Applying Security Assurance Cases for Cloud-based Systems in the Medical Domain

Bachelor of Science Thesis in Software Engineering and Management

Mohamad Drgham
Mohamed Hassan

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2020

A design science study presenting guidelines for creating security assurance cases in the cloud-based medical software service domain.

Supervisor: Jan-Philipp Steghofer, Mazen Mohamad
Examiner: Richard Berntsson Svensson

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2020

Applying Security Assurance Cases for Cloud-based Systems in the Medical Domain

Mohamad Drgham
Department of Computer Science and Engineering
Gothenburg University, Chalmers University of Technology
Gothenburg SE-41296, Sweden
gusdrgmo@student.gu.se

Mohamed Hassan
Department of Computer Science and Engineering
Gothenburg University, Chalmers University of Technology
Gothenburg SE-41296, Sweden
gushasmoi@student.gu.se

Abstract—**Regulatory compliance is of major concern to medical software companies that are involved in developing safety-critical software whose failure could result in loss of life, significant property damage or damage to the environment. A common approach to demonstrate compliance with safety requirements is through assurance cases, which are structured arguments, supported by evidence, intended to justify that a system is acceptably assured. The usage of assurance cases to prove compliance for other properties other than safety like cybersecurity has been increasing. However there are no formal guidelines to follow when creating security assurance cases as there is for safety assurance cases. The purpose of our research is to simplify the process of creating security assurance cases for their products by creating a set of guidelines. By conducting a design science study at a Swedish cloud-based medical software company, we analyzed external needs regarding the best practices in cybersecurity, regulations and standards in the medical domain. Contrasting these with the company's internal needs, we constructed a security assurance case for a part of their system based on the external and internal needs of the company. The guidelines were the outcome that emerged out of the case we created for the company.**

Index Terms—**SAC, ISO 27002, ISO 27018, HIPAA, artefact**

I. Introduction

In today's world almost every industry has been disrupted by software. As the world rapidly becomes more technology dependent it also leads to security vulnerabilities emerging [1]. There is a risk that a software's security vulnerabilities are exposed which can do severe damage to an organization's reputation, economy and in critical cases lead to loss of life [2]. The consequence of an increased amount of security breaches in technological systems is that governments increase legislation and regulations for security [3]. Especially in the medical domain, up until recent years manufacturers of medical devices were only required to prove that their device was safe and effective before putting it on the market [4]. But as medical technology is becoming more complex due to the increasing percentage of medical device functionality, tougher measures are required to ensure the security of patient data and safety. Organizations must demonstrate that their medical devices are secure by creating and implementing a security plan and finally by providing evidence that shows that their medical devices are free of vulnerability. This is known as creating a security assurance case (SAC) [5].

Assurance cases are structured arguments supported by evidence that are used to demonstrate confidence that a system meets certain requirements. They are similar to a legal case where claims made are supported by objective evidence for validity. A simple example of an assurance case is shown in Figure 1 to give readers an understanding of the structure of assurance cases. In the past assurance cases were mostly used in domains such as medical, aviation and automotive to address safety concerns for systems. However, today assurance cases are used in many industries to argue for properties such as security, safety, maintainability and reliability. A security assurance case argues the security of a system and takes people, processes and technology into consideration [7] [8].

Since security was not a major concern up until recent years, there are no formal guidelines to follow when implementing a security assurance case. However, security assurance cases need to be developed further and should be considered as highly important in the medical domain.

The objective of our study is to extract guidelines that can be used to construct security assurance cases, based on a case we create in the cloud-based medical software domain.

A set of guidelines will save companies time, reduce the complexity and simplify the process of creating security assurance cases for their products. It will be serving as a reusable artefact for cloud-based medical software organizations. The guidelines can be considered as a framework that includes external requirements such as standards, regulations, and best practices of cybersecurity both in general, and specifically in the medical domain. Examples of the general ones are the ISO 27000 series of standards in information security management systems [9] and General Data Protection Regulation GDPR [10]; domain-specific resources include, e.g., the Framework for Responsible Sharing of Genomic and Health-Related Data [11]. Companies can then build on top of this framework to fit their internal processes in order to create a security assurance case that can be integrated into their risk management procedures.

To create the guidelines we will study the external and internal needs of 1928 Diagnostics, a Swedish medical company that develops software to analyze the DNA of pathogens for antibiotic resistance. The guidelines will be derived from a security assurance case we create for the company. The company puts high value on ensuring the integrity and availability of confidential data they receive from customers. Therefore we will create a security assurance case covering data transfer between clients and 1928 Diagnostics cloud service.

