Eindhoven University of Technology

MASTER

SaaS security automated

Grexxboxx as continuous assurance tool

Laarhoven, B.J.A.

Award date:
2012

Link to publication

Disclaimer
This document contains a student thesis (bachelor's or master's), as authored by a student at Eindhoven University of Technology. Student theses are made available in the TU/e repository upon obtaining the required degree. The grade received is not published on the document as presented in the repository. The required complexity or quality of research of student theses may vary by program, and the required minimum study period may vary in duration.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain

Technische Universiteit
Eindhoven
University of Technology

grexx

SaaS security automated

Grexxboxx as continuous assurance tool

B.J.A. Laarhoven BSc
Eindhoven, February 2012

Supervisors:
dr. P.M.E. Van Gorp, TU/e
(S.A. Angelov PhD, TU/e)
drs. P.G.M. Hufen, Grexx
prof.dr.ir. W.M.P. van der Aalst, TU/e
dr. M. Comuzzi, TU/e

ABSTRACT

This report describes a solution to the problem that audits of the security of SaaS solutions take a long time and are outdated at the moment they are released. Using the existing auditing standards ISAE 3402 and SOC 2, we create a SaaS security framework that defines what a SaaS solution needs in order to be considered secure. To minimize the delay between the audit and its result, we integrate workflow systems into the SaaS solution to a) get a quicker and more up-to-date certainty that the auditing standards are complied with, and b) get a higher level of certainty of this compliance because the requirements are checked by an automated system instead of a human being. We prototype this solution by doing a partial integration in an existing workflow system.

PREFACE

This report concludes my master Business Information Systems in the Information Systems group of the School of Industrial Engineering in the department of Industrial Engineering & Innovation Sciences at the Eindhoven University of Technology. This research has been conducted for and at Grexx in Naarden.

I have had a very nice time at Grexx conducting this research. I could not have done this without the support of a few people. I would like to thank them here.

First of all, I would like to thank my supervisor Samuil Angelov for his very important guidance during this project. He has always given me his honest opinion, thorough feedback and has pushed me in the right directions. Because Samuil unfortunately left the university, Pieter Van Gorp took over in the last weeks of my research, giving me the last important pointers, for which I also thank him. I also want to thank Wil van der Aalst for being my second supervisor despite his very busy schedule and his very important and useful remarks. Marco Comuzzi has given me his clear view and opinion about my thesis, for which I'm also grateful.

At Grexx, I mostly have Pieter Hufen to thank. He didn't just act as my company supervisor, but he gave me the possibility to enter the magical world of Grexx. He also offered me the possibility to stay in that magical world after my graduation, an offer I eagerly accepted. Related to Grexx I also have to thank Erica Rietveld for being my first connection between the TU/e and Grexx and therefore starting this process. The magical world of Grexx can't exist without my colleagues there who have offered me a warm welcome and a very nice working environment.

At the personal level I also have to thank people. First of all my parents for all their support, my little brother for graduating a few months before me, so pushing me to graduate too. I want to mention my roommates here too, for listening to all my stories and giving me some new views on the subject. I want to mention my other friends for giving me mental support, especially Elisa and Daniël for the support during the journeys between Eindhoven and Naarden.

And last, but certainly not least, I want to thank my girlfriend Linda for her support and motivation and for accepting my periods of mental absence during my graduation period. I will probably never have the Swiss discipline, but she has brought me a little bit closer to it.

Now let's hope you all agree it was worth it.

TABLE OF CONTENTS

1 INTRODUCTION

> ***"The whole idea behind cloud computing is to go ahead and get everything on a server where the professionals are managing it.***
>
> ***[…]***
>
> ***When you put everything that is important somewhere else, keep it secure, keep it under your control, it's available to you on every demand, on every device, everywhere you are."***
>
> ***-- Eric Schmidt, CEO of Google (Schmidt, 2011)***

Cloud computing is hot. Not only email and office suites are more and more outsourced to the cloud (i.e. Gmail, Hosted Exchange, Google Docs, Office 365, etc.), but also other applications are reachable (only/mainly) by web browsers and not hosted locally anymore. Besides the many advantages like flexibility, centrally managed backup and lower maintenance costs, it also raises concerns about data security. What if these externally hosted applications have to handle customer data, which could be really privacy-sensitive? What if, for example, a hospital uses a cloud application to keep track of patient data? Who owns the information, who is responsible for physical and virtual security? Who is responsible for backups and who decides who has access to this data?

There are several standards that a company or application can comply with to give a certain level of confidence on how this company handles data security. All these standards require a high degree of custom work per company or application. Each company that wants to comply with one of these standards must follow a long process of identifying possible problems, defining solutions and policies, implementing them into the organization and more. These processes must be then followed by an audit by an official independent auditor for at least 6 consecutive months. With at most one audit per year, this also means that at least 6 months per year, a company is not actively audited and it can take up to a year for a security breach to be identified. In the current age of fast moving data, the impact of a security breach 12 months ago is big. Next to that, this long process seems inefficient as most cloud providers will suffer basically the same problems. Why can't there be a general solution for cloud providers that provides a continuous certainty that a proven standard has been met? And why don't we use computers where possible to give a quicker, more up-to-date and more accurate verdict about the data safety?

In this research, we will try to make a step towards developing this solution. The rise of cloud computing changes the way we should address security and privacy. It also changes the way we should consider risks, controls and audits on those areas.

1.1 PROBLEM CONTEXT

In this section we will introduce the terminology and concepts that are needed to understand the rest of the report. First of all it's necessary to make clear what the "cloud" is in this context. Next we will introduce the standards that currently exist to audit these cloud solutions. As Grexx is the company where this research is executed, we will give an overview of the company and why they are involved in this research topic.

1.1.1 THE CLOUD

The cloud is used as a term to indicate a network of computer resources (hardware, virtualized hardware, middleware, software services), managed by others. Cloud-based services can be divided into three groups: IaaS, PaaS and SaaS.

A company delivers IaaS (Infrastructure as a Service) when it delivers infrastructure to its customers, but not including any software or even an OS. Of course the provider can deliver the OS or install an initial version, but the customer is responsible for keeping it up to date. The customer has no worries though about hardware maintenance, electrical power supply, network maintenance etc. Examples are Amazon's Elastic Compute Cloud[1] and every dedicated server provider like Rackspace[2].

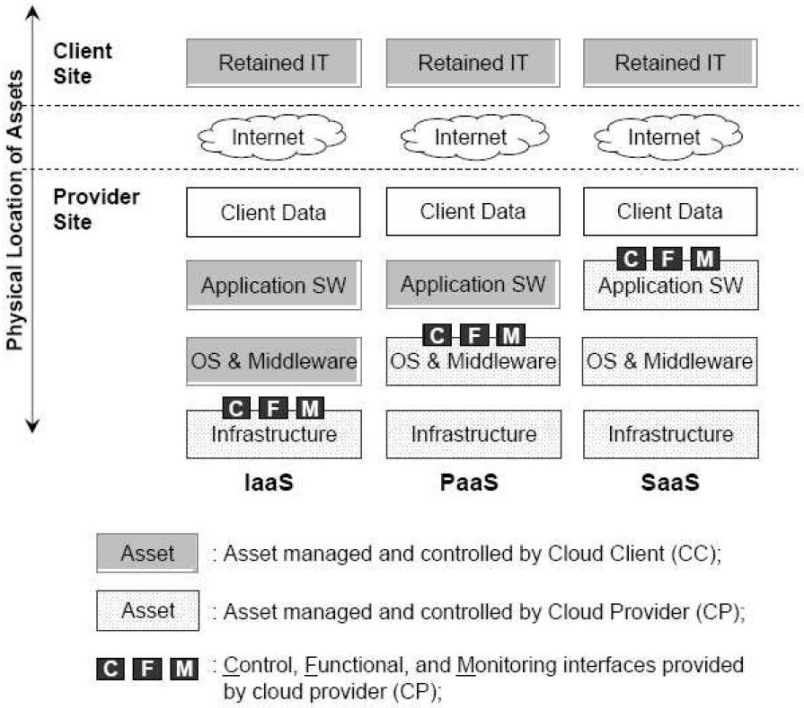


FIGURE 1: IAAS, PAAS, SAAS. SOURCE: (JULISCH, ET AL., 2010)

A company that delivers PaaS (Platform as a Service) also takes care of the maintenance of the OS and a platform to develop applications on/for. For example, a company that provides an instance of SQL Server, but also Facebook that delivers a platform[3] where third parties can develop applications for.

The third version of cloud-based services, which is the one most people think of when the cloud is mentioned, is SaaS (Software as a Service). In this version, the cloud provider takes care of almost anything; all the end user usually needs is a web browser. The SaaS provider takes care of infrastructure, platform ánd develops/delivers application software over the internet to the end users.

An organization that delivers (and maybe also develops) SaaS services is called a Service Organization[4]. The Service Organization delivers the service to the User Organization and is therefore often handling confidential data of the User Organization and its clients. The Service Organization is the organization that would like the security label.

When we talk about security of cloud solutions, a form of inclusion applies. The criteria applicable to PaaS providers (e.g. "Make sure access to the Operating System is only granted to authorized people") also applies to SaaS providers. It could be that the SaaS provider doesn't manage the OS layer himselve, but to convince someone that the SaaS solution is secure, the provider still needs to make sure that the security in the OS layer is well managed. IaaS providers on the other hand, have nothing to do with operating system authorization and these criteria don't apply to them. The same form of inclusion is valid in a lower level, where the control and monitoring of the infrastructure is also needed in case of a PaaS or SaaS solution. If shown graphically, Figure 1 could be extended with extra C, F and M blocks at all the white assets. These extra C, F and M blocks are then not offered to the Cloud Client though, but have to be present at the Cloud Provider's side to be able to maintain security. Therefore it can be concluded that the broadest form of "cloud security" is SaaS security. Because of that, from now on we will focus on SaaS and the security

[1] http://aws.amazon.com/ec2/
[2] http://www.rackspace.com/cloud/
[3] http://developers.facebook.com/
[4] "Service Organization" has a broader meaning, but for the sake of this report I will use this one. Same for "User Organization"

of SaaS solutions. This has the advantage that SaaS is the best known type of cloud solutions, which makes it easier to give real life examples and find documentation.

Why is SaaS so hot at the moment? Some good examples of widely used SaaS environments are Google's Gmail[5] and Google Apps[6], Microsoft's Office 365[7], etc. The advantage to the end users is quite obvious: they don't have to worry about server management nor software management; the browser is enough to access the SaaS solution. Payment for the service is usually calculated based on usage (per user, per GB storage capacity, etc.)

The SaaS provider has to take care of the infrastructure and the platform (or outsource that to an IaaS resp. PaaS provider), so there is no need for expensive server management people at the customer side anymore. Neither does the customer need people with any knowledge of server software anymore. And a big advantage is also that usually the SaaS provider takes care of backups, updates of the software, security patches, data traffic, etc.

The provider, on the other hand, also has some benefits. It doesn't have to "physically" sell its software and install it in the weirdest locations or on servers that it has never seen before. The provider can keep that all into its own hands. The provider can also easily "force" updates to customers by just updating the software server-side. And the cost of resources can be kept low as usually several customers fit onto one server. Sudden peak loads of one customer can be compensated by low loads at another customer and vice versa.

One of the few disadvantages of SaaS has been mentioned in the introduction, though. The customer has to put its sensitive data onto the servers of the provider. This provider then shares this server with other customers. How can the customer ever be sure that its data is secure and that other customers on the same server can't access it, for example? Remember that the SaaS provider, to convince the customer of the security of the customer's data, has to provide security on application level, on platform (OS/middleware) level and on infrastructure level.

1.1.2 STANDARDS

	SAS 70	ISAE 3402	SSAE 16	ISO 27001	SOC 2
Goal	Financial audits	Financial audits	Financial audits	Information security management systems	Security, Availability, Processing Integrity, Confidentiality or Privacy
Effective since	April 1992	June 2011	June 2011	November 2005	July 2011
Written by	AICPA	IAASB	AICPA	ISO	AICPA
Type I/II	Yes	Yes	Yes	No	Yes
Target market	USA	International	USA	International	USA
Carve-out	Yes	Yes	Yes	No	Yes

TABLE 1: OVERVIEW OF AUDITING STANDARDS

As an answer to the concerns about the safety of the data, SAS 70 was widely used for a long time. SAS 70 originally was intended for "service organizations" in a meaning dated April 1992, when SAS 70 was developed, and mainly focused on financial auditing and financial risks. Service organizations were organizations that had to handle sensitive data from its customers, but in that time they could never foresee the size that the internet has now and the role SaaS plays in the current IT environments. Nevertheless, as no other (better) standard was available, SAS 70 was used for years to audit SaaS environments.

[5] http://www.gmail.com/
[6] http://www.google.com/apps/
[7] http://www.office365.com/

The compared standard's reports usually come in two flavors: type I and type II. The type I contains the service organization's description of controls[8] and an opinion of an independent service auditor on those controls. A type II report also contains an auditor's opinion on the operating effectiveness, which means that the service organization is audited over a period of at least 6 months and the auditor gives an opinion about the effectiveness of the controls during this audit. In essence, in a type I report, the auditor states whether he thinks the controls are complete, functional, feasible and applicable, whereas he in a type II report also gives an opinion about the effectiveness of the controls over a period of a few months.

Two new standards have been developed (SSAE 16 and ISAE 3402) to replace SAS 70. ISAE 3402 was developed by the International Auditing and Assurance Standards Board (IAASB) and is the international successor of SAS 70. SSAE 16 is based on ISAE 3402 but specifically aimed at the North-American laws and market. The differences between these two are very small and only concerning American law. These standards still focus on the financial controls and are meant to be used for financial audits. Nevertheless, as they are replacing SAS 70, the companies that currently audit/validate their cloud services using SAS 70 will probably continue validating it with one of these new standards.

Another standard that is found in literature about this topic is ISO 27001. This is a certification standard for information security management systems. A certification standard differs from the previously mentioned standards as the certification standard gives strict rules to which a product should comply. In the other mentioned standards, the organization can define its own rules and then has to apply to them. When all the rules (or a representative subset) are applied and considered compliant, a certification can be given to the product. Information security management systems can therefore have the label "ISO 27001 compliant" which means it complies to the rules mentioned in this standard. Unfortunately for this research, ISO 27001 is not focused on cloud security (yet). The standard explicitly states that exclusion of any of the given policies is not allowed, unless very clearly motivated. This will allow cloud providers to get an ISO 27001 certification when necessary, but does not make it easy. The absence of the carve-out method or something alike also shows that this standard is based merely on internal security systems in regular organizations than on the security systems in service organizations like cloud providers.

The last standard we will consider in our report is SOC (Service Organization Controls) 2. This is a completely new standard, developed in 2011, focusing on other aspects than the financial one, being security, confidentiality, processing integrity, availability and privacy. This focuses more on the subjects that cloud computing environments are prone to be insecure for, and is therefore a more applicable solution to the problem stated in the introduction. As it is a completely new standard though, not based on an existing standard like SAS 70, it has to be researched whether this completely covers all aspects of SaaS solution providers' security issues.

Most standards mentioned in this subchapter support the carve-out method. This method supports relaying the responsibility of certain constrains to another party. If a SaaS provider outsources its platform maintenance to a PaaS provider, testing "network redundancy" would involve mainly the business of the PaaS provider. If the PaaS provider has proven compliance to the same standard already, the SaaS provider can skip the chapter on "network redundancy" using the carve-out method. This can be done with all relevant control objectives and related controls, under the following conditions:

- The system description by the SaaS provider identifies the nature of the services performed by the PaaS provider, that are excluded from the report, and
- The SaaS provider's report does include the SaaS provider's controls that monitor the effectiveness of the PaaS provider's policies.

Of course the terms "SaaS provider" and "PaaS provider" can be replaced with other parties, as long as the first outsources certain services to the second and these services are relevant to the (security) standard.

[8] A control is *a means of regulation or restraint* (Farlex, 2011) or *a means of limiting or regulating something* (OED, 2011)

1.1.3 GREXX

Grexx is a Dutch company based in Naarden. Grexx supports companies becoming more efficient and more organized by delivering workflow management services on its own SaaS platform: the Grexxboxx. The Grexxboxx is used by several (large) customers all over the Netherlands, like KPN, KLM, sanofi-aventis and others. The core of the Grexxboxx itself (basically an Apache Tomcat server with some Java Server Pages (JSP) and a Microsoft SQL Server with custom-built stored procedures) can be considered a platform-as-a-service. On this platform, Grexx' own developers build applications as designed and requested by the customers. This application is then offered to the customer in the form of a SaaS solution. These SaaS solutions are also called "Grexxboxx" and for the rest of the report, a "Grexxboxx" is actually an "application built on the Grexxboxx platform".

Competitors of Grexx and the Grexxboxx are comparable services like Cordys Business Operations Platform[10], Siebel CRM[11], SAP[12] etcetera. Grexx has chosen to handle the platform and the service layer itself, therefore being a SaaS provider outsourcing the interface to an IaaS provider. Because of the costs aspect and some legacy reasons, Grexx is not using flexible IaaS solutions like Amazon's Elastic Compute Cloud[13], but uses ordinary dedicated servers and dedicated virtual servers which are not easily scalable. The current hosting provider of Grexx is SaaSplaza, based in Amstelveen, the Netherlands. SaaSplaza explicitly aims at SaaS providers and therefore also understands and acknowledges the importance of a decent security policy. SaaSplaza has been SAS 70, type II compliant since 2006 and gets audited every year since then.

Grexx takes care of all the aspects of the Grexxboxx. This involves:

- Development of the software: implementing new features, resolving bugs, releasing new versions;
- Rolling out these new versions to the customers' instances and keeping these instances up to date;
- Installing new instances for customers;
- Maintaining the hardware (servers) and software (OS, database, web server) the Grexxboxxes run on;
- Consultancy for deploying new instances of the Grexxboxx for customers;
- Consultancy for updating customers' instances of the Grexxboxx;
- Incident management for existing customers.

As Grexx takes care of all of these aspects, it is practical to divide these tasks (and therefore Grexx itself) into three different "subcompanies":

Grexx continuous operation	Grexx consultancy	Grexx internal
All tasks that involve the continuous operation of the Grexxboxxes for customers, this involves mainly: • Incident management • Problem management • Deployment of new instances • Deployment of new versions for existing instances	All tasks that involve project-based tasks for customers, which mainly includes all consultancy work.	All tasks that involve internal tasks, not directly related to customers: • Software development • Server and software management

TABLE 2: OVERVIEW OF GREXX STRUCTURE

The Grexxboxx can be best described as a **dynamic case-oriented software-as-a-service workflow management platform**. This description contains several terms, explained and justified below:

[10] http://www.cordys.com/cordyscms_com/business_operations_platform.php
[11] http://www.oracle.com/us/products/applications/siebel/index.html
[12] http://www.sap.com/
[13] http://aws.amazon.com/ec2/

- Grexxboxx is a tool that supports processes in companies that are constructed from tasks. These tasks are executed by employees but it's not necessary that all tasks in one process are executed by the same employee. Handling and supporting these processes is called workflow management.
- Grexxboxx is offered as a 100% SaaS (software-as-a-service) application; all the user needs is a web browser.
- All the Grexxboxxes can cooperate and communicate together. They're all built on the same system, with each a different implementation, therefore it's not so much a "system" as well as a "platform".
- The core elements of the Grexxboxxes are cases. Where a standard BPM platform pushes its "tokens" through a pre-defined path of tasks, cases are more flexible. Tasks can be applied to cases, or not. Cases can be transferred into completely different processes (even in a totally different Grexxboxx).
- Finally, the Grexxboxx is also called dynamic as the path of tasks that cases travel through, is dynamic. Certain tasks can be optional and certain required tasks can be executed in arbitrary order. Task order can change based on time, user interaction, case data, etc. (Le Clair, et al., 2011)

A more complete overview of the Grexxboxx can be found in (van Roy, 2010) and will be elaborated on in a later chapter.

Each Grexxboxx is a SaaS application. It is used by quite large companies in the Netherlands. These companies often enter privacy-sensitive (customer) data into the Grexxboxx. When they run a BPM solution or workflow management solution on their own servers, locally, they are responsible for the protection of that data themselves and can keep all security management in-house. In the case of a SaaS application, though, these companies have no control over that anymore.

That is where compliance to a security standard can be useful for Grexx' customers, because proven compliance with such a standard implies that the sensitive data is safe and that Grexx has created and applied policies to ensure a certain level of data security.

Next to the appliance of the security standard to Grexx itself, Grexx would also like to provide customers with a product that can ensure security standard compliance of these customers' processes. If Grexx has implemented the security processes for itself already, the advantages of the Grexxboxx platform will pay, as it then leaves just a small step to implement these processes, maybe slightly modified, for the customers. These customers can then also reach the standard's compliance easily using the Grexxboxx.

Grexx is not primarily responsible for all hardware and software maintenance as it has outsourced the interface layer. SaaSplaza is responsible for all hardware maintenance, but Grexx has implemented some own hardware monitoring. SaaSplaza also maintains software, on request. Grexx has Administrator access to all (virtual) server nodes too, so Grexx can do basic software maintenance tasks too.

Given the terminology of the previous subchapter, Grexx is a Service Organization, although it also is a User Organization. Grexx uses the services of its hosting provider SaaSplaza. In that relation, Grexx is the User Organization and the hosting provider is Service Provider. Concerning offering the Grexxboxx solution to customers, Grexx is a Service Organization and the customers are User Organizations. Another level deeper, Grexx' customers could use the Grexxboxx services to offer services to their own customers. This means that Grexx' customers are potential Service Organizations too. If that happens, Grexx' customers could have the same need for standards' compliance.

The carve-out method can be applied on several relations here. First of all, Grexx can use the carve-out method on services of SaaSplaza. Because of the implemented hardware monitoring by Grexx, the second aspect of the carve-out method is met. Grexx' customers can use the carve-out method on the Grexxboxx services. The customers of Grexx' customers can use the carve-out method on the services delivered using the Grexxboxx services. We will only consider the first carve-out method here as the others are highly dependent on the customers' needs. Luckily, SaaSplaza already has proven SAS 70 compliance.

