(s) your organization uses. **Checkbox**

    - Source-code escrow
    - SaaS-escrow
    - SaaS guarantee fund
    - External data back-up
    - Other:

18. If not, what do you think the main reasons are for your organization not to use a continuity solution? **Checkbox**

- Costs
- Not being aware of the risks
- Not being offered a continuity solution
- Other

19. If you had the opportunity to do so, would you adopt a continuity solution when using SaaS? **Y/N**

20. If so, why? **Checkbox**

    - The ossible impact is too great not to
    - It is too likely something will happen
    - It offers a feeling of security
    - Other:

21. If not, why not? **Checkbox**

    - The costs are too high
    - The risk is too low
    - It is not likely enough that something will happen
    - Other:

22. Please arrange the following items in order of urgency, based on your own opinion. Number 1 is the most urgent and number 5 the least.

    (a) Business continuity risks with SaaS
    (b) Cyber security risks
    (c) Natural disasters
    (d) Reputation risks
    (e) Fraud

23. How much would you be willing to pay to guarantee business continuity when using SaaS? A maximum of ...% on top of the monthly SaaS package price.

    - 0%
    - 1%-4%
    - 5%-9%
    - 10%-15%
    - 16%-25%
    - 26%-50%
    - 51%-75%
    - 76%-100%

- More than 100%

24. Would you prefer a continuity solution to be directly included in the price of a SaaS package or to have this be an optional service? **Included/Optional**

25. Has this survey made you more aware of the possible risks of using SaaS? **Y/N**

26. Are you planning on looking into the possible risks and solutions when using SaaS? **Y/N**

27. Would you like to elaborate on the topics of this survey? **Open**

28. Would you like to enter the draw for a "dinercheque" worth 150,- euro? **Y/N**

29. Would you like to receive the results of this research? **Y/N**

30. Could you leave your email address here? *Required if you want to enter the draw for a dinercheque / receive the results of this research. Your data will be handled with care.* **Open**

31. Do you allow us to...
    - contact you for follow-up questions? **Y/N**
    - contact you for information about continuity solutions? **Y/N**

Once again, thank you for your participation in this research. Sharing the survey would be much appreciated. For this, you can use the social buttons below. If you have any questions, remarks or concerns please do not hesitate to email me at d.r.vanvelzen@uu.nl or contact me via LinkedIn at `https://www.linkedin.com/in/denisevanvelzen/`.

SaaS Solution	**Losing access to your data**	**Losing access to the application**	**Losing support**	**Losing maintenance**
ERP	*High*	*Medium*	*Low*	*Medium*

Table 10. Design of survey question 7 with an answer example

B Survey Dutch

De Universiteit Utrecht doet in samenwerking met ACC ICT onderzoek naar bedrijfscontinuïteit bij het gebruik van Software-as-a-Service. Dit onderzoek richt zich op Nederlands midden- en kleinbedrijf binnen de IT sector. Het doel van dit onderzoek is het belichten van een nog te weinig besproken onderwerp. Wij willen u bedanken voor uw deelname. Uw bijdrage aan dit onderzoek zal zorgen voor een versterking van de Nederlandse MKB IT sector. Onder de deelnemers zal drie keer een dinercheque ter waarde van 150,- euro verloot worden.

Het onderzoek zal ongeveer 15 minuten van uw tijd in beslag nemen. Er zal betrouwbaar met uw gegevens worden omgegaan en de resultaten worden geheel anoniem verwerkt.

SaaS : Software-as-a-Service. Software waarvan de toegang verleend wordt via een internet verbinding. Vaak wordt er gebruikgemaakt van een abonnementsvorm als betaalmodel. Voorbeelden van SaaS oplossingen zijn een CRM, ERP, productiviteits tools, online workspaces en boekhoudsoftware.
Bedrijfskritisch : Indien een applicatie bedrijfskritisch is, dan brengt downtime van meerdere dagen en/of het verlies van de bijbehorende data uw bedrijf ernstige financiële- en/of imago schade toe.