Deriving the guidelines from a real life case done at 1928 Diagnostics, will justify the value of the guidelines, which aims to facilitate the process of constructing SAC for cloud-based medical software organizations. Besides from the guidelines, our study can be used as a starting point for cloud-based medical software organizations that wants to introduce the usage of security assurance cases in their company's development process. By using our results (the created artefacts) and learning from our mistakes they can both save time and avoid potential pitfalls.

The rest of this paper is organized as follows: Section II presents more background on assurance cases and an overview of relevant research. Section III presents our research questions and describes the research methodology, our data collection and data analysis strategies. Section IV presents the results of our research. Section V discusses the findings of our study and limitations to our research. Lastly, section VI concludes the paper with the key points of our research.

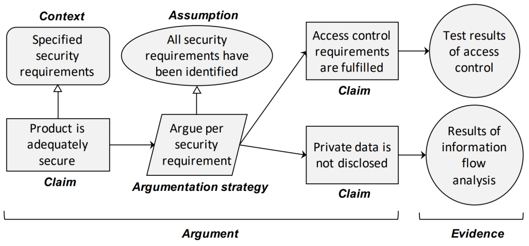

Context
Specified security requirements
Assumption
All security requirements have been identified
Access control requirements are fulfilled
Claim
Test results of access control
Product is adequately secure
Claim
Argue per security requirement
Argumentation strategy
Private data is not disclosed
Claim
Results of information flow analysis
Argument
Evidence

Fig. 1. Example structure of a simple assurance case [28]

II. Background And Related work

Security is a key factor when developing software, especially today as medical devices become more digitized and are constantly evolving with everything from wearable trackers to implantable sensors. The challenge for organizations is how to mitigate the security risks for their medical products. Many institutes such as The National Defense Industrial Association (NDIA) and National Institute of Standards and Technology (NIST) suggest the use of assurance cases in their documents for providing justification to stakeholders that critical properties of systems uphold certain requirements [30].

Security assurance cases consist of a structured arguments part where claims about a system's security are made and an evidence part that is used to justify the claims made on the argumentation part by providing evidence such as results of tests, simulations, analysis, etc. SAC can either be presented textually or graphically, but a graphical representation is more common and also more understandable [7].

Since security was not a major concern in the medical domain up until recent years, there has not been as much usage of SAC in literature as there is for safety assurance cases. One of the related studies we found is the work by Finnegan et al. [12]. The research presents a security case framework which is currently under development. The purpose of the framework is to provide healthcare organizations and medical device manufacturers a solution to ensure the security of medical devices. The researchers present a number of existing international standards, guidance documents and processes which aim to guide the development of the security argument pattern. Since there is no standardised way to address security requirements in the medical devices domain, the researchers aim to investigate the gaps that exist when medical devices organizations want to fulfill new security requirements. Part of their study is to validate the security case framework in industry both with medical device manufacturers and health-care delivery organisations. Similar to our study, the goal of their research is to simplify the process of creating SAC in the medical domain, however the difference is that we are creating guidelines while they are creating a pattern. A distinction can be made between patterns and guidelines, guidelines are a set of recommendations that can be followed to solve a problem, whereas a pattern suggests a specific solution to a problem [31]. Their work provides guidance documents and processes which can be useful for our study to address the security requirements and identify problems when covering security cases in a medical software organization.

In one study by Weinstock et al. [7]. The authors simplify the process of constructing security assurance cases, by presenting an explicit example on how to create a pattern from a security case and generalize it. This pattern can then be used as a template to construct other security assurance cases. For example, they address security vulnerabilities that appear during different stages of the software development life cycle (requirements, design, implementation). The researchers also discuss the benefits of creating security case patterns and how the patterns provide usability by outlining the security claims. The approach and the techniques used in their study for creating and generalizing security cases, will be used in our research to construct a SAC for 1928 Diagnostics.

Another paper we reviewed is about safety assurance cases by Smith et al. [6]. Despite the difference between security and safety we can use this paper for inspiration when creating SAC. In software, a safe system is one that does not accidentally harm people, property, environment or itself. While security is about ensuring that a system works correctly even under attack, by applying security techniques and practices [21].

In their study Smith et al. gives an overview about assurance cases and the development of an assurance case for 3dfim+, an existing Medical Imaging Application (MIA) for analyzing activity in the brain. The researchers present this example to explain the value of applying assurance cases for Scientific Computing Software (SCS) [6].