1.2 Report Structure

The report is built up in a straightforward manner. After the first introduction of terminology and defining the context of our research, which is done in this chapter, we will explain what the problem is faced during this research. This leads to research questions that then lead to a research approach. All this can be found in chapter 2. Chapter 3 contains a literature study and leads to chapter 4, which contains a SaaS security framework, based both on literature as well as on experience from practice. The result of chapter 4 is the answer to the first research question. The second and third research questions are answered in chapter 5, which explains what is needed to develop or find a software tool that applies the framework from chapter 4 to a SaaS solution. Chapter 6 applies the results from chapter 5 to the Grexxboxx platform, to answer the fourth research question. Research question 5, the validation, is answered in the last subchapter of chapters 4, 5 and 6. This way the validation is directly linked to the achieved results. In chapter 7, we will summarize the results and the answers to the research questions and give a conclusion and discussion.

2 RESEARCH DESCRIPTION

In this chapter we explain the research subject and our motivation for choosing this subject. In 2.1 we define the problem we faced and form that into the main research questions. In 2.2 we explain and outline the approach we have followed when executing this research. In 2.3 we explain why we limited ourselves to not cover the complete spectrum of possible topics and solutions and where we did that.

2.1 PROBLEM DEFINITION AND RESEARCH QUESTIONS

Security of SaaS solutions has been given little attention where the usage of SaaS solutions increases. The growth of cloud-based solutions (mostly SaaS solutions) has been very high over the past years. The first SaaS solutions that got a big market were mostly aimed at the Business to Consumer market. A good example of these solutions is Gmail by Google, but also social networks like Facebook. Once the Business to Consumer market for SaaS started growing, also companies started to see the benefits of these solutions. The more companies start using these solutions, the more often the request for security arises. There is no literature-founded framework that describes requirements for a SaaS solution to be considered "secure". Next to that, security requires external and independent audits. With the movement towards SaaS and the cloud, users of these solutions get used to being able to connect and use their system 24/7. This is possible, as the systems are available over the internet and online all the time. As people start to get used to being able to continuously access data and information, the need for a continuous stream of up-to-date information grows too. When applying this to the SaaS security, it makes sense that a customer of a SaaS provider is not satisfied anymore with an audit report of over 6 months ago. It wants to know whether the SaaS solution is safe right now and how it behaved the past few days, weeks or months. With the regular auditing methods and plannings, this is not possible. Therefore, the SaaS security should, ideally, be checked continuously. Grexx as a company is active and innovating at the SaaS area. Its Grexxboxx is a PaaS solution offering SaaS solutions to its customers. Grexx would like the Grexxboxx to be a tool that can continuously check for SaaS security on itself, and on other SaaS solutions.

The problem faced in this thesis can therefore be summarized as:

With the quickly growing use of SaaS solutions, regular auditing techniques don't suffice anymore. Assuring the security of the SaaS solution takes months using the existing standards and the resulting report is based on old data. There should be a way to give a more fast and up-to-date assurance of the security of SaaS solutions. Using a software tool is one of the ways to do this. Grexx wants to know whether it is possible to achieve this using a software tool and if so, whether the Grexxboxx can be used to do that.

This results in the following research questions

1. What is needed for a SaaS solution to be secure?
2. What requirements should be met by a software tool to ensure a SaaS solution's security?
3. Are these requirements feasible? In other words: is such a tool buildable?
4. Is it possible to use the Grexxboxx as such a tool?

2.2 RESEARCH APPROACH

To answer the 4 research questions, we have defined an approach to get to the answers. Next to answering these questions, they all also need to be validated. How this validation occurs is also defined in this section.

The first research question is answered by studying literature, studying examples from practice and studying and explaining the current standards that are applicable. This delivers a **SaaS Security Framework** that consists of a list of requirements a SaaS solution has to meet to be considered secure. To develop this framework, we create a basis based on literature and history, i.e. existing standards like SAS 70 or its successors like ISAE 3402. Also experiences from practice are used to develop the draft framework. Once we created a draft framework based on those sources, we can improve the framework by comparing it to the newer, but less tested standard SOC 2.

Validation: The draft framework based on ISAE 3402 can be validated when comparing it to SOC 2. As the SOC 2 list has the same goal as our draft framework, can be considered an authority and is not created by us, we can use it as validation for our draft framework.

This framework is then the basis to answer the second research question. For this, we walk through the framework and define for each item or requirement what is needed to automate this. Automation can vary from complete automation of a requirement to supporting the requirement in a workflow system. By supporting it in a workflow system, it can be ensured that the requirement is met by checking whether the task was completed in time and correctly, for example. The necessary properties of the software tool to automate the security checking are collected, deduplicated and turn into a list: the **SaaS Security Automation Requirements**.

Validation: This list can be validated by creating a software tool that completely (and only) has the requirements of the SaaS Security Automation Requirements list. This tool should then be used to implement the automation of the SaaS Security Framework and it should be checked whether each item can be implemented with just these requirements. As this goes beyond the scope of this research, it is validated in the answering of question 4, where the Grexxboxx is used to prototype the automation tool. The Grexxboxx is checked in the answering of question 4 for compliance with the SaaS Security Automation Requirements, which makes it a valid tool for validating this question.

The third question requires checking the SaaS Security Automation Requirements for buildability. This answers the first part of the question of Grexx in the problem description: whether it is at all possible to build a tool that can ensure a SaaS solution's safety. For this, it needs to be checked whether all the SaaS Security Automation Requirements from question 2 are buildable.

Validation: This can be validated by effectively building it, but this also goes beyond the scope of this research. Therefore, the validation will be performed in the answering of question 4 again, where the Grexxboxx is used to build a prototype.

The fourth question answers the second part of the question of Grexx: whether the Grexxboxx can ensure a SaaS solution's safety. For this, in theory we just need to check the Grexxboxx's compliance with the SaaS Security Automation Requirements from question 2. To prove this to more depth, we implement a part of the SaaS Security Framework which delivers a partial prototype of the final tool.

Validation: This implementation forms the validation of the basic checking whether the Grexxboxx complies with the SaaS Security Automation Requirements.

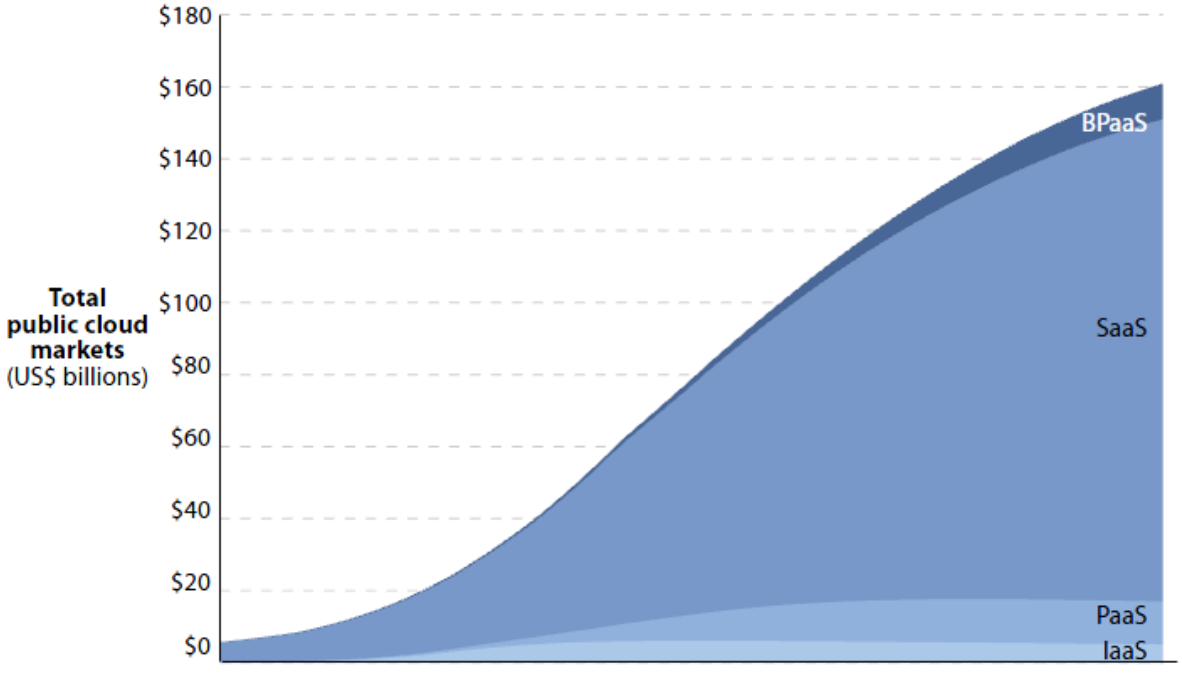
2.3 RESEARCH FOCUS

Given the amount of time available, we have made some decisions to limit (or focus) my research. First of all, we focus on the security of SaaS providers and its SaaS solutions and not the complete cloud spectrum. We have chosen this focus because SaaS is the most common form of cloud computing (See Figure 3: SaaS, PaaS and IaaS Market shares according to Forrester and (Dignan, 2011)), SaaS is the cloud computing that Grexx uses, and most of the known "cloud computing" environments are SaaS-based. Next, we decided to focus on the new standards, mainly ISAE 3402 and SOC 2. SAS 70 is outdated but it's very known, widely used and carved into auditors minds, so we will have to cover it partially. The differences between ISAE 3402 and SSAE 16 are minimal, so we will exclude SSAE 16 from deep research. The SSAE 16 variant is the US variant, where ISAE 3402 is for international markets. ISO 27001 is a different type of certification, which can't cope with all the requirements we are looking for as it is aimed at non-cloud environment and is not meant for service organizations but rather for regular organizations. Therefore, ISAE 3402 and SOC 2 will be the main focus standards in this report. ISAE 3402 is the international standard which is the most logical alternative for a Dutch company to try to live up to. On the other hand, SOC 2 has been launched specifically for the types of controls that cloud solutions need explicitly, so I will compare these standards and try to get the best of both worlds.

As the last point of focus, we will not develop a completely functional security checking Grexxboxx application, as that will take too much time for this project. We will pick a typical process to show the possibilities of the Grexxboxx. By implementing this process, we can deduct whether the complete compliance to a standard (or multiple standards) is possible.

Figure 3 Forecast: Global Public Cloud Market Size, 2011 To 2020

The spreadsheet detailing this forecast is available online.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BPaaS ($)	0.15	0.23	0.35	0.53	0.80	1.26	1.95	2.93	4.28	6.00	7.66	9.08	10.02
SaaS ($)	5.56	8.09	13.40	21.21	33.09	47.22	63.19	78.43	92.75	105.49	116.39	125.52	132.57
PaaS ($)	0.05	0.12	0.31	0.82	2.08	4.38	7.39	9.80	11.26	11.94	12.15	12.10	11.91
IaaS ($)	0.06	0.24	1.02	2.94	4.99	5.75	5.89	5.82	5.65	5.45	5.23	5.01	4.78

58161 Source: Forrester Research, Inc.

FIGURE 3: SAAS, PAAS AND IAAS MARKET SHARES ACCORDING TO FORRESTER

3 LITERATURE

In this chapter, we will cover literature on a number of topics relevant to this research. First of all, the general topic of cloud computing is addressed. There is a lot of literature on this as it is a general topic that generates a lot of attention. For this research, it is not necessary to cover the complete topic of cloud computing, just the security aspects are relevant (and the origins of these aspects). we will therefore not cover the entire topic of cloud computing, but just the parts related to security aspects.

After that, we will try to cover some of the standards mentioned in the research description. SAS 70 is quite an old standard and covered by quite some literature. SAS 70 is the predecessor of the standards we are really researching here and the reason we are looking at different standards is that SAS 70 did not suffice for security in cloud computing. On the other hand, concerning the new standards there is hardly any literature to be found yet. These standards are too new at this moment to be already covered in this report. The standards are not a result of scientific research and do not mention any other standards or frameworks they are based on. Therefore scientific literature is hard to find at the moment. Probably, a year or two later, literature on this subject will be more available.

The sources we therefore are forced to use now (for these standards) are not academic sources, but rather (high-valued) sources from the business itself. This ranges from whitepapers to quite extensive and thorough analyses of the standards. While reading the sources, it showed that they contained too important and interesting information to not use it in this report, even though this did not appear in journals (yet) and are not considered academic sources.

This literature chapter ends with an extensive subchapter about continuous assurance. This is the methodology used to move from a periodic audit/assurance towards a continuous one. As we want to implement the audit of the new standard in a continuous way, this is an important issue.

3.1 CLOUD COMPUTING

Cloud computing is not a new technology, even though it is sometimes marketed as such. Cloud computing is merely a new approach of delivering resources. This approach brings a number of advantages, like: (Julisch, et al., 2010) and (Cloud Security Alliance, 2009)

- Low cost: Businesses spend a lot of money on system maintenance tasks. This overhead can be reduced by using cloud services. The cloud provider uses the economy of scale by doing the system maintenance combined for many customers at the same time and is therefore cheaper for its customers than when they would have to do the maintenance themselves. Next to that, the cloud providers are usually better equipped to handle possible errors and downtime.
- On-demand: Cloud services can usually be set up very flexibly as the resources (memory usage; disk space; number of users; etc.) can be scaled on demand. This also means that a customer only has to pay for what he really uses which can be a very attractive pricing model.
- Short time-to-market: Cloud services are already developed, tested and implemented for other customers. Therefore the time-to-market will usually be a lot lower than when the same functionality is developed in-house.
- Collaboration: It is generally easier to collaborate using cloud services as everyone, everywhere can reach the same resources as long as an internet connection is available and the necessary authentication is provided.

On the other hand, it also brings a number of disadvantages, such as: (Julisch, et al., 2010)

- Security: Cloud providers are responsible for most of the security controls, especially (but not only) the physical security. How to ensure that the sensitive customer data is safe and stays safe?
- Continuity: How to handle downtime? Who is responsible and when/how can they be reached?
- Reliability: What if connections get slow or data seems to go missing?

- Vendor lock-in: If new functionality or a new system has to be built, how dependent are cloud customers then to their current providers? Is it possible to choose another provider/company and will everything then still be compatible?
- Migration: To move from an existing (local, custom-made) system towards a cloud based solution brings migration costs that do not need to be paid when the company stays with its own (non-cloud) system.
- Integration: Integrating a cloud-based solution with other systems inside a company (cloud-based or not) takes extra effort.
- Legal implications: What are the legal consequences of outsourcing processes to an external party somewhere in the world?

It can be argued that most of these disadvantages are also true for regular, non-cloud software. This is true to a certain level. Except the legal implications, all the above mentioned disadvantages are also big issues when a new regular software product is rolled out in an organization. The vast difference with cloud solutions though, is the dependence for all of these issues on the cloud provider, which is an external party. This brings an extra level of complexity. Not only do agreements have to be made and should these topics be discussed, a company using a cloud solution always has to balance between the responsibility it has to its own users/customers and the responsibility it outsources (on the matter of these disadvantages) to its cloud provider. Therefore, these disadvantages can be considered as the disadvantages of cloud computing, even though they might also exist in other approaches.

It can also be argued that these most of these topics are not disadvantages but advantages; security, reliability, continuity: it's all taken care of. And because of the scale of cloud solutions, migration issues and integration issues are no problem either as the cloud provider probably has developed a solution to connect with other systems already. It could save a company a lot of work to use a cloud solution because all of these issues are taken care of already. That is true, but it is usually based on trust. Trust that the cloud provider that claims that its data is secure also really checks that, trust that the cloud provider will update its ports to other applications when these other applications get big version updates, trust that the cloud provider is capable of handling big downtime events. The issue in this research is to get a validated, academic verdict on whether the cloud provider indeed does all these things. Trust is usually seen as something non-academic and giving a verdict using a structural and validated approach will take away the need of trust when it considers these issues. Once the security, reliability and other disadvantages mentioned above are proven to be taken care of, the compliance to the framework developed in this research can be considered an advantage that washes away most of these disadvantages.

Another big difference with "regular software" is that ad-hoc solutions are more complicated. (van der Aalst, 2011) Where in regular installations of, for example, SAP, an ad-hoc solution can be created for a process not supported by SAP by default, this is not that easy in cloud environments. Cloud environments make use of "multi-tenant" environments, which means that multiple customers typically use the same hardware and software. This implies that an ad-hoc solution usually involves updates for all customers of a cloud solution. It is possible, technically, to create ad-hoc solutions for one specific customer, but that involves that all the areas where the cloud provider gets its economy of scale, it loses that for this customer. For example, when the SaaS software is updated, the cloud provider has to check manually whether the ad-hoc solutions for all his customers are still valid. This removes the scale advantage he had because he could just roll out his new SaaS software solution to all customers automatically. Although that could be seen as a disadvantage, it can also be seen as an advantage. This way, the software has to be developed in such a way that customizations are possible without the need for an ad-hoc solution. A well-implemented multi-tenant environment, as defined by Van der Aalst, allows for ad-hoc solutions up to a certain level. A certain basis of infrastructure and functionality is shared and cannot be changed, but on top of that, the "tenants" are able to define their own processes and configuration details, thus allowing ad-hoc solutions as long as they fit in the basic infrastructure and functionality.

3.2 SARBANES-OXLEY AND SAS 70

The Sarbanes-Oxley (SOx) law, introduced in 2002, was a result of a few big scandals (WorldCom, Enron) to provide legislation on internal and external audits. (Gaskin, 2009) This resulted in a higher demand for some standard to perform the audits and SAS 70 was chosen often. SAS 70 is originally meant for assurance on financial controls (Wiegand, Jr., 2010), but other types of service organizations started to use SAS 70 too as a competitive advantage. (Gaskin, 2010) As for example cloud solution providers might have big companies as a client that require assurance on their financial controls. As they are dependent on the cloud solution provider, it is a competitive advantage to get a SAS 70 report as a provider, even though you're not looking for financial assurance. That resulted in SAS 70 as a kind of "quality seal" for service-oriented IT companies. (Verweij, 2009) As that's not what SAS 70 was meant for, some new standards were born.

3.3 ISAE 3402

As SAS 70 is getting old-fashioned, a new standard had to be born. Also because of the Sarbanes-Oxley act, a new standard was necessary to judge service organizations. Where the SAS 70 standard had been developed by the American Institute of Certified Public Accountants (AICPA), ISAE 3402 (International Standard on Assurance Engagements No. 3402, Assurance Reports on Controls at a Service Organization) (International Auditing and Assurance Standards Board (IAASB), 2011) has been developed by the International Auditing and Assurance Standards Board (IAASB). This means that the ISAE 3402 standard is an international one rather than an American one. It differs on a few areas from SAS 70:

- First of all, SAS 70 is an audit standard, where ISAE 3402 is an attestation standard. Both imply that an external auditor confirms that certain facts/observations/controls are correct, but an "audit" is more based on the opinion of the auditor whereas an "attest" is mostly based on a statement of compliance by the management. The auditor just tests whether it's true what the management says.
- Secondly, ISAE 3402 does not just concern "controls", like in SAS 70, but in ISAE 3402 the complete "system" has to be described. This probably includes all controls, perhaps written down differently, but it includes more as the "system" also concerns more than just the controls.
- The third big difference is that ISAE 3402 includes a written assertion from management that states that the description of the system fairly represents the system, that the control objectives were suitably designed and operating effectively during the period under audit. Management also has to assert that the criteria for making these assertions were in place and were consistently applied.

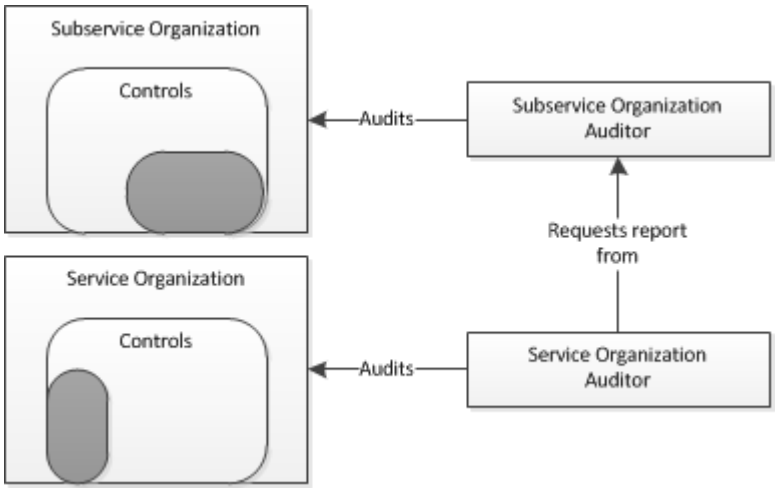
There are more differences between SAS 70 and ISAE 3402, but these are the biggest differences. (Wiegand, Jr., 2010) (Gaskin, 2010)

To make the roles in the auditing process clear, (Knolmayer, et al.) mentions the terms *user entity*, *user auditor*, *service organization* and *service auditor*. First of all: the user auditor audits the user entity and the service auditor audits the service organization. The user entity uses services provided by the service organization (for example a SaaS environment). The user entity is the primary organization that has the wish to be audited, as the user entity is primarily responsible for certain consequences (privacy issues etc.). Because the user entity uses services provided by the service organization, certain controls cannot be assured at the user entity. In usual cases, the user auditor then goes to the service organization and audits the necessary controls on behalf of the user entity. This works, but it can get frustrating, annoying and a lot of extra work when the service organization has multiple customers seeking for this compliance. Here the service auditor comes in sight. If the service auditor audits the service organization and delivers a decent report based on a proven standard that guarantees that the service organization adheres to the applicable controls, the user auditor's job gets easier. He doesn't have to go to the service organization anymore, but can instead read the report of another auditor and pick the necessary controls to ensure compliance of the user entity. Next to this advantage to the user auditor and user entity, the service organization is also guaranteed to be compliant, has thought things through and can market itself as an ISAE 3402 compliant service organization, for example.