1. Wat is het domein van uw organisatie? **Open**
2. Bent u werkzaam binnen het midden- en kleinbedrijf? **J/N**
3. Maakt uw organisatie gebruik van bedrijfskritische SaaS? **J/N**
4. Denkt u dat er risico's verbonden zijn aan het gebruikmaken van SaaS binnen een organisatie? **J/N**
5. Zo ja, wat denkt u dat deze zijn? **Open**
6. Wanneer een SaaS leverancier failliet gaat kunnen de gebruikers de toegang tot de applicatie verliezen, net als de data die hierin opgeslagen staat. Bovendien kunnen de gebruikers toegang tot ondersteuning en/of onderhoud verliezen. Bent u zich ervan bewust dat dit kan gebeuren? **J/N**
7. Geef alstublieft voor de drie belangrijkste SaaS oplossingen in uw organisatie aan welke impact de volgende continuïteitsrisico's zouden hebben op uw organisatie wanneer deze getroffen zouden worden. Mogelijke antwoorden zijn: laag, gemiddeld, hoog. *Vul alstublieft minimaal 1 rij in. Als uw meest belangrijke SaaS oplossing een CRM systeem is, dan vult u 'CRM' in op de eerste rij in de kolom 'Saas oplossing'. Vervolgens vult u voor de overige vier kolommen in die rij 'Laag', 'Gemiddeld' of 'Hoog' in, afhankelijk van hoeveel impact het bijbehorende risico zou hebben op uw organisatie wanneer uw CRM systeem aangetast zou worden.* **Matrix met de volgende items als kolommen. Laag/Medium/Hoog als mogelijke antwoorden. Zie tabel 11 onderaan voor de vormgeving van deze vraag.**

- SaaS oplossing
- Toegang verliezen tot data
- Toegang verliezen tot applicatie
- Toegang verliezen tot support
- Toegang verliezen tot maintenance

8. Geef alstublieft voor de volgende scenario's aan hoe groot u de kans acht dat deze plaats zullen vinden. **Laag, Medium, Hoog**

   - Faillissement van een SaaS leverancier
   - Faillissement van een hosting partij
   - Faillissement van een datacentrum

9. Is/zijn de SaaS oplossing(en) die uw organisatie gebruikt ooit niet toegankelijk geweest? **J/N**

10. Bent u zich bewust van het bestaan van 'continuïteitsoplossingen'? Deze bieden gebruikers een garantie dat hun organisatie kan blijven opereren wanneer er iets misgaat met de aanbieder. **J/N**

11. *'Source-code escrow'* is een overeenkomst tussen aanbieder en gebruiker die de gebruiker verzekert dat hij de broncode voor de applicatie waarvoor hij betaald heeft ontvangt wanneer de aanbieder niet kan voldoen aan zijn verplichtingen richting de gebruiker. Had u al eerder gehoord van 'source-code escrow' voor deze enquête? **J/N**

12. *'SaaS-escrow'* is een aangepaste versie van source-code escrow, die over het algemeen bestaat uit de toevoeging van een een externe data back-up bij het aanleveren van de broncode en voortzetting van hosting*. Had u al eerder gehoord van 'SaaS-escrow' voor deze enquête? *Dit betekent dat de escrow-agent de financiële obligatie richting de hosting partij overneemt, welke belooft de hosting van de SaaS applicatie en data voort te zetten.* **J/N**

13. Bij een *'SaaS guarantee fund'* zet de SaaS aanbieder een stichting op met genoeg budget om de kosten voor een aantal maanden te dekken zodat de applicatie kan blijven functioneren. Hierdoor zal er tevens geen data verloren gaan en worden datalekken voorkomen. Had u al eerder gehoord van 'SaaS guarantee fund' voor deze enquête? **J/N**

14. Tenslotte heeft een gebruiker de mogelijkheid om een externe data back-up te maken. Had u al eerder gehoord van het maken van externe back-ups als continuïteitsoplossing voor deze enquête? **J/N**

15. Kent u een andere continuïteitsoplossing die hier niet genoemd is? Zo ja, welke? **Open**

16. Maakt uw organisatie gebruik van een bepaalde continuïteitsoplossing? **J/N/Weet ik niet**

17. Zo ja, van welke continuïteitsoplossing(en) maakt uw organisatie gebruik? **Checkbox**

    - Source-code escrow
    - SaaS-escrow
    - SaaS guarantee fund
    - Externe data back-up
    - Anders, namelijk:

18. Zo nee, wat denkt u dat de voornaamste redenen zijn voor uw organisatie om geen gebruik te maken van een continuïteitsoplossing? **Radiobuttons**

    - Kosten
    - Niet bewust zijn van de risico's
    - Geen continuïteitsoplossing aangeboden gekregen hebben
    - Anders, namelijk:

19. Als u de mogelijkheid had, zou u dan een continuïteitsoplossing afsluiten bij het gebruik van SaaS? **J/N**

20. Zo ja, waarom? **Checkbox**

    - De mogelijke impact is te groot om het niet te doen
    - Het is te waarschijnlijk dat er iets zal gebeuren
    - Het biedt een gevoel van zekerheid
    - Anders, namelijk:

21. Zo nee, waarom niet? **Checkbox**

    - Te hoge kosten
    - Risico te laag
    - Niet waarschijnlijk genoeg dat er iets zal gebeuren
    - Anders, namelijk:

22. Rangschik de volgende items alstublieft op volgorde van urgentie, gebaseerd op uw eigen mening. Hierbij is nummer 1 het meest urgent en nummer 5 het minst.

    - Bedrijfscontinuïteitsrisico's bij SaaS
    - Cyber security risico's
    - Natuurrampenrisico's
    - Reputatie risico's
    - Fraude

23. Hoeveel zou u bereid zijn te betalen om bedrijfscontinuïteit bij het gebruik van SaaS te garanderen? Maximaal ...% bovenop de maandelijkse prijs van de SaaS-oplossing

    - 0%
    - 1% - 4%
    - 5% - 9%
    - 10% - 15%
    - 16% - 25%
    - 26% - 50%
    - 51% - 75%
    - 76% - 100%
    - Meer dan 100%

24. Heeft u de voorkeur voor het direct verwerken van een continuïteitsoplossing in de pakketprijs van Saas of om dit als optionele service toe te voegen? **Inclusief/Optioneel**

25. Heeft deze enquête u meer bewust gemaakt van de mogelijke risico's bij het gebruik van SaaS? **J/N**

26. Bent u van plan zich te verdiepen in de mogelijke risico's en oplossingen bij het gebruik van SaaS? **J/N**

27. Wilt u nog iets kwijt over de onderwerpen die in deze enquête voorbijgekomen zijn? **Open**

28. Wilt u kans maken op een dinercheque ter waarde van 150,- euro? *Hiervoor is het verplicht dat u uw e-mailadres achterlaat. Zie vraag 30.* **J/N**

29. Wilt u de resultaten van het onderzoek ontvangen? *Hiervoor is het verplicht dat u uw e-mailadres achterlaat. Zie vraag 30.* **Open Open**

30. Zou u uw e-mailadres achter willen laten? *Dit is verplicht als u kans wilt maken op een dinercheque en/of de resultaten van het onderzoek wilt ontvangen. Er wordt vertrouwelijk met uw gegevens omgegaan.* **Open**

31. Geeft u toestemming om u.. **J/N**

    - te mogen contacteren voor eventuele vervolgvragen? **J/N**
    - te mogen benaderen met informatie over continuïteitsregelingen? **J/N**

Nogmaals bedankt voor uw deelname aan dit onderzoek. Het delen van de enquête wordt zeer op prijs gesteld. Hiervoor kunt u de social media buttons hieronder gebruiken. Mocht u nog vragen of opmerkingen hebben over het onderzoek schroom dan niet om contact op te nemen via d.r.vanvelzen@uu.nl of via LinkedIn op `https://www.linkedin.com/in/denisevanvelzen/`.

SaaS oplossing	**Toegang verliezen tot data**	**Toegang verliezen tot applicatie**	**Toegang verliezen tot support**	**Toegang verliezen tot maintenance**
ERP	*Hoog*	*Medium*	*Laag*	*Medium*

Table 11. Vormgeving van vraag 6 met voorbeeld antwoord