In our study we will also use assurance cases in the medical field, but we will focus on creating security assurance cases. However, since the guidelines for creating security assurance cases is not established as it is for safety assurance cases, we can gain knowledge on how to create SAC through studying safety assurance cases.

III. Research Methodology

To conduct our research we used the design science research (DSR) method at 1928 Diagnostics company by following the information systems design research framework as per Hevner [13]. Being in the business environment helped us to understand the requirements and constraints of the problems while creating artefacts that fulfill the company's business needs. We chose design science methodology because the objective of our study was not to create useful artefacts that were limited to the company we studied, but rather by all companies in the same domain. To create guidelines which can be used by cloud-based medical software organizations to construct their security assurance cases, we formulated the following research questions:

A. Research Questions

- RQ1: What are the needs and the requirements for creating SAC in a cloud-based medical software service organization?
- RQ2: What does a prototypical SAC in a cloud-based medical software service organization look like?
- RQ3: Which guidelines for creating security assurance cases should cloud-based medical software service organizations follow?

RQ1: The purpose of this question is to identify the external requirements and the best practices presented in the literature and documents such as standards and regulation for creating SAC.

RQ2: aims to identify a cloud-based medical software service company's internal processes and practices when creating security assurance cases. Additionally, the question aims to demonstrate evidence that justifies the claims when covering a security case in a cloud-based medical software service organization.

RQ3: Our goal is to identify and specify guidelines that can be used to create SAC for cloud-based medical software service organizations. The guidelines will be based on the steps we take to create SAC for one of 1928 Diagnostic's products.

B. Research Strategy

To find the answers for the research questions we decided to take an iterative approach which consisted of two iterations. The aim of each iteration was to answer one or more parts of our research questions defined in this study and as a result produce an artefact.

Figure 2 shows the steps taken in each iteration during the research. Each iteration was based on following the five general steps of DSR by Vaishnavi Kuechler [17] as seen in Figure 3.

1) Problem Awareness: The first step was to identify and understand the problem by studying the current state of SACs in the cloud-based medical software service domain, through reading standards, regulations, and best practices of cybersecurity in the domain as well as gathering information from individuals in the company.

2) Suggestion: Once we got acquainted with the problem, we studied and gathered relevant data to propose a solution. In the first iteration this was done through literature review while in the next iteration the solution was based on data gathered from interviews.

3) Development: In this step we create an artefact based on the suggestion from the previous step. The artefact of the first iteration was a document consisting of the company's needs and requirements for creating SAC. The second artefact which will be created in iteration two is a security assurance case. The guidelines which can be used to construct security assurance cases, will be extracted from the SAC artefact from the second iteration.

4) Evaluation: This step is similar in both iterations, we evaluate the usefulness and understandability of the artefact that was developed in the previous step through semi-structured interviews with company representatives.

5) Conclusion: We update and improve the artefact based on the feedback we get during evaluation. The iteration reaches its end and the result is a validated artefact.

C. First Iteration

The first iteration provided us with an answer to RQ1.

1) Eliciting external requirements and identifying existing guidelines in literature (Artefact Development): The first step for us was to identify the current best practices and approaches reported in the literature for creating SAC in the medical domain. We did this by studying the papers mentioned in the related work section. We also reviewed the standards and regulations that medical software service organizations must comply with, which mainly were ISO 27002 [18] and ISO 27018 [19]. Our goal was to create a document consisting of the external requirements a medical device company needs to fulfill to put their products on the market based on the literature and the mentioned standards. However, after our first meeting with the QA/RA manager of 1928 Diagnostics we decided that our artefact would end up as a document covering both external and parts of the internal needs of the company. The reason for that is we received a draft of the company's white paper which contained the security practices the company had in place to be compliant with regulations. He also suggested that we take a look into HIPAA security rule and privacy rule papers [20]. We analyzed the white paper and suggested documents and then picked out the best security practices and requirements to create our first artefact.