This not only gives a competitive advantage to the service organization, but also makes the audit of the user entity easier. The user auditor can now use the report of the service auditor using the so called “carve-out method”, which is defined as follows:

> ***Method of dealing with the services provided by a subservice organization, whereby the service organization’s description of its system includes the nature of the services provided by a subservice organization, but that subservice organization’s relevant control objectives and related controls are excluded from the service organization’s description of its system and from the scope of the service auditor’s engagement. The service organization’s description of its system and the scope of the service auditor’s engagement include controls at the service organization to monitor the effectiveness of controls at the subservice organization, which may include the service organization’s review of an assurance report on controls at the subservice organization. (International Auditing and Assurance Standards Board (IAASB), 2011)***

In a more graphical manner, this can be displayed as follows:



Both the service organization and the subservice organization have its own security controls. A part of the security controls of the service organization do not fall under the responsibility of this service organization, though. In cloud-environments a simplified example of this is “access to the data center is restricted”. Most SaaS providers don’t own a data center but just rent a platform or a (virtual) server from a PaaS/IaaS provider. Therefore, access to the data center falls under the responsibility of the SaaS provider’s provider. The darker grey areas depict these controls. The auditor of the service organization (in this case the SaaS provider) notices that these controls are outsourced. To give a decent opinion and verdict, the service organization’s auditor needs to know whether these controls are taken care of. This auditor then contacts the auditor of the subservice organization (in this case the PaaS/IaaS provider) to request its report/verdict on the controls of the subservice organization that are relevant to the service organization. When the service organization’s auditor considers the outsourced controls to be covered by the subservice audit, the dark grey area in the service organization’s controls is covered as well, therefore allowing a positive verdict on the complete control set of the service organization.

An ISAE 3402 report requires a few aspects to be covered. First of all, the report should give a description of the complete system under audit. This includes (but not only) the controls that are the main subject of the audit. The management has to give an assertion that it complies to the controls, that the description of the system is accurate,

that it has given all information and openness to the accountant where needed and that it has voluntarily given all information about possible rule-breaking activities (fraud, failed controls, etc.). All this can still be done by the organization itself.

After the organization has done this first part of the auditing process, the auditor starts the next part. It depends on the type of report what his actions are. If it concerns a “type I” report, the auditor only checks whether the system description matches the reality and whether the given controls are implemented as promised. In case of a “type II” report, the auditor conducts an audit for at least 6 months in which he not only checks for the requirements of the “type I” report, but also whether the controls operated effectively during the period under review. (Knolmayer, et al.)

The possible use of this standard is discussed heavily though. Opponents argue that the ISAE 3402 standard has become more “auditor-friendly” (Knolmayer, et al.) in the way that the auditor can just rely on the management’s assertion instead of really auditing the controls. This means that the controls are not that strictly checked anymore which could result in less trustworthy results. Also, there does not exist a decent set of required objectives or controls. The organization is just required to have controls defined and the efficiency of these controls are (in a type II report) tested. This does not imply though that the controls cover all problematic areas. It doesn’t imply either that the controls are well-formulated nor well-chosen.

3.4 SSAE 16

SSAE 16 (Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization) is the American version of ISAE 3402. It has been developed and finalized by the AICPA and replaced SAS 70 effective June 15, 2011.

The differences between SSAE 16 and the aforementioned ISAE 3402 are very small. They can be found in Exhibit B of (American Institute of Certified Public Accountants, 2010) but are irrelevant for this research.

3.5 ISO 27001

ISO 27001 (“ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements”) (NEN, 2005) is a standard to describe an information security management system needed to ensure a high level of information security.

It is a standard that does not aim for a successful audit rather than a real certification. It describes, concretely and precisely, the requirements for an information security management system (ISMS). An ISMS is a part of a management system that focuses on all the aspects of information security. An organization that has an ISO 27001 certification has (as has been assured by an external independent auditor) an ISMS in place that complies with the specific requirements.

The downside of ISO 27001 is that it is not tailored for cloud environments. Requirements A.6.2.1 and A.6.2.3 (NEN, 2005) do mention that risks considering external parties have to be examined, recorded and controlled, but that’s all that’s mentioned that’s related to cloud environments. On the other hand, in chapter A.8 is mentioned that “external users” of the system have to be evaluated to be capable, responsible and aware of the risks before they’re allowed to use the system. This is not conforming cloud environments, where an external party is responsible for most external users. This is just one example, but ISO 27001 is not that useful for the specific cloud environments. Of course, cloud providers as a company can still hugely benefit of the requirements stated in ISO 27001.

3.6 CLOUD SECURITY

To achieve security in the cloud (for example by applying ISAE 3402), (Knolmayer, et al.) uses the 3 basic types of controls used in IT:

- Preventive controls; these are meant to prevent mistakes

- Detective controls; these are meant to detect errors; this way they measure the effectiveness of the preventive controls, which is an important job
- Corrective controls; these are broken when it's too late already for one error, but they can be used to prevent recurrence of errors in the future.

The topic of security in the cloud is current and several companies and institutions try to add something to that discussion. Where most companies try to sell themselves telling how secure they are, there's also a non-profit organization that tries to define cloud security.

The Cloud Security Alliance (CSA) is a non-profit alliance supported by (almost) all big cloud stakeholders, that tries to realize different standards on the area of cloud security. For this purpose, it has for example developed the Security Guidance for Critical Areas of Focus in Cloud Computing (Cloud Security Alliance, 2009). This report gives a load of recommendations to cloud providers for controls and checks to be undertaken in order to have covered the critical areas of cloud security. Next to that, it has also developed a Cloud Controls Matrix (Cloud Security Alliance) that maps a list of (very broad) security controls to the different compliance standards.

To get a further standardization of cloud security and the communication about it, the CSA has developed "CloudAudit" (CloudAudit Working Group). This is a web service that can be run on the server of the cloud provider. Using this service, the cloud provider can easily and in a standardized way, tell (potential) customers to which compliance standard's controls it already complies and to which not yet. This CloudAudit standard is not really used yet, but seems to offer a step forward into the (automated) communication and decision process of cloud services.

3.7 SOC 2

The AICPA has released, around the same time that SSAE 16 was released, the new TLA[14] SOC. SOC stands for Service Organization Control reports. It's an umbrella expression for "internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service." (from: aicpa.org)

As SSAE 16, the AICPA standard for financial reporting in service organizations, fits under this umbrella, the SSAE 16 reports are also called SOC 1 reports. There currently exist 3 different SOC versions, each serving a different purpose. In the table below the differences between these three are visible. (American Institute of Certified Public Accountants) (American Institute of Certified Public Accountants, 2011)

	SOC 1	SOC 2	SOC 3
Area of focus	Financial statements	Security, availability, processing integrity confidentiality, or privacy	Security, availability, processing integrity confidentiality, or privacy
Standard	SSAE 16	AT 101 + SOC 2 guide	AT 101 + TSP 100
Subject	The internal financial controls that affect user organizations' controls	Controls relevant to security, availability, processing integrity, confidentiality, or privacy	Controls relevant to security, availability, processing integrity, confidentiality, or privacy
Users	User entities' auditors, user entities' management and service organizations management	Service organizations management and other parties who have sufficient knowledge about the subject matter	Everyone who's interested

[14] Three-letter acronym

		and about the limitations thereof	
Two types? (I & II)	Yes	Yes	No
Purpose	Assurance about financial controls	Assurance about non-financial controls	Marketing instrument

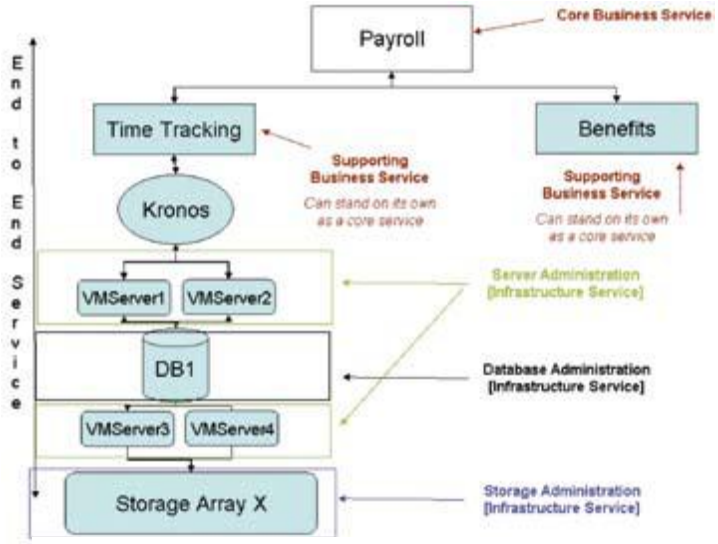
TABLE 3: OVERVIEW SOC STANDARDS

SOC 3 is purely a marketing instrument. The SOC 3 reports contain less detailed information than SOC 2 reports but can yield to a "seal of approval" that can be used on publications and on websites. The SOC 2 report, on the other hand, focuses exactly on the subjects at matter in cloud environments. As SOC 2 was not released until halfway this research, though, it has not been taken into account from the beginning. More about this in a next chapter.

3.8 ITIL

The Information Technology Infrastructure Library (ITIL) is a structured approach in providing IT services. The ITIL was originally produced in the early 80s by the Central Computer and Telecommunications Agency in the UK, which later merged into the Office of Government Commerce (OGC). The OGC is still the official maintainer of the ITIL libraries. (Barafort, et al., 2002)

ITIL is an approach to IT "service" management. A service is defined by (Arraj, 2010) as something that provides value to customers. To that extent, ITIL defines two different services: a business service and an infrastructure service. A business service is a service that a customer can directly utilize, like "Payroll" in the example in the image. The business service can be built upon some other business services, like Time Tracking or Benefits. All business services depend (either direct or indirect) on infrastructure services though, services that run in the background and are not noticeable to the customer. Most IT libraries focus on those infrastructure services and very often on just one of them ("How to build a good database" or "Best practices in distributed storage"). ITIL gives a broader perspective by considering all services at once, both business services and infrastructure services. This is called the "End to End Service" and by addressing the complete spectrum, consistency of the different parts is assured. (Arraj, 2010)



ITIL is built-up around the idea of a Service Lifecycle. It considers 5 stages: Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement. It contains best practices for several processes that are common in a certain phase. For example the Service Operation phase contains a process of Incident Management, Problem Management and others, while the Service Design phase contains processes like Service Level Management, Capacity Management and Availability Management.

When we design security measures for the cloud services that we focus on in this report, it would help if we can determine in advance whether our security measures are good. We could do this by requesting best practices from other companies, but ITIL is designed to deliver exactly that and more. Therefore, when designing the security measures, we can use ITIL as a lead. Also, it is necessary to take the complete End to End Service into account: it doesn't make a difference to the customer whether the database server or the storage array is insecure or down, if the end (SaaS) service doesn't work, the customer can't consume the services.

This is why we will choose ITIL when we have to choose an example process later in the report. ITIL contains tested and widely used best practices while focusing on the End to End Service spectrum.

3.9 Continuous Assurance

Continuous audit, *continuous monitoring* and *continuous assurance* are terms that are hugely related and that correspond a lot to this research. These terms are also very topical in today's literature. Although the first notice of continuous assurance was in the late 80s already, the real impulse in literature came in the 00s. Some big business scandals (Enron, WorldCom) caused the (American) world to doubt the regular auditing methods. Apparently these audits weren't always as reliable as thought and didn't always find the irregularities that the audits were meant to find.

Current literature about continuous assurance mostly focuses on financial audits. In this chapter, the very specific financial issues are mostly ignored as they will not cause any problems in SaaS security (ISAE 3402) assurance in the context of this research.

Continuous assurance is mentioned as a (partial) solution to the problem of the Enron/Worldcom cases and in 2004 continuous assurance is said to be firmly established as the future of auditing (Vasarhelyi, et al., 2004). Continuous assurance is IT-enabled auditing that in short time or real-time can deliver reliable auditing results based on predefined controls. Where regular audit reports are published usually months after the real auditing took place, continuous assurance makes room for real-time auditing where auditors, once approving a certain system of continuous assurance/audit, can constantly, to a given degree, give a decent opinion about the quality of the data and whether the company lives up to its own controls (Rezaee, et al., 2002) (Searcy, et al., 2003). To achieve this, (trans)action logs are monitored and processed by an automated system to test the results against the defined controls and monitors.

When looking at continuous assurance from a broader perspective, terms like continuous monitoring and continuous audit (Roozendaal, 2011) come in sight. Continuous monitoring is technology that enables the management to continuously check the company processes for risks and performance. When this continuous monitoring is audited by auditors, it delivers valuable input for continuous assurance. Continuous audit is a subset of continuous assurance where the processes, systems and transactions are checked automatically for certain controls and constraints. (Alles, et al., 2002)

According to (Alles, et al., 2002), the *demand* for continuous assurance will be the biggest rationale for the development and implementation of continuous assurance. There is no explicit need for the continuous aspect of the assurance so the market has to show a demand for continuous assurance before it will really grow. According to (Vasarhelyi, et al., 2004), there are 6 major fields that request these new needs for assurance. These 6 fields, resulting from the increasing reliance on technologically enabled business processes are:

- Changes in the environment and industry; businesses don't appear to be able to cope with these changes and don't see them coming, while the market demands fast adaptations;
- Controls: modern systems rely more and more on IT-based systems which demand for other controls than the traditional systems. These require assurance concerning whether controls are operational and that someone handles their warnings;
- Human resources: "patterns in personnel changes can indicate problem areas and increased risks";
- Outsourcing: by outsourcing certain areas of a business, virtual, abstract business parts are created. New methodologies are needed to preserve assurance;
- Process integrity: business processes usually flow through different parts of the business, which are mostly audited separately. By using new technology, the intrinsic relationships between these business parts can be examined and controlled;

- Internal and external process coherence (integrity): by using the huge amount of data and statistics available nowadays about business processes, auditors can more efficiently and more accurately define irregular behavior.

Also according to (Vasarhelyi, et al., 2004), continuous assurance should not only be used to automate audits that were previously done by hand, but it should be used to completely remodel and rethink the auditing processes. Other sources say something similar; by using continuous assurance, auditors have to use a completely new way of doing their jobs. Auditing will not be a once-a-year-task anymore, but it will become a continuous task.

To reorganize the assurance task, one needs to decide what it actually is. According to (Alles, et al., 2002), assurance has three essential components:

- Capturing information by the company under assurance
- Monitoring and analyzing the information by the assuror to ensure the reliability of the information
- Communicating the outcome of the assurance engagement by the assuror

If one wants to make that continuous assurance, all three of those elements have to be made "continuous". The data flow (bullet 1) has to be continuous, the analysis (bullet 2) has to be continuous and the reporting (bullet 3) has to be continuous. The outcome of continuous assurance lies in the reporting and that explicitly needs the other two bullets. Therefore, if one of these bullets fail, continuous assurance is off the table.

3.9.1 Downsides and pitfalls

Of course, continuous assurance also has its downsides and pitfalls. The biggest problem in introducing continuous assurance in the world is the lack of adoption by both managers and auditors.

According to (Searcy, et al., 2003), who executed a survey among 217 partners of a big accounting firm in the USA, companies are not ready yet for continuous assurance. Managers do have the wish to diminish the time between the audit activities and the reporting, but none has really taken steps to achieve that yet. And that's only continuous reporting; over 62 percent of the surveyed partners expressed the belief that big companies would work towards continuous reporting, but only 33 percent thought these companies would also go towards continuous assurance. Almost 50 percent of the partners had no opinion on that though and 18 percent thinks continuous assurance is not going to happen. According to (Alles, et al., 2002) though, assurance is good by definition and will improve any transaction and any process. Therefore, the intrinsic value of continuous assurance should be made more visible.

A recent survey of KPMG (KPMG Risk & Compliance, 2010), (only) 3 percent of the surveyed companies (Dutch organizations; 60 percent with an annual turnover of over 1 billion euros) has implemented continuous monitoring and/or continuous audit in their own organization. A third of the companies say there will be a budget to implement continuous assurance over the following years of at least 500.000 euros. But most remarkable about this research is that 79 percent of the surveyed companies are convinced that their organization is controlled effectively by mostly manual tasks. This would mean that these companies might not see the use of continuous assurance at all. Nevertheless, KPMG concludes that we are now (or in 2010) at the turning point for continuous assurance. As KPMG says, "a breakthrough of continuous audit/continuous monitoring can't be far away".

Bigger problems are even found in the facilities area. Companies don't have the money, the time nor the manpower to implement and execute continuous assurance, neither for the financial division as for the IT division. Managers don't consider auditing and financial administration to have a high priority so changing the mindset of managers is one of the biggest pitfalls for continuous assurance, according to (Searcy, et al., 2003). But not only the managers have a problem; also the auditors have to change their mentality and the way they work. It has to go faster, more efficient and they have to start thinking out-of-the-box.

Next to that, both customers and auditors need a better and closer understanding of the systems and need more knowledge to be able to notice and handle warnings and errors. The companies usually don't have a clue about their controls and are therefore unable to implement them.

As the current auditing process is mostly annual-based and the process is created around the thought that it will be executed yearly, the world needs a new audit model, one that "should be process-based and not substantive testing-based" (Searcy, et al., 2003).

Another pitfall is the lack of technological progress in this area. Current business systems are not capable of supporting continuous audit. The technology is outdated and the adaptations needed are complex.

Finally, the independence of the assuror is questionable, according to (Alles, et al., 2002). In a continuous assurance environment, the assuror will have a continuous contract with the company too. This implies a dependence relationship between business and assuror. Said differently, the assuror profits from giving a positive report to the business as that will let him keep his job. Next to that, there's also a technical dependency, as a continuous assurance system needs to be woven into the company's system; to give decent results about assurance, it needs to have access to core data of the system. Therefore, the assuror that has access to the continuous assurance system or even built it himself will get very close to the enterprise system and its data. This would mean that the assuror can be held responsible for the enterprise system and its data too. It is trivial that that is not a desirable situation.

3.9.2 PRIMARY, SECONDARY AND TERTIARY MONITORING

To overcome some of the independence problem and to implement continuous assurance, a three-level monitoring hierarchy is needed. (Vasarhelyi, et al., 2004) describe them as primary, secondary and tertiary monitoring. (Alles, et al., 2004)

The primary monitoring process is the process in which the management of a firm gets updates about various metrics from throughout the business. The management can undertake action whenever they think or feel that a certain metric doesn't meet its necessary level anymore.

The secondary monitoring process is the external audit, which can be partially the same as the primary monitoring process. The key difference is that this is executed by external, independent auditors and the business management has (in theory) no influence on the way this monitoring is performed.

Tertiary monitoring is also called "black box" monitoring and is not yet implemented anywhere. It is in more detail described by (Alles, et al., 2003). According to (Alles, et al., 2003), it should be a read-only audit trail of the secondary monitoring processes. This log file can be examined by a tertiary monitor to examine whether the audit was executed in the right way and the right actions were taken. This will inherently make most dependencies between company and auditor visible to the outside world. Of course this means that this tertiary log has to be at least read-only, if not unavailable to reach for the auditors of the secondary monitoring process and the management of the company. The contents of this log can vary from pure data collection (what happened on which transaction, when, where, by whom) to dynamic and interactive logging where warnings and alarms are generated and real-time summaries are generated.

4 SaaS Security Framework

In this chapter we will develop the new SaaS Security Framework. We will first create a basic framework that is based on the standard that's currently most used for this: ISAE 3402, as a successor of SAS 70. We have to combine this with knowledge from literature and experiences from practice to create a complete framework aimed at SaaS solutions. This first version is then improved and validated by comparing it with the SOC 2 standard. This delivers a better and more complete framework.

4.1 SaaS requirements based on ISAE 3402

As ISAE 3402 is not built for SaaS environments, it is not even aimed at software, the translation towards SaaS security requirements is arbitrary. Nevertheless, its predecessor, on which it is based, has been used very often to do exactly this: provide certainty on the security of SaaS (and other cloud/software) solutions. Therefore, it has to be possible to create a more precise framework that maintains the ideas and principles of ISAE 3402, but is more specific for software, the cloud, or even SaaS solutions.

ISAE 3402 states that the company under audit should have taken measurements that provide:

- Prevention of misinformation, or detection and correction thereof (A25 and A28 of (International Auditing and Assurance Standards Board (IAASB), 2011))
- A continuous monitoring of the controls defined (A29 of (International Auditing and Assurance Standards Board (IAASB), 2011))
- Coverage of the complete system under audit.

This can be combined with the information from literature in chapter 3.1 to cover all the disadvantages of cloud computing. These disadvantages can be seen as the major risk areas of cloud computing.

The disadvantages mentioned in chapter 3.1 (security, continuity, reliability, legal implications, vendor lock-in, migration, customization and integration) are too broad to define controls on. Therefore these disadvantages should be split up into smaller areas. For this, we use a real-world (confidential) SAS 70 report (SaaSplaza, 2011) to see which areas are covered in an auditor-approved report. Also, we study literature more precise to get a more precise subdivision of areas. This results in the following list:

- Security
  - Physical security
    - Data center entrance
    - Backup location entrance
  - User authentication / user management
    - Operating System
    - SaaS Application
  - Data encryption
- Continuity
  - Incident management[15]
  - Availability of engineers
  - Monitoring
  - Communication
    - Internal
    - External
- Reliability
  - Backups
  - Connectivity

  - Fallback for peak moments
  - Incident management[15]
- Legal implications
  - Terms and conditions
  - Usage policy
  - Privacy policy
  - Employees (NDA; trained and skilled)

Four disadvantages are not shown, as they are highly dependent on the SaaS environment itself and have nothing to do with security. These four are:

- Vendor lock-in; this concerns the possible problems when switching from one SaaS solution to another. Apart from the security of the data while moving, this is not relevant to security aspects. The security of the data while moving is the responsibility of the SaaS customer itself and cannot be written down in requirements. These processes differ per situation and the security of the moved data is outside the scope of this research. This research does concern the security of the data before the move and after the move, but that's covered in the other areas.
- Migration; this concerns migrating from a current, existing system towards a cloud solution. The same is valid for this area as for the vendor lock-in, the security of the data once inside the cloud solution is covered in the other areas. The security of the data when not in the cloud solution yet is not the responsibility of the cloud provider.
- Customization; this concerns the creation of ad-hoc solutions, which is more difficult in cloud solutions than in traditional solutions. This in itself is not a security issue. Of course the security of the data when developers create the customization is an issue, the possible presence of security leaks in the customization is an issue, but all that is covered in the other areas.
- Integration; this concerns problems when integrating a cloud solution with other systems inside a company. The security issues in this area can be found in access to the data by these other systems, which is covered in the authentication part, and possible insecurity of the other systems. The latter is the responsibility of the cloud customer though and can't be considered a responsibility of the cloud provider.

Combining the 3 areas of focus of ISAE 3402 and the list of disadvantages in cloud computing, leads to a matrix with on one axis the requirements from ISAE 3402 and on the other axis the specific risk areas of cloud computing:

	Prevention	Detection and correction	Monitoring
Data Center Entrance	Control 1	Control 2	Control 3
Backup Location Entrance	Control 4	…	…
User authentication and user management: OS	Control X	…	…
User authentication and user management: application	Control Y	…	…
…	…	…	…

TABLE 4: REQUIREMENTS CONSTRUCTION MATRIX

Each cell of this table contains one or more controls (like "control 1", "control 2", etc.) where the ISAE 3402 method is applied to the potential risk. For example, the cell of control 4 has to contain preventive controls concerning backup location entrance.

[15] Note that Incident Management is mentioned twice, both in Continuity as well as in Reliability. The requirements are similar, but the topic is important both for assuring continuity as well as for assuring reliability.

As this is not the clearest way to show these controls, they are grouped and listed in Appendix A: List of ISAE 3402 deducted requirements. The company under review is referred to as “the entity”, as it can be, theoretically, any type of organization.

The list in appendix A is the first draft of the SaaS Security Framework. It covers the ideas and principles required by ISAE 3402 and maps them to all the relevant security issues mentioned in literature. Therefore it can be concluded that using this framework, all relevant security issues from literature are covered in all ways that are required to achieve ISAE 3402 compliance.

4.2 SOC 2

In this chapter I will use the draft SaaS Security Framework to compare it with the completely new standard SOC 2. This new standard claims to be the standard to consider when looking for controls on security, confidentiality, processing integrity, availability and privacy. As this new standard doesn’t mention to be based on SAS 70 or one of its successors, it forms an interesting subject of research. How does the new standard compare to the old ones and why are the differences the way they are.

The practical goal of this chapter is to form an improved framework that considers both the requirements from ISAE 3402 as well as the requirements of SOC 2 and takes the best of both worlds. Preferable this framework achieves both ISAE 3402 and SOC 2 compliance in a coherent way.

We will compare the SaaS Security Framework in appendix A with the list of requirements of SOC 2, as found in Appendix B of (American Institute of Certified Public Accountants, 2011).

Both lists are structured in a certain way, which depicts a division of concerns. That can already show some clear differences. After that, the requirements themselves have to be compared to look at the more concrete differences between the two lists. Differences and similarities have to be listed to get a complete overview of the comparison of the two lists. This will be done in the following subchapters.

4.2.1 STRUCTURE

The structure of the two lists is comparable, though not the same. Both are first divided in main topics. Each topic is then divided into a fixed set of areas. All of these areas contain controls in this area, covering the relevant main topic.

The SOC 2 list can be split up into two big chunks. The second chunk, which is officially the fifth main topic, is completely about the topic of privacy and is split up into:

- General
- Notice
- Choice and consent
- Collection
- Use, retention and disposal
- Access
- Disclosure to third parties
- Security for privacy
- Quality
- Monitoring and enforcement

This goes far beyond chapter 9.1.18 in the ISAE 3402 list in appendix A, where privacy is covered. The privacy subject is considered a big issue and that’s exactly what the SOC 2 guide says in its own chapter 1.29: “privacy encompasses a much broader set of activities beyond security that contribute to the effectiveness of a privacy program” (American Institute of Certified Public Accountants, 2011).

The first chunk of the SOC 2 list is built up in a similar structure as our SaaS Security Framework. There are 4 main topics: Security, Availability, Processing Integrity and Confidentiality. Each of these main topics is divided into:

- Policies
- Communications
- Procedures
    - Execution and incident management
    - System components
    - Change management
- Monitoring

As mentioned before, the framework in appendix A is structured into four main topics: Security, Continuity, Reliability and Legal implications. Each main topic is then divided into subtopics and each subtopic is divided into 3 types of controls:

- Prevention
- Detection and correction
- Monitoring

When regarding the main topics of the two lists, one could argue a one-on-one relationship as follows:

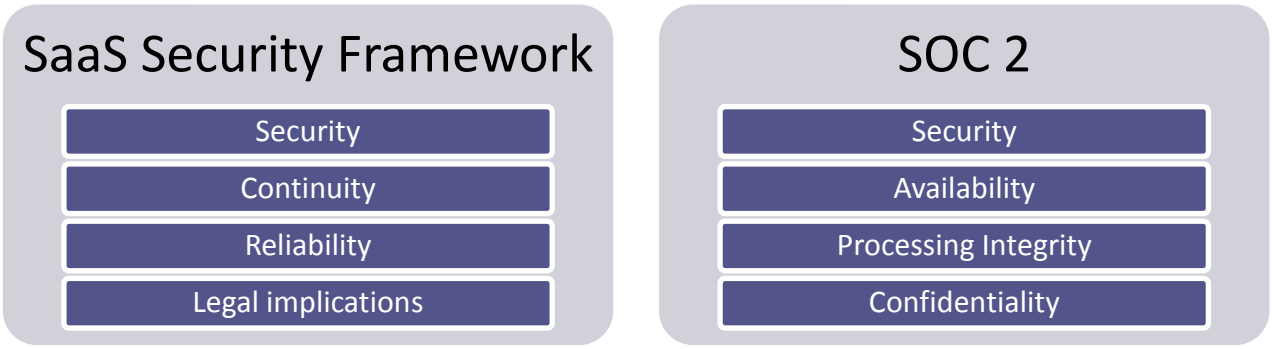
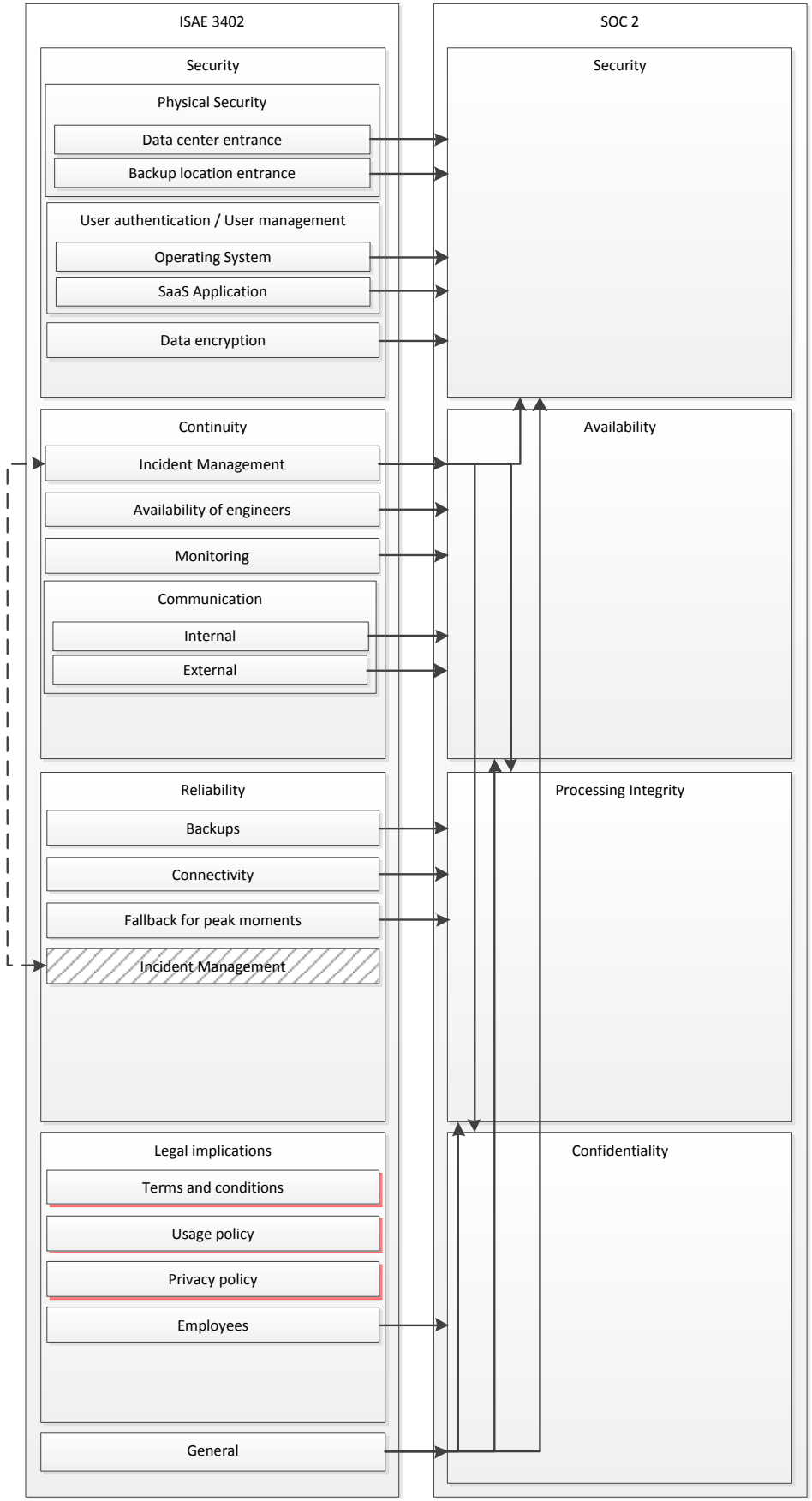


FIGURE 4: COMPARISON OF ISAE 3402 LIST AND SOC 2

Continuity can be a synonym for Availability; Reliability for the (Processing) Integrity and Confidentiality is very related to Legal implications. When taking a closer look, though, we see that there is no simple one-on-one mapping between these subjects. The diagram in **Error! Reference source not found.** shows the mapping from the ISAE 3402 list (the SaaS Security Framework) to the SOC 3402 list. We see that most subtopics from our framework map to the expected main topics in the SOC 2 list. There are some exceptions to this though:

- Incident management occurs twice in the framework. This is on purpose as the topic is relevant in both main topics. SOC 2 agrees with this as incident management policies occur in all four main topics
- In the ISAE 3402 list, some general policies are defined. As expected, the SOC 2 list agrees with this and has these policies recurring in all lists. In SOC 2, these policies are a copy-paste version of each other, where just “security”, “availability”, “processing integrity” or “confidentiality” is filled in
- Three subtopics of Legal Implications: Privacy Policy, Usage Policy and Terms and Conditions are not mentioned in the SOC 2 list. The Privacy Policy is of course highly covered in the privacy main topic, as mentioned earlier.


ISAE 3402
Security
Physical Security
Data center entrance
Backup location entrance
User authentication / User management
Operating System
SaaS Application
Data encryption
Continuity
Incident Management
Availability of engineers
Monitoring
Communication
Internal
External
Reliability
Backups
Connectivity
Fallback for peak moments
Incident Management
Legal implications
Terms and conditions
Usage policy
Privacy policy
Employees
General
SOC 2
Security
Availability
Processing Integrity
Confidentiality

4.2.2 POLICIES

The mapping on structure is still on an abstract level, as we haven't compared the specific policies yet. Doing that is more difficult though, as it's partly about interpretation and partly arbitrary. When comparing policies one-on-one, you are faced with questions like whether the following two policies are the same:

- *Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers* (SOC 2, security topic, 3.3 (American Institute of Certified Public Accountants, 2011))
- *The entity should have policies and technical facilities to detect unauthorized access to the data center* and *The entity should have policies in place on how to respond to unauthorized access to the data center* and *The entity should have policies and technical facilities to detect unauthorized access to the backup location* and *The entity should have policies in place on how to respond to unauthorized access to the backup location* (8.1.1.2.1, 8.1.1.2.2, 8.1.2.2.1 and 8.1.2.2.2 from appendix A)

As you can see, it is arbitrary and unclear to map specific policies. This problem occurs with almost all policy comparison.

Still it's needed to compare the policies, and as we have created the SaaS Security Framework ourselves already, it is safe to say that we understand the meaning and interpretation of that list. Looking at the SOC 2 list with the same view and interpretation, we can notice some differences.

For example, incident management is mentioned 4 times in the SOC 2 list, once in each chapter, each with the text: "Procedures exist to identify, report and act upon system {security breaches, availability issues and related security breaches, processing integrity and related security breaches, confidentiality and related security breaches} and other incidents". Our framework, on the other hand, has a complete chapter on incident management (see 9.1.7), including a notice of "response time", which is not present in the SOC 2 list.

There are also examples of policies present in SOC 2 and not present in the SaaS framework. The SOC 2 list mentions, for example, that there should be policies on how to assign responsibility and accountability for system security. This is not part of the own framework.

SOC 2 states that "responsibility for maintaining and developing the policies is assigned" (non-literal quote). We say (in 9.1.20) that management is responsible. Of course they can sub-assign, but that's management's decision.

In general, it is clear that SOC 2 is more complete. It has been formulated in a more precise and legal way, which is an advantage for the purpose of this list. Nevertheless, the ISAE 3402 list contains policies or details that are not (explicitly) mentioned in the SOC 2 list and should be taken into consideration for creating the final framework of policies.

These differences are:

Policy in SaaS Security Framework	Difference with SOC 2
8.1.3.1.2	Notice of policies on password strength
8.1.3.1.3	Policy that user accounts are personal and non-transferable
8.1.7.1.4	Notice of response time policies in the incident management process
8.1.8.1.1	Policies that there should be backup engineers available for peak moments or huge downtime situations and the response time of these engineers
8.1.8.1.3	
8.1.10.1.1	Policies about the internal communication system: new employees should get a training and the system should allow for easy searching through historical communication
8.1.10.1.3	
8.1.10.2.1	
8.1.11.1.1	Notice of policies for external communication
8.1.11.3.1	Notice of policies on response times of external communication

8.1.12.1.1	Notice of policies on frequency, location and contents of backups
8.1.12.2.1	Notice of policies on backup integrity; testing backups frequently and how to respond to failed backups
8.1.12.2.2	
8.1.12.2.3	
8.1.12.3.1	Notice of policies on the status of backups
8.1.16 (whole chapter)	Notice of the existence of a Terms and Conditions document
8.1.17 (whole chapter)	Notice of the existence of a Usage Policy document
8.1.19.1.1	Policies on the existence, use and regular review of a non-disclosure agreement for employees
8.1.19.2.1	
8.1.19.3.2	

TABLE 5: MISSING OR DIFFERENT POLICIES IN SOC 2

If the policies and improvements noted in the table above are added to the SOC 2 list, this will create a framework that both implies SOC 2 compliance as well as ISAE 3402 compliance. The policies can probably not be added one-on-one, as the SOC 2 list uses more legal terms and another way of formulating its criteria. For the sake of this research, though, it is sufficient to use the formulations of our own framework. We don't have the legal background to formulate the criteria in the right way and the goal of this research is to make a comparison and try to make a software tool. That's both also possible with the current way of formulating.

It can be questioned whether these policies are needed to ensure ISAE 3402 compliance when a SOC 2 compliance is reached. Remember that the creation of the SaaS Security Framework consisted of arbitrary choices based on three main principles of ISAE 3402 and the big risk areas for cloud computing from literature. ISAE 3402 never mentions explicitly that a company should have a Terms and Conditions document, for example. When studying Table 5, it only consists of differences that result from our arbitrary choices. When these differences would be taken out of the SaaS Security Framework (instead of implemented in SOC 2), it would still be a valid framework and meet all the ISAE 3402 requirements. Based on this, it can be concluded that a SOC 2 compliance implies an ISAE 3402 compliance. The other way around is not true, as ISAE 3402 is much more abstract and can be used much broader. For example, a ISAE 3402 audit can be used to report on financial controls, where the SOC 2 does not.

5 CONTINUOUS SAAS SECURITY ASSURANCE

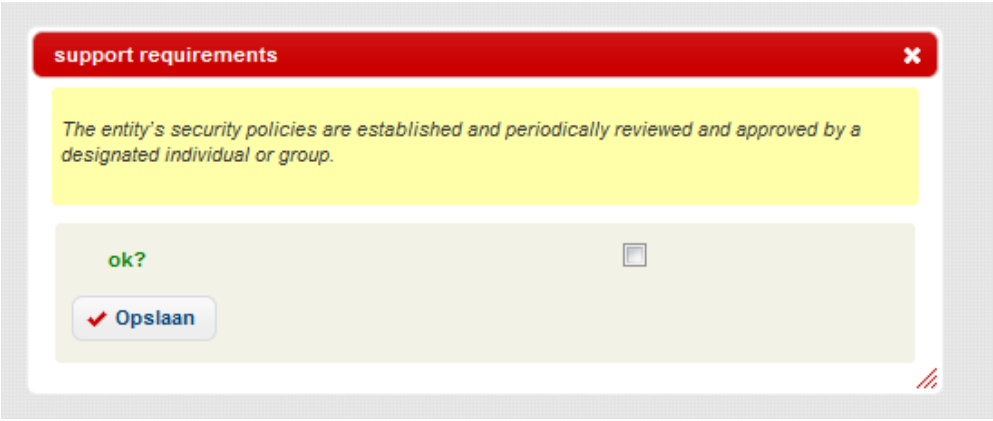
In this chapter we will answer the second and third research questions. These questions concern building a tool to automatically check or enforce the SaaS Security Framework as defined elsewhere in this report. First, we discuss the boundaries. It is not possible to complete automate the system, so we discuss what the realistic options are. Given the idea that we are looking for the highest level of automation, we can deduct a list of requirements a tool should meet to be able to enforce the SaaS Security Framework upon a SaaS solution. This requirements list is what the SaaS Security Automation Requirements consists of. With this list of software requirements, we check whether it's buildable and if so, whether existing tools can reach this goal.

When talking about a tool to assure security, it is evident that insecurity of the tool itself should be avoided at all times. The tool will investigate potential security issues, so it has access to core parts of the system. If the tool that checks it contains security leaks, all the systems it checks are unsafe. The security of the checking tool is an area of special interest and will be covered in this chapter too.

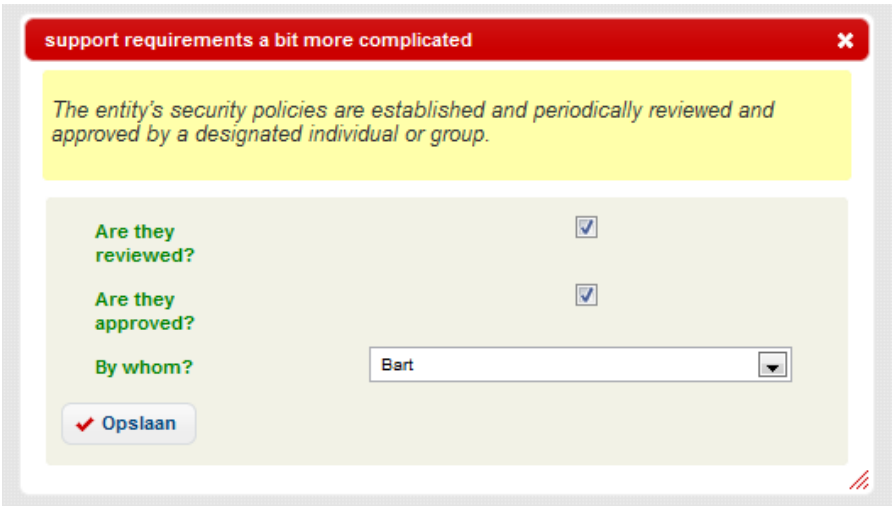
5.1 POSSIBILITIES AND LIMITATIONS TO AUTOMATE THE REQUIREMENTS

We can start by saying that it is never possible to completely automate all the requirements. In a previous chapter, we have decided that the SOC 2 list, with some additions, forms the best framework to ensure security of the SaaS environments. Let's take a look at the first requirement in the SOC 2 list:

The entity's security policies are established and periodically reviewed and approved by a designated individual or group.



We can immediately see that this is not a candidate for complete automation. This policy involves human interaction and human work. On the other hand, it is of course possible for an automated system to **support** the entity when executing this requirement. When an automated system can periodically send a reminder to "a designated individual or group" that they should establish and/or review a security policy, the system supports compliance with this requirement.



If we abstract that into the extreme, we can conclude that any item on the list can be supported like this. In the most abstract form, the exact text of the requirement is given to someone in the role of "Security

Officer" and this person has to decide whether this requirement is met. Examples how this would be done are given in **Error! Reference source not found.** and **Error! Reference source not found.**.

Any workflow management system that has notice of tasks and roles can implement this most basic behavior. One can create a process in which all the aspects of the lists follow each other, resulting in a positive result when all checkboxes are checked. Assigning tasks to others, timed triggers and uploading documents as proof or supportive material are enhancements that most workflow management systems offer.

If we look at commercial software aimed at this market, we find surprising results. Most audit management systems, usually offered at high prices, offer not much more than the described functionality above. We have inspected the feature lists, whitepapers, websites, screenshots and demos of six commercial Audit Management systems that claim to have a large customer-base, seem to be mature and show up high in Google's search results. These six are:

- MetricStream Audit Management System[16]
- Master Control Audit Management Software System[17]
- RSA Archer Audit Management[18]
- Infoland iAudit[19]
- ARC Logics CCH TeamMate[20]
- MKinsight[21]

If we look at these systems, we see that none of them offers any kind of real automation. Most of these systems are aimed at internal audits where an internal auditor or an internal audit team gets an advanced checklist where documents can be uploaded and tasks can be scheduled. Agreed, such a system can make the life of internal auditors a lot easier, but they don't offer the functionality of free workflow management systems like YAWL[22].

If we would use one of these commercial Audit Management Systems or the same basic functionality in any other workflow management system, we would just organize internal information. We would still need an independent auditor to check whether the person saying "yes" to the questions, was telling the truth. We are looking for a solution in which a (preferably large) part of the job of the auditor is already done and there's no need to check it again. For this, we need to add some intelligence to the basic workflows described above and we need software with some more functionality than the commercial Audit Managers that we looked at.

This more intelligent software should not have the same downside as the less intelligent audit management. The goal of the intelligent tool is first of all to give a more up-to-date and fast verdict on the compliance with our SaaS Security Framework. This is defined as such in our problem description and research questions. To be able to do this, though, we need to diminish the need for external, independent auditors. This can be achieved by handing over the task of the auditor to another, trustworthy, party: software. Of course software is only as reliable as the programmer that built it, but that pitfall can be prevented. The software tool could be checked by an auditor (or another independent third party). If then the software tool cannot be altered by the customer or end users, one investment to have an auditor check the tool can be returned by selling enough instances/copies of the software. There is not much to be found about the prices of a SOC 2 / ISAE 3402 audit, but a SAS 70 audit is reported to cost between 25.000 and 90.000 dollars[23] and should be conducted every year. If the actual cost of the audit can only be cut by 25 percent, this would already save 6 to 22 thousand dollars a year. Per company that has an audit done. So if a tool can be developed and is

[16] http://www.metricstream.com/products/auditmangmt_features.htm
[17] http://www.mastercontrol.com/audit-management/audit-management-software-systems.html
[18] http://www.archer.com/solutions/audit_management.html
[19] http://infoland.nl/Default.aspx?MenuItemID=3a29707e-47ef-4f40-a39a-428d611e02f2
[20] http://www.arclogics.com/TeamMate_Home.aspx
[21] http://www.mkinsight.com/default.aspx
[22] http://www.yawlfoundation.org/
[23] http://www.sas70.us.com/services/sas70-pricing.php

used by 10 companies, this tool can have a development budget of over 50.000 dollars. This can be cost-efficient for both the builder of the tool as well as for the company that uses the tool. The only ones losing money here are the auditors. But with our goal to automate and generalize the auditing process, this is unavoidable.

So what should this more intelligent system do? Let's take a look at our previous example from the SOC 2 list:

The entity's security policies are established and periodically reviewed and approved by a designated individual or group

It would be for example better if the system does not just remind the designated people that they should do it, but also requires them to. This means the system does not do the actual checking, but it does check the progress and execution of the workflow of the check. This can be implemented in many ways, from a nagging pop-up where someone has to press "Okay, I have done this" to a more sophisticated system where the user(s) are required to upload the reviewed security policy before a certain deadline. If that does not happen, a message is sent to the higher management that there is a problem with the security policies and a possible audit breach is logged.

If we take a look at the more sophisticated system for the policy mentioned above, the system is then able to (automatically) fulfill the requirement 2.2 of the security chapter of SOC 2, stating:

The security obligations of users and the entity's security commitments to users are communicated to authorized users.

As the document containing this information has been uploaded to the system, it is easy to implement that, once uploaded, this document is sent to authorized users. Of course, the system has to know how to reach the authorized users. That information can be given to the system in a few ways, for example by uploading or entering a list of authorized users. That is prone to errors. It would be better if the system already knew which users are authorized. It can do a query on an (external) database containing the users, for example. If the systems are more tightly coupled, the security tool could also be used to manage user rights on the target system. When user authentication on the target system is maintained via the security tool system, the security tool will know which users are authenticated.

Each of the policies in the SaaS Security Framework has different possibilities to implement it in an "intelligent" way. Some policies are not suitable for it at all and some can be fully automated. The only way to know exactly how intelligent this system can become, is by checking the complete SaaS Security Framework for possibilities for intelligent implementation. As a basis we take a workflow management system that has basic notion of tasks, users, roles, assigning tasks to users based on roles, assigning tasks to users manually, timed triggers, uploading documents to gather proof for the auditor, scheduling tasks and several types of input fields per task based on which criteria can be defined to trigger a next task. This approximately defines the more advanced versions of the audit management software tools mentioned earlier and any workflow management system (like for example YAWL) supports these principles too. Now we take the SaaS Security Framework and check how much more intelligence can be added.

5.2 Extra intelligence to the SaaS Security Framework

The tables in this section are literally the tables from SOC 2 (American Institute of Certified Public Accountants, 2011), extended with an extra column for "extra intelligence". This column contains how extra intelligence on top of putting the criteria into a basic workflow system, can improve the support and sometimes automation of the criteria.

In subsection 5.2.15 we consider the additions we have from our own SaaS Security Framework and add the same column for extra intelligence.

As you can see, in over 58% (123 out of 210 items) of the criteria, we can offer extra intelligence to extra support or sometimes completely automate the requirement. If we don't take the privacy sections into account, this even comes at almost 73% (100 out of 137) of the items for which we can offer extra intelligence.

5.2.1 Security Principle and Criteria Table

The system is protected against unauthorized access (both physical and logical)

	Criteria	***Extra intelligence***
1.0	**Policies: The entity defines and documents its policies for the security of its system.**	
1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	Policy uploaded during this task and "designated individual or group" (roles) fetched from external system.
1.2	The entity's security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the security requirements of authorized users *b.* Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements *c.* Assessing risks on a periodic basis *d.* Preventing unauthorized access *e.* Adding new users, modifying the access levels of existing users, and removing users who no longer need access *f.* Assigning responsibility and accountability for system security *g.* Assigning responsibility and accountability for system changes and maintenance *h.* Testing, evaluating, and authorizing system components before implementation *i.* Addressing how complaints and requests relating to security issues are resolved *j.* Identifying and mitigating security breaches and other incidents *k.* Providing for training and other resources to support its system security policies *l.* Providing for the handling of exceptions and situations not specifically addressed in its system security policies *m.* Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements *n.* Providing for sharing information with third parties	
1.3	Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.	Roles in the WfMS; these roles are possibly managed in external system; link between WfMS and these systems.
2.0	**Communications: The entity communicates its defined system security policies to responsible parties and authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to	Upload during the task and automatically send it to the users.

	authorized users.	
2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	Upload during the task and automatically send it to the users.
2.3	Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	Upload during the task and automatically send it to the users.
2.4	The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	Upload during the task and automatically send it to the users.
2.5	Changes that may affect system security are communicated to management and users who will be affected.	Upload during the task and automatically send it to the users.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	If these procedures are processes in the WfMS, identify them as such. Updates or removal of these processes then triggers possible compliance breach.
3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
	a. Logical access security measures to restrict access to information resources not deemed to be public.	These security measures can be implemented as workflow processes themselves, if there is a link to a system where users and roles are defined.
	b. Identification and authentication of users.	Can be a workflow process itself.
	c. Registration and authorization of new users.	Users can be centrally managed from within the tool.
	d. The process to make changes and updates to user profiles.	Users can be centrally managed from within the tool.
	e. Distribution of output restricted to authorized users.	Can be a workflow process itself.
	f. Restriction of access to offline storage, backup data, systems, and media.	An automated task can assign and revoke access based on users and roles in an external system.
	g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	
3.3	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	These procedures can be implemented as workflow processes or automated based on user roles.
3.4	Procedures exist to protect against unauthorized access to system resources.	These procedures can be implemented as workflow processes.
3.5	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	A procedure to automatically regularly check for virus updates and install them.
3.6	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	
	Criteria related to execution and incident management used to achieve objectives	
3.7	Procedures exist to identify, report, and act upon system security breaches and other incidents.	An incident management system can be part of the tool.
	Criteria related to the system components used to achieve the objectives	
3.8	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	If these classification policies are programmable/automatable, it can be done automatically; else no extra intelligence possible.
3.9	Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	These issues can be managed by the incident management system inside the tool.
3.10	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	
3.11	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	
	Change management-related criteria applicable to the system's security	

3.12	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	
3.13	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	This process (authorize, test and document -> change) can be a process in the tool.
3.14	Procedures exist to provide that emergency changes are documented and authorized timely.	Emergency changes can be documented and managed using the incident management tool.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.**	
4.1	The entity's system security is periodically reviewed and compared with the defined system security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.3	Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.	

5.2.2 AVAILABILITY PRINCIPLE AND CRITERIA TABLE

The system is available for operation and use as committed or agreed.

	Criteria	***Extra Intelligence***
1.0	**Policies: The entity defines and documents its policies for the availability of its system.**	
1.1	The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	Policy uploaded during this task and “designated individual or group” (roles) fetched from external system.
1.2	The entity's system availability and related security policies include, but may not be limited to, the following matters:	
	a. Identifying and documenting the system availability and related security requirements of authorized users.	
	b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements	
	c. Assessing risks on a periodic basis	
	d. Preventing unauthorized access.	
	e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.	
	f. Assigning responsibility and accountability for system availability and related security.	
	g. Assigning responsibility and accountability for system changes and maintenance.	
	h. Testing, evaluating, and authorizing system components before implementation.	
	i. Addressing how complaints and requests relating to system availability and related security issues are resolved.	
	j. Identifying and mitigating system availability and related security breaches and other incidents.	
	k. Providing for training and other resources to support its system availability and related security policies.	
	l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.	
	m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	
	n. Recovering and continuing service in accordance with documented customer commitments or other agreements.	
	o. Monitoring system capacity to achieve customer commitments or other agreements regarding availability	

1.3	Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.	Roles in the WfMS; these roles are possibly managed in external system; link between WfMS and these systems.
2.0	**Communications: The entity communicates the defined system availability policies to responsible parties and authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	Upload during the task and automatically send it to the users.
2.2	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	Upload during the task and automatically send it to the users.
2.3	Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	Upload during the task and automatically send it to the users.
2.4	The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	Upload during the task and automatically send it to the users.
2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	Upload during the task and automatically send it to the users.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	If these procedures are processes in the WfMS, identify them as such. Updates or removal of these processes then triggers possible compliance breach.
3.2	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	Where possible, these measures can be implemented in the tool.
3.3	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	Executing backup and restore procedures can be executed from the tool; backup procedures can be scheduled periodically
3.4	Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	Integrity checks can be launched automatically and the results can be communicated back by the tool.
	Security-related criteria relevant to the system's availability	
3.5	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
	a. Logical access security measures to restrict access to information resources not deemed to be public.	These security measures can be implemented as workflow processes themselves, if there is a link to a system where users and roles are defined.
	b. Identification and authentication of users.	Can be a workflow process itself.
	c. Registration and authorization of new users.	Users can be centrally managed from within the tool.
	d. The process to make changes and updates to user profiles.	Users can be centrally managed from within the tool.
	e. Restriction of access to offline storage, backup data, systems and media.	An automated task can assign and revoke access based on users and roles in an external system.
	f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	
3.6	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	These procedures can be implemented as workflow processes or automated based on user roles.
3.7	Procedures exist to protect against unauthorized access to system resources.	These procedures can be implemented as workflow processes.
3.8	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	A procedure to automatically regularly check for virus updates and install them.

3.9	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	
	Criteria related to execution and incident management used to achieve objectives	
3.10	Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	An incident management system can be part of the tool.
	Criteria related to the system components used to achieve the objectives	
3.11	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	If these classification policies are programmable/automatable, it can be done automatically; else no extra intelligence possible.
3.12	Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	These issues can be managed by the incident management system inside the tool.
3.13	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.	
3.14	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.	
	Change management-related criteria applicable to the system's availability	
3.15	Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.	
3.16	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	This process (authorize, test and document -> change) can be a process in the tool.
3.17	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Emergency changes can be documented and managed using the incident management tool.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system availability policies.**	
4.1	The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.3	Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.	

5.2.3 PROCESSING INTEGRITY PRINCIPLE AND CRITERIA TABLE

System processing is complete, accurate, timely, and authorized.

	Criteria	***Extra intelligence***
1.0	**Policies: The entity defines and documents its policies for the processing integrity of its system.**	
1.1	The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.	Policy uploaded during this task and “designated individual or group” (roles) fetched from external system.
1.2	The entity's system processing integrity and related security policies include, but may not be limited to, the following matters: *a.* Identifying and documenting the system processing integrity and related security requirements of authorized users *b.* Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements *c.* Assessing risks on a periodic basis	

d. Preventing unauthorized access

e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access

f. Assigning responsibility and accountability for system processing integrity and related security

g. Assigning responsibility and accountability for system changes and maintenance

h. Testing, evaluating, and authorizing system components before implementation

i. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved

j. Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents

k. Providing for training and other resources to support its system processing integrity and related system security policies

l. Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies

m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements

1.3	Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.	Roles in the WfMS; these roles are possibly managed in external system; link between WfMS and these systems.
2.0	**Communications: The entity communicates its documented system processing integrity policies to responsible parties and authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. If the system is an e-commerce system, additional information provided on its website includes, but may not be limited to, the following matters: *a.* Descriptive information about the nature of the goods or services that will be provided, including, where appropriate, ○ condition of goods (whether they are new, used, or reconditioned). ○ description of services (or service contract). ○ sources of information (where it was obtained and how it was compiled). *b.* The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters: ○ Time frame for completion of transactions (*transaction* means fulfillment of orders where goods are being sold and delivery of service where a service is being provided) ○ Time frame and process for informing customers of exceptions to normal processing of orders or service requests ○ Normal method of delivery of goods or services, including customer options, where applicable ○ Payment terms, including customer options, if any ○ Electronic settlement practices and related charges to customers ○ How customers may cancel recurring charges, if any ○ Product return policies and limited liability, where applicable *c.* Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its website.	Upload during the task and automatically send it to the users. ○

	d. Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.	
2.2	The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	Upload during the task and automatically send it to the users.
2.3	Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Upload during the task and automatically send it to the users.
2.4	The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.	Upload during the task and automatically send it to the users.
2.5	Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.	Upload during the task and automatically send it to the users.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.	If these procedures are processes in the WfMS, identify them as such. Updates or removal of these processes then triggers possible compliance breach.
3.2	The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but may not be limited to, the following matters: *a.* The entity checks each request or transaction for accuracy and completeness. *b.* Positive acknowledgment is received from the customer before the transaction is processed.	a and b can be monitored by inspecting the audit trail or log files of the e-commerce system.
3.3	The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters: *a.* The correct goods are shipped in the correct quantities in the time frame agreed upon, or services and information are provided to the customer as requested. *b.* Transaction exceptions are promptly communicated to the customer. *c.* Incoming messages are processed and delivered accurately and completely to the correct IP address. *d.* Outgoing messages are processed and delivered accurately and completely to the service provider's (SP's) Internet access point. *e.* Messages remain intact while in transit within the confines of the SP's network.	If the e-commerce backend is a workflow system, a, b, c, d and e can be checked automatically by inspecting log files on the servers and audit trails in the workflow system.
3.4	The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies. If the system is an e-commerce system, the entity's procedures include, but are not necessarily limited to, the following matters: • The entity displays sales prices and all other costs and fees to the customer before processing the transaction. • Transactions are billed and electronically settled as agreed. • Billing or settlement errors are promptly corrected.	The third bullet can be handled in the incident management system.
3.5	There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.	
	Security-related criteria relevant to the system's processing integrity	
3.6	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	

	a. Logical access security measures to access information not deemed to be public	These security measures can be implemented as workflow processes themselves, if there is a link to a system where users and roles are defined.
	b. Identification and authentication of authorized users	Can be a workflow process itself.
	c. Registration and authorization of new users	Users can be centrally managed from within the tool.
	d. The process to make changes and updates to user profiles	Users can be centrally managed from within the tool.
	e. Distribution of output restricted to authorized users	Can be a workflow process itself.
	f. Restriction of access to offline storage, backup data, systems, and media	An automated task can assign and revoke access based on users and roles in an external system.
	g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)	
3.7	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.	These procedures can be implemented as workflow processes or automated based on user roles.
3.8	Procedures exist to protect against unauthorized access to system resources.	These procedures can be implemented as workflow processes.
3.9	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	A procedure to automatically regularly check for virus updates and install them.
3.10	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	
	Criteria related to execution and incident management used to achieve objectives	
3.11	Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.	An incident management system can be part of the tool.
	Criteria related to the system components used to achieve the objectives	
3.12	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	If these classification policies are programmable/automatable, it can be done automatically; else no extra intelligence possible.
3.13	Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	These issues can be managed by the incident management system inside the tool.
3.14	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	
3.15	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.	
	Change management-related criteria applicable to the system's processing integrity	
3.16	Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.	
3.17	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	This process (authorize, test and document -> change) can be a process in the tool.
3.18	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Emergency changes can be documented and managed using the incident management tool.
	Availability-related criteria applicable to the system's processing integrity	
3.19	Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.	
3.20	Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.	

3.21	Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.	Backup procedures can be automatically executed by the tool.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.**	
4.1	System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.3	Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.	

5.2.4 CONFIDENTIALITY PRINCIPLE AND CRITERIA TABLE

Information designated as confidential is protected by the system as committed or agreed.

	Criteria	***Extra intelligence***
1.0	**Policies: The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.**	
1.1	The entity's system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.	Policy uploaded during this task and “designated individual or group” (roles) fetched from external system.
1.2	The entity's policies related to the system's protection of confidential information and security include, but are not limited to, the following matters: *a.* Identifying and documenting the confidentiality and related security requirements of authorized users *b.* Classifying data based on its criticality and sensitivity that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements *c.* Assessing risk on a periodic basis *d.* Preventing unauthorized access *e.* Adding new users, modifying the access levels of existing users, and removing users who no longer need access *f.* Assigning responsibility and accountability for confidentiality and related security *g.* Assigning responsibility and accountability for system changes and maintenance *h.* Testing, evaluating, and authorizing system components before implementation *i.* Addressing how complaints and requests relating to confidentiality and related security issues are resolved *j.* Handling confidentiality and related security breaches and other incidents *k.* Providing for training and other resources to support its system confidentiality and related security policies *l.* Providing for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies *m.* Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements *n.* Sharing information with third parties	
1.3	Responsibility and accountability for developing and maintaining the entity's system confidentiality and related security policies, and changes and updates to those polices, are assigned.	Roles in the WfMS; these roles are possibly managed in external system; link between WfMS and these systems.
2.0	**Communications: The entity communicates its defined policies related to the system's protection of confidential information to responsible parties and authorized users.**	
2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	Upload during the task and automatically send it to the users.

2.2	The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters: *a.* How information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information. *b.* How access to confidential information is authorized and how such authorization is rescinded. *c.* How confidential information is used. *d.* How confidential information is shared. *e.* If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity. *f.* Practices to comply with applicable laws and regulations addressing confidentiality.	Upload during the task and automatically send it to the users.
2.3	Responsibility and accountability for the entity's system confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	Upload during the task and automatically send it to the users.
2.4	The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.	Upload during the task and automatically send it to the users.
2.5	Changes that may affect confidentiality and system security are communicated to management and users who will be affected.	Upload during the task and automatically send it to the users.
3.0	**Procedures: The entity placed in operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.**	
3.1	Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system confidentiality commitments and (2) assess the risks associated with the identified threats.	If these procedures are processes in the WfMS, identify them as such. Updates or removal of these processes then triggers possible compliance breach.
3.2	The system procedures related to confidentiality of inputs are consistent with the documented confidentiality policies.	
3.3	The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.	
3.4	The system procedures related to confidentiality of outputs are consistent with the documented confidentiality policies.	
3.5	The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.	Automated disclosure can be monitored by the tool; manual disclosure is not automatable.
3.6	The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	
3.7	In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the system confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer's confidential information.	
	System security-related criteria relevant to confidentiality	
3.8	Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters: *a.* Logical access security measures to restrict access to information resources not deemed to be public	These security measures can be implemented as workflow processes themselves, if there is a link to a system where users and roles are defined.

	b. Identification and authentication of all users.	Can be a workflow process itself.
	c. Registration and authorization of new users.	Users can be centrally managed from within the tool.
	d. The process to make changes and updates to user profiles.	Users can be centrally managed from within the tool.
	e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	If the tool is not only used for user management but also for user authentication (as Single Sign-On tool, for example), user identification can be provided to other tools. It can not be checked automatically whether other tools do not disclose too much information.
	f. Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.	Access to restricted sources can be managed automatically by the tool, based on users and roles.
	g. Distribution of output containing confidential information restricted to authorized users.	Can be a workflow process itself.
	h. Restriction of access to offline storage, backup data, systems, and media.	An automated task can assign and revoke access based on users and roles in an external system.
	i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	
3.9	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	These procedures can be implemented as workflow processes or automated based on user roles.
3.10	Procedures exist to protect against unauthorized access to system resources.	These procedures can be implemented as workflow processes.
3.11	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	A procedure to automatically regularly check for virus updates and install them.
3.12	Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.	
	Criteria related to execution and incident management used to achieve the objectives	
3.13	Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.	An incident management system can be part of the tool.
	Criteria related to the system components used to achieve the objectives	
3.14	Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.	If these classification policies are programmable/automatable, it can be done automatically; else no extra intelligence possible.
3.15	Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	These issues can be managed by the incident management system inside the tool.
3.16	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined confidentiality and related security policies.	
3.17	Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.	
	Change management-related criteria relevant to confidentiality	
3.18	Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.	
3.19	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	This process (authorize, test and document -> change) can be a process in the tool.
3.20	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Emergency changes can be documented and managed using the incident management tool.

3.21	Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.	If a DTAP principle is used for deploying solutions, this can be managed or done automatically by the tool. Part of this procedure can be to anonimyze data.
4.0	**Monitoring: The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.**	
4.1	The entity's system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.	Partly automatable by inspecting audit trails from the processes inside the tool.
4.3	Environmental, regulatory, and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.	

5.2.5 Generally Accepted Privacy Principles and Criteria

Ref.	*Management Principle and Criteria*	*Extra intelligence*
1.0	**The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.**	
1.1	**Policies and Communications**	
1.1.0	**Privacy Policies** The entity defines and documents its privacy policies with respect to the following: *a.* Notice (See 2.1.0) *b.* Choice and consent (See 3.1.0) *c.* Collection (See 4.1.0) *d.* Use, retention, and disposal (See 5.1.0) *e.* Access (See 6.1.0) *f.* Disclosure to third parties (See 7.1.0) *g.* Security for privacy (See 8.1.0) *h.* Quality (See 9.1.0) *i.* Monitoring and enforcement (See 10.1.0)	
1.1.1	**Communication to Internal Personnel** Privacy policies and the consequences of noncompliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	Upload the policy to the tool, which then sends it automatically to the correct users
1.1.2	**Responsibility and Accountability for Policies** Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	Roles in the WfMS; these roles are possibly managed in external system; link between WfMS and these systems. The names of the people that have this role assigned can be communicated via the tool (either by message or by giving the possibility to look it up real-time)
1.2	**Procedures and Controls**	
1.2.1	**Review and Approval** Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Can be a process in the tool

1.2.2 **Consistency of Privacy Policies and Procedures With Laws and Regulations**

Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.

1.2.3 **Personal Information Identification and Classification**

The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.

Identification of processes, systems and third parties can be done from inside the tool. This information is useful when checking other items on this list.

1.2.4 **Risk Assessment**

A risk assessment process is used to establish a risk baseline and to, at least annually, identify new or changed risks to personal information and to develop and update responses to such risks.

1.2.5 **Consistency of Commitments With Privacy Policies and Procedures**

Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.

1.2.6 **Infrastructure and Systems Management**

The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:

- Infrastructure
- Systems
- Applications
- Websites
- Procedures
- Products and services
- Data bases and information repositories
- Mobile computing and other similar electronic devices

The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.

1.2.7 **Privacy Incident and Breach Management**

A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:

- Procedures for the identification, management, and resolution of privacy incidents and breaches
- Defined responsibilities
- A process to identify incident severity and determine required actions and escalation procedures
- A process for complying with breach laws and regulations, including stakeholders breach notification, if required
- An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate
- A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following:
  - Incident patterns and root cause
  - Changes in the internal control environment or external requirements (regulation or legislation)
- Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed

Incidents and breaches can be managed by the incident management system inside the tool. This incident management system should then include the notion of severity, escalation, etcetera.

1.2.8 **Supporting Resources**

Resources are provided by the entity to implement and support its privacy policies.

1.2.9 **Qualifications of Internal Personnel**

The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received needed training.

If the tool has access to the HRM system, that system should document who has had training and who has qualifications. User rights and roles can be determined based on that.

1.2.10 **Privacy Awareness and Training**

A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.

1.2.11 **Changes in Regulatory and Business Requirements**

For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:

- Legal and regulatory
- Contracts, including service-level agreements
- Industry requirements
- Business operations and processes
- People, roles, and responsibilities
- Technology

Privacy policies and procedures are updated to reflect changes in requirements.

5.2.6 NOTICE

Ref. Notice Principle and Criteria	***Extra intelligence***
2.0 The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.	
2.1 Policies and Communications	

2.1.0 **Privacy Policies**

The entity's privacy policies address providing notice to individuals.

2.1.1 **Communication to Individuals**

Notice is provided to individuals regarding the following privacy policies:

a. Purpose for collecting personal information
b. Choice and consent (See 3.1.1)
c. Collection (See 4.1.1)
d. Use, retention, and disposal (See 5.1.1)
e. Access (See 6.1.1)
f. Disclosure to third parties (See 7.1.1)
g. Security for privacy (See 8.1.1)
h. Quality (See 9.1.1)
i. Monitoring and enforcement (See 10.1.1)

If personal information is collected from sources other than the individual, such sources are described in the notice.

The notice has to be given in another way, but when processes exist (for example an online shop) where a user has to explicitly consent to the privacy policy, it can be automatically checked whether all users consented to this. Especially the ones that ordered by phone or email, for example.

2.2 Procedures and Controls

2.2.1 **Provision of Notice**

Notice is provided to the individual about the entity's privacy policies and procedures (*a*) at or before the time personal information is collected, or as soon as practical thereafter, (*b*) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (*c*) before personal information is used for new purposes not previously identified.

2.2.2 **Entities and Activities Covered**

An objective description of the entities and activities covered by the privacy policies and procedures is included in the entity's privacy notice.

2.2.3 **Clear and Conspicuous**

The entity's privacy notice is conspicuous and uses clear language.

5.2.7 CHOICE AND CONSENT

Ref.	***Choice and Consent Principle and Criteria***	***Extra intelligence***
3.0	**The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.**	
3.1	**Policies and Communications**	
3.1.0	**Privacy Policies** The entity's privacy policies address the choices available to individuals and the consent to be obtained.	
3.1.1	**Communication to Individuals** Individuals are informed about (*a*) the choices available to them with respect to the collection, use, and disclosure of personal information, and (*b*) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.	Consent can be checked automatically, see 2.1.1 of the privacy part of this list
3.1.2	**Consequences of Denying or Withdrawing Consent** When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	
3.2	**Procedures and Controls**	
3.2.1	**Implicit or Explicit Consent** Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.	Consent can be checked automatically, see 2.1.1 of the privacy part of this list

3.2.2 **Consent for New Purposes and Uses**
If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified, and implicit or explicit consent is obtained prior to such new use or purpose.
When a new privacy policy/notice is approved by the management, this can be executed automatically.

3.2.3 **Explicit Consent for Sensitive Information**
Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.
Consent can be checked automatically, see 2.1.1 of the privacy part of this list

3.2.4 **Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices**
Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.
Consent can be checked automatically, see 2.1.1 of the privacy part of this list

5.2.8 COLLECTION

Ref. Collection Principle and Criteria	*Extra intelligence*
4.0 The entity collects personal information only for the purposes identified in the notice.	
4.1 Policies and Communications	
4.1.0 **Privacy Policies** The entity's privacy policies address the collection of personal information.	
4.1.1 **Communication to Individuals** Individuals are informed that personal information is collected only for the purposes identified in the notice.	
4.1.2 **Types of Personal Information Collected and Methods of Collection** The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	
4.2 Procedures and Controls	
4.2.1 **Collection Limited to Identified Purpose** The collection of personal information is limited to that necessary for the purposes identified in the notice.	
4.2.2 **Collection by Fair and Lawful Means** Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (*a*) fairly, without intimidation or deception, and (*b*) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	
4.2.3 **Collection From Third Parties** Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	
4.2.4 **Information Developed about Individuals** Individuals are informed if the entity develops or acquires additional information about them for its use.	

5.2.9 USE, RETENTION, AND DISPOSAL

Ref. Use, Retention, and Disposal Principle and Criteria	*Extra intelligence*
5.0 The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.	
5.1 Policies and Communications	
5.1.0 **Privacy Policies** The entity's privacy policies address the use, retention, and disposal of personal information.	

5.1.1 **Communication to Individuals**

Individuals are informed that personal information is (*a*) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (*b*) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (*c*) disposed of in a manner that prevents loss, theft, misuse, or unauthorized access.

5.2 Procedures and Controls

5.2.1 **Use of Personal Information**

Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.

5.2.2 **Retention of Personal Information**

Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.

5.2.3 **Disposal, Destruction and Redaction of Personal Information**

Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.

When a SaaS deployment is removed, this can be managed or executed from within the tool. The tool then also takes care of correct disposal of all personal information.

5.2.10 Access

Ref.	***Access Principle and Criteria***	***Extra intelligence***
6.0	**The entity provides individuals with access to their personal information for review and update.**	
6.1	**Policies and Communications**	
6.1.0	**Privacy Policies** The entity's privacy policies address providing individuals with access to their personal information.	
6.1.1	**Communication to Individuals** Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.	Access can be granted using the tool. If the tool is aware of the location and authentication mechanisms for the mentioned individuals, the tool can manage the review, update and correct procedures.
6.2	**Procedures and Controls**	
6.2.1	**Access by Individuals to Their Personal Information** Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	See 6.1.1
6.2.2	**Confirmation of an Individual's Identity** The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	See 6.1.1
6.2.3	**Understandable Personal Information, Time Frame, and Cost** Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	
6.2.4	**Denial of Access** Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	
6.2.5	**Updating or Correcting Personal Information** Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	See 6.1.1

6.2.6 **Statement of Disagreement**

Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.

5.2.11 Disclosure to Third Parties

Ref.	*Disclosure to Third Parties Principle and Criteria*	*Extra intelligence*
7.0	**The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.**	
7.1	**Policies and Communications**	
7.1.0	**Privacy Policies** The entity's privacy policies address the disclosure of personal information to third parties.	
7.1.1	**Communication to Individuals** Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.	
7.1.2	**Communication to Third Parties** Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.	
7.2	**Procedures and Controls**	
7.2.1	**Disclosure of Personal Information** Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.	
7.2.2	**Protection of Personal Information** Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	
7.2.3	**New Purposes and Uses** Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	
7.2.4	**Misuse of Personal Information by a Third Party** The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	These incidents can be managed using the incident management system inside the tool.

5.2.12 Security for Privacy

Ref.	*Security for Privacy Principle and Criteria*	*Extra intelligence*
8.0	**The entity protects personal information against unauthorized access (both physical and logical).**	
8.1	**Policies and Communications**	
8.1.0	**Privacy Policies** The entity's privacy policies (including any relevant security policies), address the security of personal information.	
8.1.1	**Communication to Individuals** Individuals are informed that precautions are taken to protect personal information.	
8.2	**Procedures and Controls**	

8.2.1 **Information Security Program**

A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas [fn 1] insofar as they relate to the security of personal information:

a. Risk assessment and treatment [1.2.4]
b. Security policy [8.1.0]
c. Organization of information security [sections 1, 7, and 10]
d. Asset management [section 1]
e. Human resources security [section 1]
f. Physical and environmental security [8.2.3 and 8.2.4]
g. Communications and operations management [sections 1, 7, and 10]
h. Access control [sections 1, 8.2, and 10]
i. Information systems acquisition, development, and maintenance [1.2.6]
j. Information security incident management [1.2.7]
k. Business continuity management [section 8.2]
l. Compliance [sections 1 and 10]

8.2.2 **Logical Access Controls**

Logical access to personal information is restricted by procedures that address the following matters:

a. Authorizing and registering internal personnel and individuals
b. Identifying and authenticating internal personnel and individuals
c. Making changes and updating access profiles
d. Granting privileges and permissions for access to IT infrastructure components and personal information
e. Preventing individuals from accessing anything other than their own personal or sensitive information
f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities
g. Distributing output only to authorized internal personnel
h. Restricting logical access to offline storage, backup data, systems, and media
i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)
j. Preventing the introduction of viruses, malicious code, and unauthorized software

Restricting and allowing access can be managed from inside the tool automatically by managing users, assigning roles, linking to external systems, managing access profiles. Automated virus updates will cover for item j.

8.2.3 **Physical Access Controls**

Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).

8.2.4 **Environmental Safeguards**

Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.

8.2.5 **Transmitted Personal Information**

Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other nonsecure networks, and wireless networks is protected by deploying industry standard encryption technology for transferring and receiving personal information.

8.2.6 **Personal Information on Portable Media**

Personal information stored on portable media or devices is protected from unauthorized access.

8.2.7 **Testing Security Safeguards** — Tests of logical access can be executed automatically.

Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.

5.2.13 QUALITY

Ref.	*Quality Principle and Criteria*	*Extra intelligence*
9.0	**The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.**	
9.1	**Policies and Communications**	
9.1.0	**Privacy Policies** The entity's privacy policies address the quality of personal information.	
9.1.1	**Communication to Individuals** Individuals are informed that they are responsible for providing the entity with accurate and complete personal information, and for contacting the entity if correction of such information is required.	
9.2	**Procedures and Controls**	
9.2.1	**Accuracy and Completeness of Personal Information** Personal information is accurate and complete for the purposes for which it is to be used.	
9.2.2	**Relevance of Personal Information** Personal information is relevant to the purposes for which it is to be used.	

5.2.14 MONITORING AND ENFORCEMENT

Ref.	*Monitoring and Enforcement Principle and Criteria*	*Extra intelligence*
10.0	**The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.**	
10.1	**Policies and Communications**	
10.1.0	**Privacy Policies** The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.	
10.1.1	**Communication to Individuals** Individuals are informed about how to contact the entity with inquiries, complaints and disputes.	
10.2	**Procedures and Controls**	
10.2.1	**Inquiry, Complaint, and Dispute Process** A process is in place to address inquiries, complaints, and disputes.	This can be handled by the incident management system inside the tool
10.2.2	**Dispute Resolution and Recourse** Each complaint is addressed, and the resolution is documented and communicated to the individual.	This is handled by the incident management system
10.2.3	**Compliance Review** Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements, and other contracts is reviewed and documented, and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	
10.2.4	**Instances of Noncompliance** Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	
10.2.5	**Ongoing Monitoring** Ongoing procedures are performed for monitoring the effectiveness of controls over personal information, based on a risk assessment [1.2.4], and for taking timely corrective actions where necessary.	Monitoring can be (partly) implemented using the tool by automatically and periodically analyzing and inspecting the audit trail and other logs

Footnotes (Security for Privacy):

fn 1 These areas are drawn from ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at http://webstore.ansi.org/ and in Canada from the Standards Council of Canada at www.standardsstore.ca/eSpecs/index.jsp. It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy *Generally Accepted Privacy Principles*' criterion 8.2.1. The references associated with each area indicate the most relevant *Generally Accepted Privacy Principles'* criteria for this purpose.

5.2.15 EXTRAS FROM ISAE 3402

The policies above are literally the policies from SOC 2. The following policies are taken from the self-created ISAE 3402 compliance requirements, which can be found in appendix A. In section 4.2.2 it is described which policies should be appended to this list and why. The table below is the same table as in section 4.2.2, extended with the extra intelligence column.

Policy in SaaS Security Framework	Difference with SOC 2	Extra intelligence
8.1.3.1.2	Notice of policies on password strength	If user management is done via the tool, passwords can be random generated or checked for strength.
8.1.3.1.3	Policy that user accounts are personal and non-transferable	
8.1.7.1.4	Notice of response time policies in the incident management process	This is handled by the incident management process inside the tool
8.1.8.1.1	Policies that there should be backup engineers available for peak moments or huge downtime situations and the response time of these engineers	If staff planning is done via a workflow process in the tool, these extra requirements can be enforced too.
8.1.8.1.3		
8.1.10.1.1	Policies about the internal communication system: new employees should get a training and the system should allow for easy searching through historical communication	If the tool is linked with the HRM system, it can automatically check whether all employees have had their training.
8.1.10.1.3		
8.1.10.2.1		
8.1.11.1.1	Notice of policies for external communication	
8.1.11.3.1	Notice of policies on response times of external communication	Response times on external communication can be monitored by checking log files, audit logs etc. If the external communication is done via the incident manager, response times can be enforced and easily monitored by analyzing the audit log.
8.1.12.1.1	Notice of policies on frequency, location and contents of backups	
8.1.12.2.1	Notice of policies on backup integrity; testing backups frequently and how to respond to failed backups	If backups are executed automatically by the tool, it will notice when a backup has failed. When this happens, tasks can be executed to inform engineers or management.
8.1.12.2.2		
8.1.12.2.3		

8.1.12.3.1	Notice of policies on the status of backups	The tool can give an overview of the status of the last backups, if the tool is responsible for the backup process
8.1.16 (whole chapter)	Notice of the existence of a Terms and Conditions document	
8.1.17 (whole chapter)	Notice of the existence of a Usage Policy document	
8.1.19.1.1	Policies on the existence, use and regular review of a non-disclosure agreement for employees	The process of reviewing and communicating can be implemented as a workflow process in the tool.
8.1.19.2.1		
8.1.19.3.2		

TABLE 6: EXTRA POLICIES BASED ON ISAE 3402 + EXTRA INTELLIGENCE

5.3 INTELLIGENCE IN PRACTICE

If we gather all the extra requirements that our requested extra intelligence asks, we get the following list of requirements for maximum automation:

- **Links to external systems**. For many purposes, links to external systems are necessary. Not just the SaaS solution that is being checked, but also connection to the operating system and other hardware systems is necessary to authorize users or import user data, check for virus scanner updates, execute backups, inspect audit trails and log files of other systems, etcetera. The exact technical implementation is not important here, that can be using web services, using direct access to the database or using a specific custom-built interface;
- **Central user management**. It would be easiest and best if the security checking tool would handle all user management. As that is not always possible when considering external solutions, the tool should have access to the user management functions of the SaaS solutions it checks;
- **Sending emails**. Several tasks involve sending emails automatically. Not all workflow management systems support that out-of-the-box;
- **Incident management**. If the tool contains a system or process to handle incidents, requests, problems and security breaches, it can cover many aspects of the framework. The audit check for all these policies covered by the incident management system then only involves checking whether the incident management system worked and what exceptions the incident management system noticed, like late response times;
- **Create extra processes**. We cannot just use an audit manager as mentioned in section 5.1. It is necessary to develop and implement specific processes, sometimes framework-wide, sometimes customer-specific. Using these processes gives certainty and the possibility to audit using analysis of the audit logs;
- **User authentication**. If the tool does central user management, it can also perform as central user authentication. Apart from the ease of use for users (one login for multiple systems, possibly), it also allows the tool to keep a closer eye on the users entering the systems and accessing the data;
- **Deploying and un-deploying SaaS environments**. Whether for DTAP or for a new or existing customer, if the tool is responsible for deploying and removing SaaS environments, it always has overview of the current systems that are “live”. This information can be used to identify potential threats like privacy-sensitive data in a developer environment. The tool can then automatically anonymize the privacy-sensitive data such that the entity holds compliance with the framework;
- **Random password generator**. It’s a relatively small item on this list and not absolutely necessary, but if users are centrally managed, a random password generator is needed. Not all workflow management systems deliver this out-of-the box.

This list directly implies extra requirements to the SaaS solution that is being checked:

- Having suitable interfaces such that the security tool can get/set the information it needs
- Maintaining a log such that historical data can be found and possible security breaches can be detected (for example a log with all users entering the data center)

The items on the list with extra requirements to the checking tool can be solved by requiring 3 general principles:

- **Creating new processes**; this allows for modeling and implementing all the extra tasks that have to be created, but also for incident management;
- **Links to external software**; either via web services or via direct database connection, this allows to read and edit data in other solutions, either hosted locally or remotely;
- **Shell or command line access and programming skills**; if a random password generator is not included, it has to be built manually, deploying and removing SaaS environments can probably not be done without shell access.

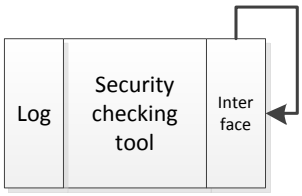
Do tools exist that offer these three principles plus the basic workflow management tasks as defined in the last paragraph of section 5.1?

Yes. For example the aforementioned YAWL has all this functionality built-in. Also the Grexxboxx by Grexx knows all this functionality; we will focus on that later.

5.4 SECURITY OF THE CONTINUOUS ASSURANCE TOOL

When creating a tool for SaaS security, it's important that the tool itself is secure too. Especially as it has access to the core data of the system (including user credentials, for example), abuse should be prevented and all communication channels have to be secure. In other words: the security tool should comply with the same requirements as the tool it checks.

This can be achieved in a number of ways. An external auditor can investigate the tool and judge whether it's secure. Although some customers of the tool will require that, it's exactly that manual auditing that we wanted to avoid and that doesn't bring the continuous assurance we are looking for. Isn't it possible that the security of the security checker is checked by an automated tool? This brings us back where we started. Without getting into deep circular arguments, what if it's possible to use the security checker to check its own security?



Using the rules of mathematical induction, we can get to the continuous assurance this way. Appliance of induction on proposition P has 2 requirements:

1. At t = 0 validity P has to be proven valid
2. It has to be proven that if P is valid on t = N, P is also valid on t = N+1

Conformity with both requirements proves that P is valid for every t >= 0.

If we take the proposition P being:

The security checking tool is secure

we just need external auditors to prove the two requirements above. Once they have proven that, and we make no changes that could influence the security, the security checking tool is secure. Continuously. The tool can monitor its own security and in case a security policy break shows up, security assurance has to be re-established. Given the auditing reports from the past and the audit log from the system itself, this shouldn't be a big problem though.

Another possible security issue is the use of communication channels towards the systems to check. It has to be ensured that these channels are secure.

5.5 BUILDABILITY OF THE TOOL

This section answers research question 3, whether the requirements that we derived in section 5.3 are feasible and whether a tool with such requirements is buildable. Given the fact that we have given 2 existing tools that are able to each meet all the requirements, it can be easily concluded that such a tool is buildable.

6 GREXXBOXX AS SAAS SECURITY THERMOMETER

In this chapter we will discuss the practical aspect of this research where the Grexxboxx is tested as a prototype of the security checking tool as described in the previous chapters. First we will take a look at what the Grexxboxx is, what it can do and cannot do and how it can be positioned. Next, we see how continuous assurance can be implemented using the Grexxboxx platform. To really create the prototype, we implement an important example process in the Grexxboxx.

6.1 (IM)POSSIBILITIES OF THE GREXXBOXX

The Grexxboxx is a workflow platform capable of handling all kinds of workflow processes. Each task can be required, optional, system-executed, assigned, calling another script, output to another task, getting input from another task, getting input from the user, giving output to the user, etc. Next to that, it keeps a complete audit trail, logging every step a user or the system makes in the system. So how does the Grexxboxx perform when we compare it to the list of needs for the most intelligent version of the security checking tool from section 5.3?

Links to external systems	Yes, communication with external systems is possible, sometimes via a custom system service
Central user management	Yes, this is possible, given the links to external systems
Sending emails	Yes, the Grexxboxx has a mailer service that sends an email
Incident management	Yes, this is a process that can be created in the Grexxboxx, see section 6.3
Create extra processes	Yes, this is possible
User authentication	Yes, via a custom system service
Deploying and un-deploying SaaS environments	Yes, via a custom system service[24]
Random password generator	Yes, via a custom system service

TABLE 7: INTELLIGENT TOOL REQUIREMENTS ON THE GREXXBOXX

When looking at this table, we can see that the Grexxboxx supports all of these requirements. Not all requirements are natively supported, but it has extensive support for creating custom “system services”. A system service is a Stored Procedure in the MSSQL database with a user-defined input and a user-defined output. MSSQL stored procedures are capable of running batch scripts and interpreting the output. This can be done by calling the `xp_cmdshell` T-SQL Stored Procedure. (Microsoft, 2011)

With that technology in mind, the Grexxboxx qualifies as a security checking tool, complying with all the requirements mentioned in section 5.3.

For more information on the Grexxboxx and its architecture, see (van Roy, 2010)

6.2 CONTINUOUS ASSURANCE IN THE GREXXBOXX

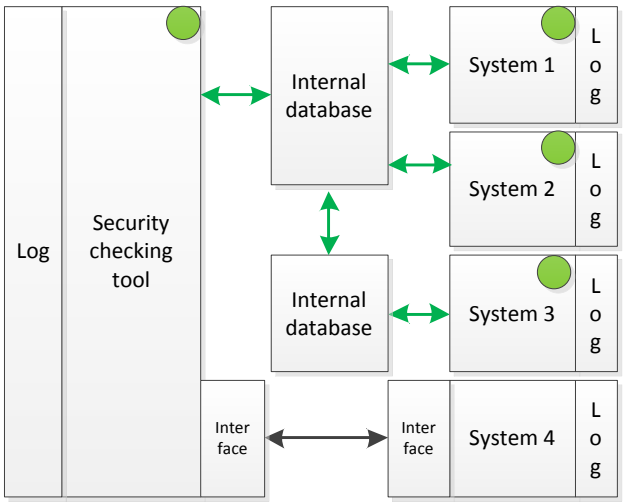
Section 5.3 has shown that systems can be created to support achieving and maintaining compliance with the SaaS Security Framework. Section 5.3 also gave a list of requirements this supporting system (“security checking system”) needs to meet. Section 5.4 shows that the security of the security checking system has to be taken seriously and that it could be possible that the security checking system checks itself. Communication channels between the security checker and the entity’s systems still have to be checked. Section 6.1 shows that the Grexxboxx meets all the requirements of section 5.3, but how about those communication channels and will this really deliver **continuous** assurance?

[24] This is currently being developed at Grexx with succesful results

Let's first look at those communication channels. The Grexxboxx itself requires the use of an SSL HTTP connection (HTTPS) for users to interact with the Grexxboxx. The database is usually hosted on the same physical server as the Grexxboxx application, so that connection can be considered secure. Sometimes communication is needed between Grexxboxxes. As all the data of the Grexxboxx is inside its database, a connection between the two database servers is enough. but as all the (production) servers are in the same data center, these are connections over the internal network of SaaSplaza with only private IP addresses, so this will never reach the internet. SaaSplaza has its SAS 70 compliance checked yearly, which means that these connections can also be considered secure.

Connections within and between Grexxboxxes and between Grexxboxx and user are secure, but what about connections between a Grexxboxx and another computer system? That is of course a question that has to be addressed per situation.

If we take a look at the diagram on the right, we can see a schematic view of the situation. The systems with a green circle are Grexxboxx systems and the green arrows are secure connections. The security checking tool and systems 1 and 2 use the same database server. This usually means that they are also on the same physical server, and if that's not the case, the connection between application and database uses an internal SaaSplaza connection, which is secure too. System 3 is on another (database) server, but given the SaaSplaza compliance with SAS 70, all the connections between system 3 and the security checker are secure too. System 4 is an external system. For this it can't be defined yet whether it's secure. Also, a special interface probably has to be created to be able to communicate with each other.



This answers the question about the secure communication channels. Now we will focus on the other question from the introductory paragraph: can the Grexxboxx really establish **continuous** assurance?

To answer the question, we have to check the 3 aspects of assurance according to chapter 3.8:

1. Capturing information by the company under assurance
2. Monitoring and analyzing the information by the assuror to ensure the reliability of the information
3. Communicating the outcome of the assurance engagement by the assuror

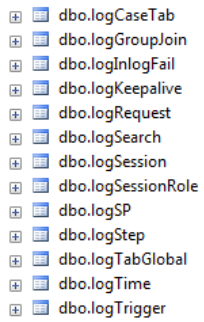


FIGURE 5: GREXXBOXX LOG TABLES

The Grexxboxx logs every action of a user. It will be a relatively easy job to capture the necessary information from another Grexxboxx as all the information will be available, but just has to be filtered and maybe reformatted. If the Grexxboxx should confirm assurance on a non-Grexxboxx system, it all depends on the amount of data the source system can give. Item 1 is therefore relatively easy at other Grexxboxx instances, but can get more difficult on other systems. However, once this interface has been created and the access to the target system has been granted, it's possible for the security checking Grexxboxx to capture the necessary data. By doing that at a certain interval, this item of continuous assurance can be considered covered.

Item 2 will involve creating processes in the Grexxboxx and having them executed (automatically) every X minutes/hours/etc. Analysis can be done in an automated way or a (required) task (with a deadline) can be assigned to an employee. This task can then show the employee the necessary data and the employee has to decide whether a

certain rule has been violated. If this is done with regular intervals, this item of assurance is covered in a continuous way.

Item 3 is a matter of data reformatting. The complexity depends on the way the output should be formatted and the amount of information it should contain. If it's simply a "yes" or "no" answer to the question "has this system been secure the past X days", this can be an automated task that gathers all input from previous tasks and delivers a result to the management or responsible individuals. If some extra management information should be included (Where did it go wrong? What were average response times?), this information has to be retrieved. As this information was needed already to come to the final judgment on security of the system, the security checking Grexxboxx has the information already and simply has to process it. So yes, the Grexxboxx is capable of handling this as well. Next to that, the Grexxboxx uses some Java/Flash libraries to create interactive "dashboards": web pages with management information shown in graphs or tables. This shows that the Grexxboxx is capable of implementing monitoring in both engineering-friendly as well as management-friendly ways. Unfortunately, due to customer-sensitive information, it's not possible to show an example of such a dashboard here.

To summarize this subchapter, we can take a look at the table below. The rows represent the four aspects studied in this section. The columns represent whether the security checking tool checks a Grexxboxx or a non-Grexxboxx system.

	Grexxboxx	Non-Grexxboxx
Communication channels	Secure	To be determined
Capturing information	Easy	Depends on the system and the interface
Monitoring and analyzing information	Possible	Possible
Communicating the outcome	Possible	Possible

TABLE 8: CONTINUOUS ASSURANCE PROPERTIES COMPARISON

It can be concluded that the Grexxboxx as security checking system is capable of providing continuous assurance, but it is best at providing continuous assurance at other Grexxboxx instances. It has functionality built-in to communicate and get data from other Grexxboxx instances already, which makes it easy to collect the information necessary for continuous assurance.

6.3 ITIL PROCESSES IN THE GREXXBOXX

To completely validate that the Grexxboxx is indeed a good security checking system, we would have to implement all processes and policies of the SaaS Security Framework in the Grexxboxx. Given the length of the framework this is a very time-consuming task that would take a relatively too large effort for this research. Therefore we have chosen to implement one ITIL (version 3) process to demonstrate the possibilities of the Grexxboxx. ITIL processes are based on best practices and ITIL processes are incorporated in companies all over the world. Big multinationals like Microsoft, HP and Disney use ITIL, but also smaller and medium-sized companies have implemented them (Cartlidge, et al., 2007). ITIL is not specifically aimed at our goal (nor security nor SaaS/cloud), but it delivers a library of standard processes that is very useful and forms a firm base, because of its widespread use and adoption.

If the Grexxboxx is capable of implementing and supporting an ITIL process, it at least supports the implementation of what is widely considered to be best practice in this field. It is neither possible to document, collect nor demonstrate all possible exceptions. Implementation of an ITIL process implies covering the widely most accepted model, always with the specific situation in mind.

We have chosen the process of incident management, as documented before by (van Roy, 2010). We have chosen this process as it is in the Service Operation stage of the IT Services Lifecycle (Cartlidge, et al., 2007), which means it's in the phase where the actual value to customers is delivered. That makes it an important process. It's also mentioned in all different chapters of SOC 2, which emphasizes again the importance of incident management.

We have converted the text-based model of (van Roy, 2010) into a process workflow diagram in Grexxboxx-terms. This model can be seen in Figure 6; a larger version of this image is found in PDF format on http://bit.ly/grexxIMmodel.

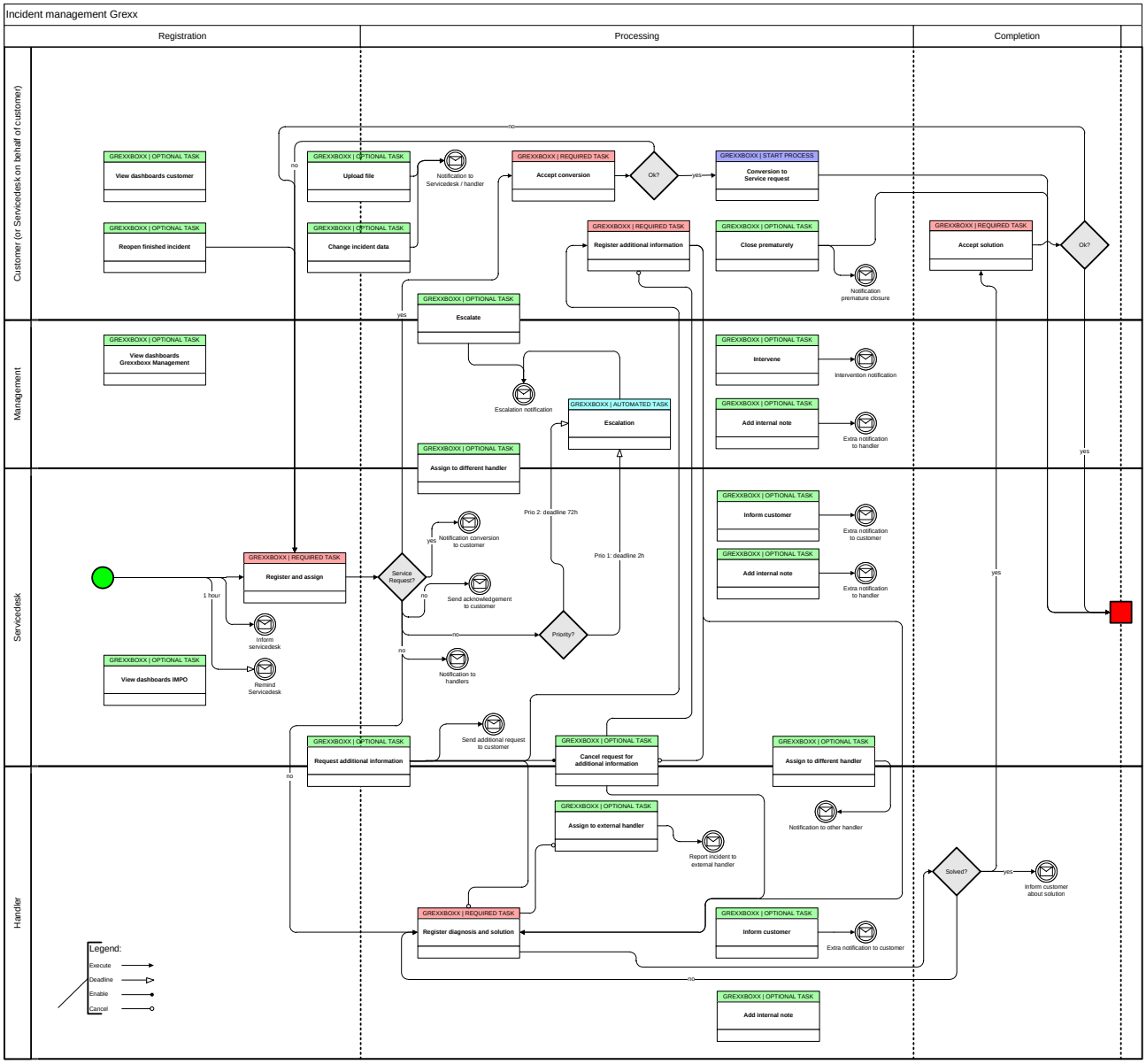


FIGURE 6: INCIDENT MANAGEMENT MODEL

The red tasks indicate a required task, the green tasks an optional task and the horizontal and vertical swim lanes indicate respectively who can execute a task and in which stage of the process the tasks can be started.

The light blue tasks indicate an automated system task, for example after a certain period of time escalating the incident to higher management.

The dark blue tasks indicate the start of another process, in this case starting a change request.

The diamonds indicate a choice and the circles with an envelope indicate sending a message. The process starts at the green circle and ends at the red square.

Finally, there are four different arrows; the normal closed arrow indicates triggering a required task (“execute”), the open arrow indicates triggering a task after a certain period of time (“deadline”). The line with a closed black dot at the end indicates enabling an optional task so that it can (but doesn’t have to) be executed by the respective actor(s). The line with the open dot at the end indicates disabling an optional task so it cannot be executed anymore.

I have implemented this process in a Grexxboxx instance and it will be used in the soon-to-come release of the Grexx Incident Manager. It is difficult to show and prove this in a document like this, but using some screenshots might help. Note that the incident manager is implemented in Dutch.

The overview page of an incident in the incident manager looks like this:

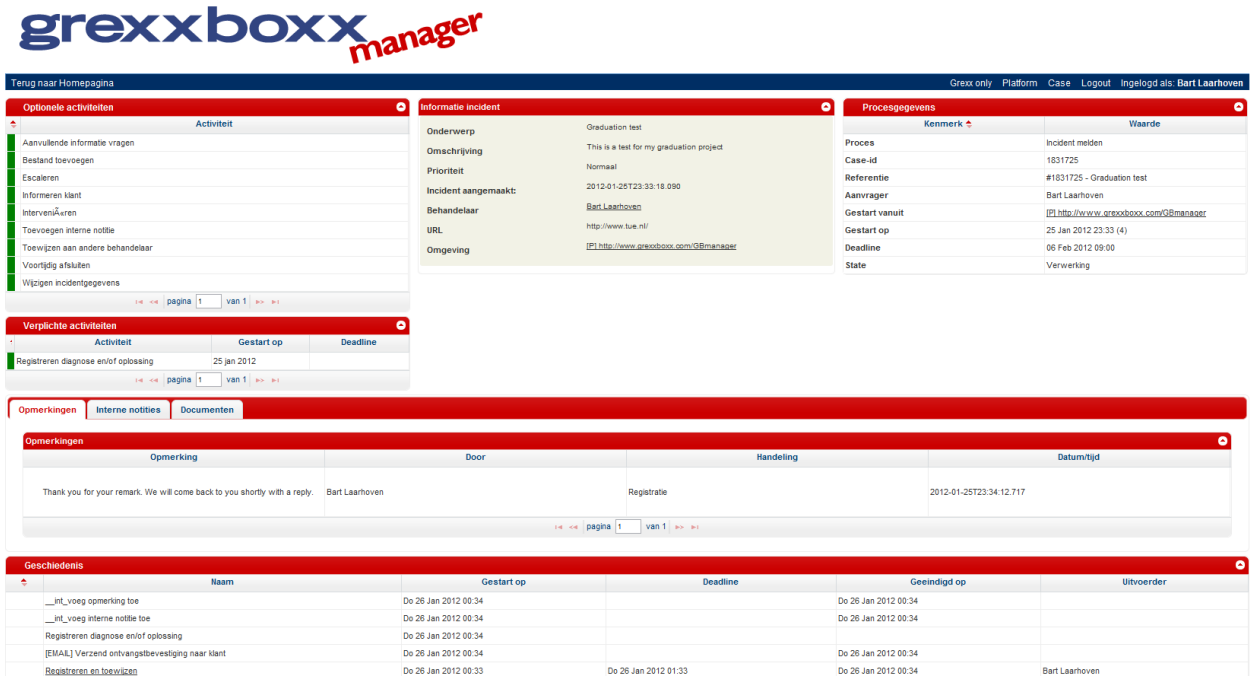


FIGURE 7: GREXX IM: OVERVIEW OF A CASE

As this picture is too small to see something, we will pick out the most important parts, starting with the two blocks underneath each other at the top left, which contain the current optional and required activites. We are logged in as a user with all the possible roles, to show the complete implementation. The process has started and just finished the task “Register and assign” (“Registreren en toewijzen” in Dutch) and the servicedesk has established that the current incident does not involve a service request. Therefore we now see the following tasks, which can easily be mapped to the English counterparts in the model.

FIGURE 8: GREXX IM: ACTIVITIES READY TO BE STARTED

The block in the middle top row shows some general information about the current incident:

FIGURE 9: GREXX IM: CASE INFORMATION

The block at the bottom shows the audit trail, of which a small part is shown here. All tasks, either automatically executed by the system or manually executed by a user, are shown here. It is possible to hide some of these tasks from the audit trail, but for the sake of showing everything, we did not do that here. Other columns in the audit trail are the start date, deadline, finished date and the actor.

FIGURE 10: GREXX IM: AUDIT TRAIL

The two tasks labeled "[EMAIL]" concern sending a message. Either to the servicedesk that a job is waiting for them, or to the customer that the incident has been received. As user with both roles (servicedesk and customer), we get both mails:

FIGURE 11: GREXX IM: MAIL TO SERVICEDESK

FIGURE 12: GREXX IM: MAIL TO CUSTOMER

Next tasks would be for example to request additional information from the customer, add a document to the current case or assign this case to another person. Screenshots of those tasks follow below.

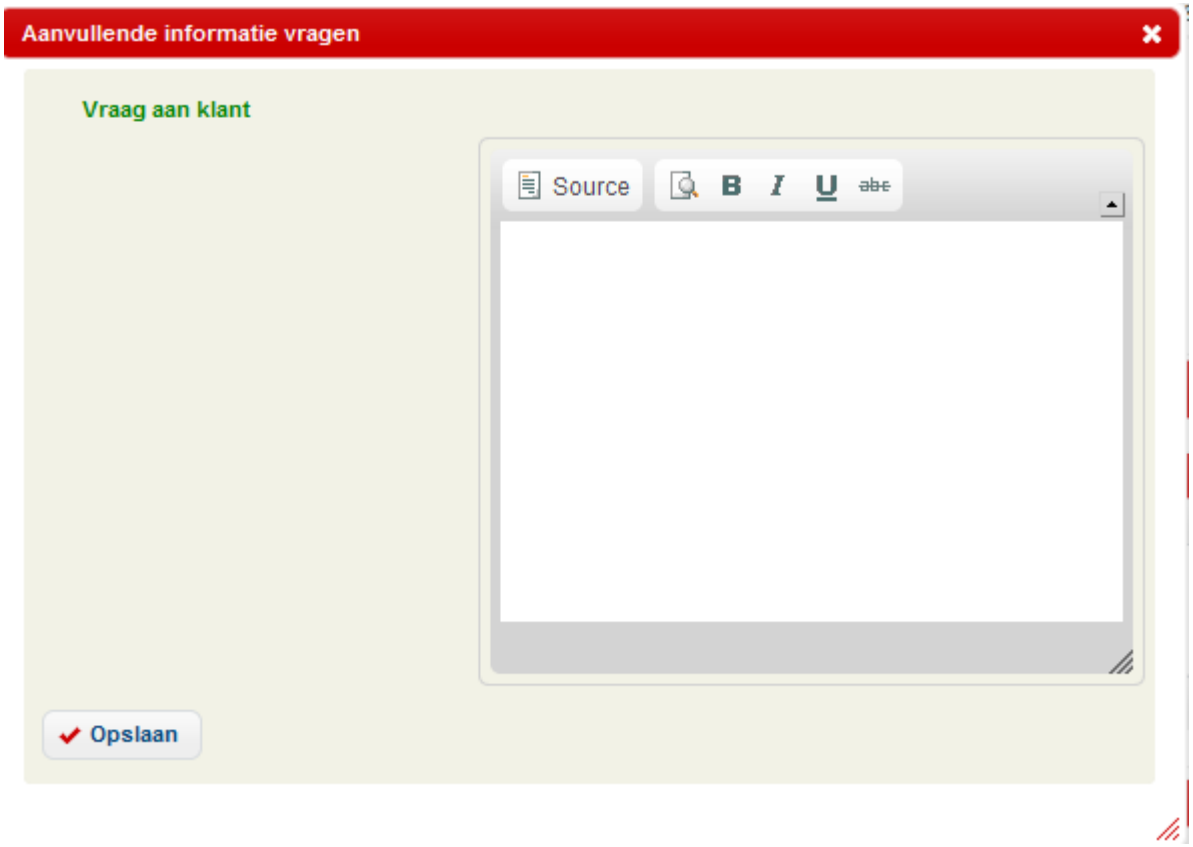


FIGURE 13: GREXX IM: REQUEST ADDITIONAL INFORMATION

FIGURE 14: GREXX IM: ADD/UPLOAD FILE

FIGURE 15: GREXX IM: ASSIGN TO SOMEONE ELSE

This implementation shows that the Grexxboxx is capable of handling an implementation of an ITIL process. This specific ITIL process is important for the tool I'm demonstrating by implementing the process.

6.4 GREXXBOXX AS CONTINUOUS ASSURANCE TOOL?

Chapter 5 has given the requirements for a tool such that it can be used to automatically check the requirements from the SaaS Security Framework. Section 5.4 shows that it might be possible that the tool takes care of its own security, if certain preconditions are met and the 2 requirements of induction are checked. Section 6.1 shows that the Grexxboxx qualifies as a security checking tool as it complies with all the requirements from chapter 5. Section 6.2 shows that the Grexxboxx is also capable of handling **continuous** assurance, although it's easier for a Grexxboxx to investigate another Grexxboxx than to investigate a non-Grexxboxx system. The limitations on the capabilities are at the other system, though. Section 6.3 shows by demonstration/prototyping that the Grexxboxx is indeed capable of implementing processes that are needed to become a security checking tool, thereby validating the conclusions of sections 6.1 and 6.2.

7 DISCUSSION

One of the big advantages of using SaaS solutions, for the SaaS customers, is that they explicitly don't have to worry about the technical details anymore and can just use the software they always wanted to use, wherever they are. For the SaaS customers all that counts is that the functionality is working as expected. How the SaaS provider does that, where they host it and how they monitor it is not the SaaS customer's concern anymore. This gives the SaaS provider a lot of opportunities to improve efficiency and cut costs if he does his business the right way.

Although the SaaS customer is not interested in the technical details of the solution he's using, he does want to make sure that his data is secure, that the service uptime will be as expected, and that the privacy of the data he puts into the cloud is respected. But, as it involves a SaaS solution here, it doesn't matter whether the SaaS solution has big memory leaks, uses a lot of network traffic in the backend, or which type of encryption it uses; the SaaS customer will never have to deal with that side of the product anyway. The "security" as defined in this report therefore does not involve typical software security measurements. The security does not concern source code checks, fake hacker attacks, profiling software to show memory leaks or database (structure) analyses. But this has never been the plan; this type of security is (apparently) not requested by SaaS customers. That security more concerns the processes around the SaaS solution: "it doesn't matter how they do it, as long as they can show that they take care of it".

The problem I have defined at the beginning of my research, together with Grexx, was to research (as far as possible automated and continuous) compliance with SAS 70, which was at that moment the main applicable standard. SAS 70 is very known in the industry and widely seen as one of the best ways to guarantee that a cloud-oriented solution is secure. SAS 70, just like ISAE 3402 and SSAE 16, is based on the thought expressed at the end of the previous paragraph. This makes these standards usually "vague" and "hardly scientific", especially for computer scientists. On the other hand, it gives both provider and customer a safe feeling if the provider can show his compliance with one of the mentioned standards. This has been a dilemma that I've had to balance during this research. I was developing a solution based on a very vague and arbitrary standard, but it was a good thing as the industry can profit very much from a concrete solution.

I believe I diminished the vagueness of one of the vaguest standards, ISAE 3402, by creating a concrete framework with concrete requirements. Then, after having created this framework and having done the major part of my literature research and the research planning, SOC 2 was released. I couldn't ignore that standard, as it stood for exactly what I was looking for. It did diminish the value of the concrete framework though, as it quickly appeared that SOC 2 was a more extensive and formally defined set of requirements. My research was overtaken by the AICPA. It was then decided to continue this research, while taking SOC 2 into account. The automation part was still to be done and was still useful with SOC 2 as a basis.

Some gaps are left untouched though. A complete library of (workflow) processes could be created to completely cover SOC 2, for example. Also, a more thorough review of SOC 2 could be executed. We now concluded that it's better than our own framework, which is based on ISAE 3402 and literature, but that doesn't mean SOC 2 is complete. Giving an answer to that question involves a complete new research though.

Also, this research's focus was from the start on SaaS solutions. SaaS is market leader and will continue to grow over the next few years, so security of SaaS solutions was the problem discussed in this research. Nevertheless, this research could be very applicable to PaaS, IaaS or even regular IT outsourcing or service organizations too. This was not researched here, as that was not necessary to solve our problem and would incur more research into those topics, but our feeling says it could be very well applicable to other areas too.

8 CONCLUSIONS

This research shows once again that cloud computing is “hot” but also relatively new. New standards focused on cloud computing are being developed at the moment (“hot” issues), while academic literature on this topic is hard to find (relatively new subject). Many companies are working with the cloud and writing whitepapers and articles about it, but academic literature is rare in this field.

Nevertheless, using literature and the best source on ISAE 3402 we could find: the ISAE 3402 standard itself, we came up with a list of requirements to which service organizations and SaaS solutions should comply in order to get a comparable level of secureness. Except from the fact that literature and the standard mention several topics that should be addressed, the exact interpretation and content of the topics are undefined. This means we had to come up with our own list, based on our own experiences, explanations from literature and an example SAS 70 report.

A newly introduced standard (SOC 2), which was introduced when we already started this research, shows again that cloud computing is a “hot” issue. Comparison with the list derived from ISAE 3402 and literature shows that the SOC 2 standard is more precise and complete. However, certain topics were not mentioned in the SOC 2 list and they should be added. The SOC 2 list, completed with some small additions from ISAE 3402 forms the SaaS Security Framework.

This whole SaaS Security Framework can be supported and partly automated using a software tool. With this software tool, we can give extra support or automation to over 58% of the items in our framework, almost 73% if we don’t count the privacy issues. This can lead to a save in auditing costs of over $ 60.000 a year.

One of the tools that can deliver the necessary extra support and automation is the Grexxboxx, a SaaS dynamic case-oriented workflow management platform by Grexx. Using the techniques of the Grexxboxx, this provides continuous assurance of the requirements and that means, in turn, continuous assurance of SOC 2 and ISAE 3402 by the Grexxboxx. Using induction, external audits of the Grexxboxx are only needed to a limited extent, while still ensuring continuous compliance. Using the model and internal communication possibilities of the Grexxboxx, other Grexxboxxes can be checked easily. To check non-Grexxboxx systems takes some extra effort, but the limitations are not dependent on the Grexxboxx.

This research also shows that cloud computing is not much more than selling existing technologies under a new name. Although the problem we faced was SaaS focused and we therefore took that point of view, probably 90% of the thesis is also applicable to regular software. We did not research that and explicitly used a SaaS focus, so that can be subject of some further research.

If we come back to the research questions defined in chapter 2, we can now answer them:

1. What is needed for a SaaS solution to be secure?
2. What requirements should be met by a software tool to ensure a SaaS solution’s security?
3. Are these requirements feasible? In other words: is such a tool buildable?
4. Is it possible to use the Grexxboxx as such a tool?

Research question 1 was answered in chapter 4, resulting in a SaaS Security Framework based on a merge from SOC 2 and our own list in appendix A. Research question 2 was answered in sections 5.1 to 5.4, by finding the highest possible level of automation for the SaaS Security Framework from chapter 4. Question 3 was answered in section 5.5, where examples from practice resulted in an easy “yes” to this question. Question 4 was answered in chapter 6, resulting in the conclusion that the Grexxboxx is capable of being the tool that is requested.

The validation of question 1 resulted in a highly improved framework by combining it with SOC 2. Validation of questions 2 and 3 were done by question 4 which showed a prototype. The validation of the pure requirements check of the Grexxboxx was executed by implementing a process.

This concludes my research.

REFERENCES

Alles Michael G., Kogan Alexander and Vasarhelyi Miklos A. Feasibility and Economics of Continuous Assurance [Journal] // Auditing: A Journal of Practice. - March 2002. - 1 : Vol. 21.

Alles Michael G., Kogan Alexander and Vasarhelyi Miklos A. Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems [Journal] // International Journal of Accounting Information Systems. - 2004. - pp. 183-202.

Alles Michael, Kogan Alexander and Vasarhelyi Miklos Black Box Logging and Tertiary Monitoring of Continuous Assurance Systems [Journal] // Information Systems Control Journal. - 2003. - Vol. 1.

American Institute of Certified Public Accountants AICPA Guide: Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) [Book]. - 2011.

American Institute of Certified Public Accountants SOC for CPAs [Online] // AICPA website. - July 27, 2011. - http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/CPAs.aspx.

American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements 16: Reporting on Controls at a Service Organization [Book]. - New York : [s.n.], 2010.

Arraj Valerie ITIL®: The Basics [Report]. - [s.l.] : TSO, 2010.

Barafort Béatrix, Di Renzo Bernard and Merlan Olivier Benefits Resulting from the Combined Use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL) [Report] / Centre for IT Innovation ; Centre de Recherche Public Henri Tudor, Luxembourg. - Berlin : Springer-Verlag, 2002. - pp. 314-325.

Cartlidge Alison [et al.] An Introductory Overview of ITIL® V3 [Book] / ed. Cartlidge Alison and Lillycrop Mark. - [s.l.] : The UK Chapter of the itSMF, 2007. - 0-9551245-8-1.

Chong Frederick and Carraro Gianpaolo Architecture Strategies for Catching the Long Tail. - [s.l.] : Microsoft Corporation, April 2006.

Cloud Security Alliance Cloud Controls Matrix [Online]. - http://www.cloudsecurityalliance.org/cm.html.

Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing v2.1 [Report]. - 2009.

CloudAudit Working Group A6 - The Automated Audit, Assertion, Assessment, and Assurance API [Online] // CloudAudit. - September 1, 2011. - http://www.cloudaudit.org.

Dignan Larry Cloud computing market: $241 billion in 2020 [Online] // ZDNet. - April 22, 2011. - http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702.

Farlex Control [Online] // The Free Dictionary. - Farlex, November 16, 2011. - http://www.thefreedictionary.com/control.

Gaskin Fiona Goodbye SAS 70, Hello ISAE 3402? [Article] // Accountancy Ireland. - June 2009.

Gaskin Fiona Roll Over, SAS 70. It's time for ISAE 3402 and SSAE 16 [Article] // Accountancy Ireland. - October 2010. - 5 : Vol. 42.

Gewald Heiko and Helbig Kay A Governance model for Managing Outsourcing Partnerships: A View from Practice [Conference] // 39th Hawaii International Conference on System Sciences. - [s.l.] : IEEE, 2006.

International Auditing and Assurance Standards Board (IAASB) International Standard on Assurance Engagements (ISAE) 3402: Assurance Reports on Controls at a Service Organization [Report]. - 2011.

Julisch Klaus and Hall Michael Security and Control in the Cloud [Journal] // Information Security Journal: A Global Perspective. - 2010.

Knolmayer Gerhard F. and Asprion Petra Assuring Compliance in IT Outsourcing Relationships: Frameworks and Selected Applications [Report]. - Bern, Switzerland : Institute of Information Systems, University of Bern.

KPMG Risk & Compliance Continuous Auditing en Continuous Monitoring: Levert het de beloofde voordelen op? [Report]. - Amstelveen : KPMG, 2010.

Le Clair Craig and Miers Derek Dynamic Case Management // The Forrester Wave / ed. Moore Connie and Magarie Andrew. - [s.l.] : Forrester Research, Inc., January 31, 2011.

Microsoft xp_cmdshell (Transact-SQL) [Online] // MSDN Library. - November 17, 2011. - http://msdn.microsoft.com/en-us/library/ms175046.aspx.

NEN Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2005,IDT) [Book] = NEN-ISO/IEC 27001 (nl). - Delft : Nederlands Normalisatie-instituut, 2005.

OED Control [Online] // Oxford Dictionaries. - November 16, 2011. - http://oxforddictionaries.com/definition/control.

Rezaee Zabihollah [et al.] Continuous Auditing: Building Automated Auditing Capability [Journal] // Auditing: A Journal of Practice & Theory. - [s.l.] : ABI/INFORM Global, March 2002. - 1 : Vol. 21. - pp. 147-163.

Roozendaal Wietse Op naar 'continuous assurance' [Article] // Spotlight. - [s.l.] : pwc, February 2011. - 1 : Vol. 2011. - pp. 12-16.

SaaSplaza Statement on Auditing Standards No.70 (Type II) For the SaaSplaza services [Report]. - 2011.

Schmidt Eric Inside Google [Interview]. - [s.l.] : National Geographic Channel, August 7, 2011.

Searcy DeWayne, Woodroof Jon and Behn Bruce Continuous Audit: The Motivations, Benefits, Problems and Challenges Identified by Partners of a Big 4 Accounting Firm [Conference] // 36th Hawaii International Conference on System Sciences. - [s.l.] : IEEE, 2003.

van der Aalst W.M.P. Business Process Configuration in The Cloud: How to Support and Analyse Multi-Tenant Processes? [Report]. - [s.l.] : Eindhoven University of Technology, 2011.

van Roy Dennis Incident Management in de Grexxboxx [Report]. - Eindhoven : [s.n.], 2010.

Vasarhelyi Miklos A., Alles Michael G. and Kogan Alexander Principles of Analytic Monitoring for Continuous Assurance [Journal] // Journal of emerging technologies in accounting. - New Jersey : [s.n.], 2004. - Vol. 1. - pp. 1-21.

Verweij Stefan SAS 70 maakt plaats voor ISAE 3402 [Artikel] // Spotlight. - [sl] : PricewaterhouseCoopers, October 2009. - Special IT & controls. - 3 : Vol. 2009. - pp. 52-56.

Wiegand, Jr. George SSAE 16, SAS 70 and ISAE 3402: Do You Know Your Number?. - [s.l.] : Crowe Horwath LLP, August 13, 2010.

TABLES

FIGURES

APPENDICES

9 APPENDIX A: LIST OF ISAE 3402 DEDUCTED REQUIREMENTS

9.1.1 DATA CENTER ENTRANCE

9.1.1.1 PREVENTION

1. The entity should take care of physical security systems to prevent unauthorized access to the data center
2. The entity should have policies in place to allow people access to the data center
3. The entity should have policies in place to disallow people access to the data center

9.1.1.2 DETECTION AND CORRECTION

1. The entity should have policies and technical facilities to detect unauthorized access to the data center
2. The entity should have policies in place on how to respond to unauthorized access to the data center

9.1.1.3 MONITORING

1. The entity should monitor access to the data center; unplanned or unauthorized visits to the data center should be logged and actively monitored

9.1.2 BACKUP LOCATION ENTRANCE

9.1.2.1 PREVENTION

1. The entity should take care of physical security systems to prevent unauthorized access to the backup location
2. The entity should have policies in place to allow people access to the backup location
3. The entity should have policies in place to disallow people access to the backup location

9.1.2.2 DETECTION AND CORRECTION

1. The entity should have policies and technical facilities to detect unauthorized access to the backup location
2. The entity should have policies in place on how to respond to unauthorized access to the backup location

9.1.2.3 MONITORING

1. The entity should monitor access to the backup location; unplanned or unauthorized visits to the backup location should be logged and actively monitored

9.1.3 USER AUTHENTICATION / USER MANAGEMENT

9.1.3.1 PREVENTION

1. The entity should have policies in place on creating, editing and deleting users on all their systems, applications and other fields where user authentication is needed
2. The entity should have policies in place on password strength
3. User accounts should be personal and non-transferable
4. The entity should have policies in place on who is granted the right to do user management as mentioned above

9.1.3.2 DETECTION AND CORRECTION

1. Any deviations of the policies should be detected and upon detection, action should be undertaken

9.1.3.3 MONITORING

1. The entity should have policies in place on how to monitor user authentication (i.e. once a year a full review of all user rights)

9.1.4 USER AUTHENTICATION / USER MANAGEMENT: OPERATING SYSTEM

See 9.1.3.

9.1.5 User authentication / user management: SaaS Application

See 9.1.3.

9.1.6 Data encryption

9.1.6.1 Prevention

1. The entity should have policies in place on how data is encrypted, both when stored i.e. in a database, and when transferred i.e. over the internet
2. The entity should have policies in place on how the backups are encrypted
3. The entity should have policies in place to assure that data needed to decrypt the data (i.e. private keys) is kept secure and safe

9.1.6.2 Detection and correction

1. Circumventions of data encryption should be noticed and these circumvention possibilities should be disabled

9.1.6.3 Monitoring

1. The entity has to monitor whether the data is still sent and stored encrypted

9.1.7 Incident management

9.1.7.1 Prevention

1. The entity should have an incident management system in place, preferably according to ITIL standards
2. The entity should enforce its employees to use this incident management system when registering and solving incidents
3. If the incident management system is directly available to customers, the entity should have policies in place on how customers should use it, including policies on access restrictions, communication about the existence of the system and availability of the system
4. The entity should have policies on handling incidents, i.e. response times and escalation procedures

9.1.7.2 Detection and correction

1. Incident reports that are received through different channels (i.e. telephone or e-mail) should be put into the incident management system (either manually or automatically)
2. Response times exceeding the limits set by the entity should be detected and action should be undertaken to both respond to this incident as soon as possible and to prevent exceeding this limit in the future

9.1.7.3 Monitoring

1. The availability of the incident management system should be monitored. In case of maintenance, all affected users should be informed
2. The entity management should have overview on (average) response times, customer satisfaction and numbers of incidents

9.1.8 Availability of engineers

9.1.8.1 Prevention

1. The entity should make sure that always enough engineers are available for possible peak moments; this can be achieved by having people stand-by, hiring more people etc.
2. Engineers should have had adequate training and education before starting their job
3. The entity should make clear what the required response time of engineers is in certain situations

9.1.8.2 Detection and correction

1. Guidelines should be available on how to respond to the sudden unavailability of engineers (i.e. hiring external freelance engineers)

9.1.8.3 MONITORING

1. The entity should take care of adequate training during the employment of engineers

9.1.9 MONITORING (CONTINUITY)

9.1.9.1 PREVENTION

1. Monitoring systems should be in place to monitor the core (business-critical) parts of the system
2. Monitoring systems should be in place to monitor the availability of the systems to users
3. The entity should decide on which monitoring systems should be placed on the non-business-critical parts of the system

9.1.9.2 DETECTION AND CORRECTION

1. The monitoring systems itself should be checked regularly for possible failures
2. Policies should be in place on how to respond to alerts from the monitoring system

9.1.9.3 MONITORING

1. Monitoring systems, if more than one, should monitor each other

9.1.10 COMMUNICATION: INTERNAL

9.1.10.1 PREVENTION

1. Every starting employee should be informed about how the internal communication system works
2. An internal communication system should be in place that is used for communication about production issues and continuity reports
3. The communication system should allow for easy searching through previous communication
4. Regular backups should be used of the data in this system

9.1.10.2 DETECTION AND CORRECTION

1. Policies should be in place to check and ensure that the internal communication system is used for internal communication

9.1.10.3 MONITORING

1. The entity should allow employees to notice and report problems and incompleteness of the communication system

9.1.11 COMMUNICATION: EXTERNAL

9.1.11.1 PREVENTION

1. The entity should have policies in place on external communication. This could for example contain disclaimer texts in emails, but also when and how a customer is redirected to an incident management system or which information can and cannot be disclosed to potential customers
2. The entity should have policies in place on response time, where necessary

9.1.11.2 DETECTION AND CORRECTION

1. The entity should respond to customer complaints in a decent way and undertake action where necessary

9.1.11.3 MONITORING

1. The entity should monitor response times
2. The entity should monitor the amount and source of customer complaints

9.1.12 Backups

9.1.12.1 Prevention

1. The entity should have policies in place on the frequency, location and contents of backups
2. The entity should have policies in place on who has access to the backups
3. The entity should have explicit policies in place on how to handle privacy sensitive data in backups

9.1.12.2 Detection and correction

1. In case of a failed backup, the responsible engineers should be informed
2. In case of multiple failed backups in a row (the entity management should define this number), the entity management should be informed
3. The consistency and correctness of the backups should be tested regularly, at least once every 100 backup cycles

9.1.12.3 Monitoring

1. The entity should have overview of recently executed backups and the status of them

9.1.13 Connectivity

9.1.13.1 Prevention

1. The entity should ensure connectivity of the cloud solution in both quantity and quality sufficient for average use
2. The entity should have abuse policies on how to respond to abuse of connectivity (e.g. spam)

9.1.13.2 Detection and correction

1. The entity should test the connection(s) regularly
2. The entity should be able to upgrade (or downgrade) the connectivity facilities as the needs change

9.1.13.3 Monitoring

1. The entity should monitor connectivity usage to monitor peak usage
2. The entity should monitor possible abuse of the connectivity and respond to it according to abuse policies

9.1.14 Fallback for peak moments

9.1.14.1 Prevention

1. The entity should have fallback capacity (extra servers, extra manpower, extra disk space, etc.) available for peak moments
2. The entity should have procedures on starting the fallback capacity
3. The entity should have policies in place on how and when to start these procedures

9.1.14.2 Detection and correction

1. When the regular capacity is updated (upgraded, downgraded, etc.), the fallback capacity should be reviewed too

9.1.14.3 Monitoring

1. The entity should test the procedures at least once a year

9.1.15 Incident management

See 9.1.7

9.1.16 Terms and conditions

9.1.16.1 Prevention

1. The entity should have terms and conditions in place to assure default values in customer contracts and prevent liabilities in default cases
2. The terms and conditions should be checked by an expert in regulations for possible leaks
3. The terms and conditions should be handed to the customer before signing a contract
4. The terms and conditions should be part of each contract signed

9.1.16.2 Detection and correction

1. Changes to the terms and conditions before signing a contract should be agreed upon by the management of the entity and agreed upon in writing by the customer
2. The entity should have policies in place on how to respond to a violation of the terms and conditions
3. The entity should have policies in place on how to detect violations of the terms and conditions

9.1.16.3 Monitoring

1. The entity should review the terms and conditions at least every two years and inform all customers of changes
2. The entity should, where possible, have monitoring systems in place to find violations of the terms and conditions

9.1.17 Usage policy

9.1.17.1 Prevention

1. The entity should have a usage policy in place to prevent the entity of liabilities when the service is used intentionally in a wrong way
2. The usage policy should be handed to the customer before signing a contract
3. The usage policy should be part of the contract or at least signed by the customer for agreement when signing a contract for a service

9.1.17.2 Detection and correction

1. The entity should register whether customers signed the usage policy
2. The entity should have policies in place on how to respond to a violation of the usage policy
3. The entity should have policies in place on how to detect violations of the usage policy

9.1.17.3 Monitoring

1. The entity should review the usage policy at least every two years and inform all customers of changes
2. The entity should, where possible, have monitoring systems in place to find violations of the usage policy

9.1.18 Privacy policy

9.1.18.1 Prevention

1. The entity should have a privacy policy stating how the company uses privacy-sensitive data of its customers (and the customers of its customers etc.)

9.1.18.2 Detection and correction

1. The entity should have policies in place to respond to complaints about violations of the privacy policy
2. The entity should check its own systems for possible violations every time a change in the privacy policy is made

9.1.18.3 Monitoring

1. The entity should review the privacy policy at least once every two years

9.1.19 Employees

9.1.19.1 Prevention

1. The entity should have a non-disclosure agreement (NDA) for its employees
2. Employees should have had adequate training before their employment

9.1.19.2 Detection and correction

1. The entity should register whether all employees signed the NDA

9.1.19.3 Monitoring

1. The entity should take care of sufficient training for its employees
2. The entity should review the NDA every two years

9.1.20 General

9.1.20.1 general

1. The entity management should be informed when substantial deviations of the policies take place
2. The entity management reviews, confirms and communicates the policies mentioned at least once a year
3. The entity management is responsible for application to these policies
4. The carve-out method is applicable to complying with these policies