The initial artefact was a table showing the best practices and the techniques to ensure and mitigate security risks based on the company white paper. We then described each practice as it was referred to the in standards (ISO 27002 [18], ISO 27018 [19]). Finally we described how each listed practice was

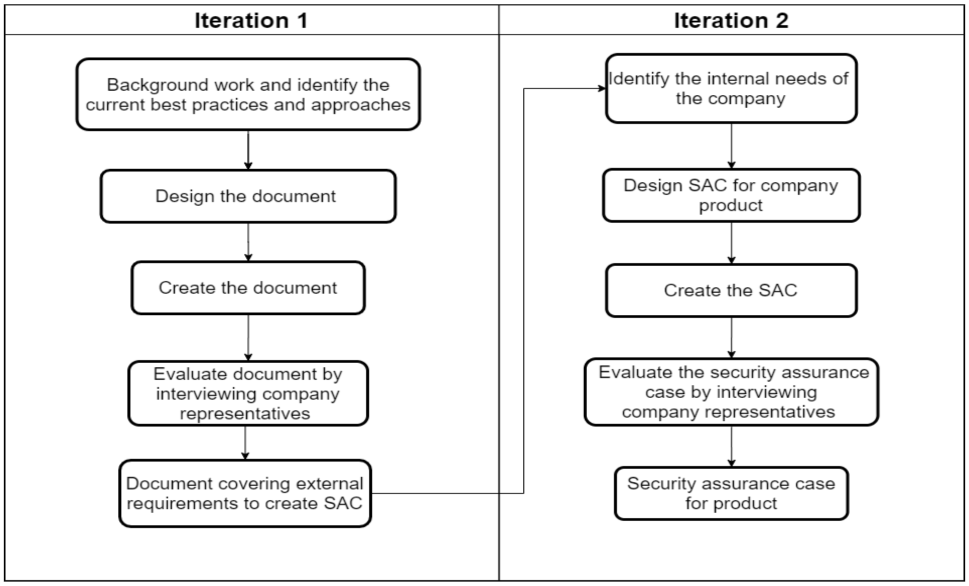

Iteration 1
Background work and identify the current best practices and approaches
Design the document
Create the document
Evaluate document by interviewing company representatives
Document covering external requirements to create SAC
Iteration 2
Identify the internal needs of the company
Design SAC for company product
Create the SAC
Evaluate the security assurance case by interviewing company representatives
Security assurance case for product

Fig. 2. Our research process

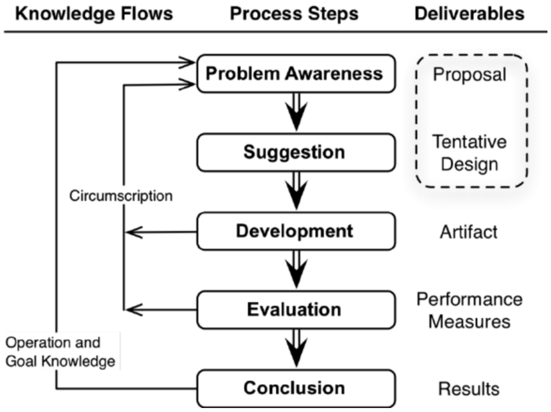


Fig. 3. Design Science Research general steps

related to SAC whether using SAC to show usage of a practice was beneficial or mentioned implicitly in the standards.

2) Evaluating the created artefact with the company (Data Collection): To evaluate the artefact we developed, we conducted interviews with two practitioners from 1928 Diagnostics. One with the CTO of the company to gain a broader understanding of their system and security and another with a developer to learn about the technical details such as functions and components. The interviews were semi-structured to allow the interviewee to explain their thoughts and highlight the most important insights in the area, as well as to enable deep answers about certain questions to gather qualitative data [16]. Appendix A contains the defined questions aimed to evaluate the first artefact.

The interviews were hosted through a web chat application and recorded with consent of the interviewees. The interviews lasted about 30 minutes each and started with an introduction about our study. During the interview we presented the practitioners with a simple example of SAC as seen in Appendix B and the created document.

3) Analyzing the collected data from the company to improve the artefact (Data Analysis): We followed the thematic analysis method and divided data into themes and categories [14]. The interview questions we came up with were divided into different themes before we began with the interviews. The questions were divided into the following four themes:

- **Demographic:** Participants' backgrounds and knowledge regarding SAC.
- **Values:** Understanding what the participant regards as valuable when it comes to security.
- **Structure:** In what way and how the company is taking measurements to assure security and comply with practices before creation of SAC.
- **Usefulness:** In what way will SAC be useful to the company, who will benefit from it and how can it be used.

After the interviews we transcribed the gathered data from the interviews with Temi, an online transcription tool. Once all the raw data was transcribed, we followed the thematic analysis method and read through the transcribed data and systematically code the data we had by categorizing parts of information under the identified themes as seen in Appendix C.

D. Second Iteration

The second iteration provided us with an answer to RQ2 and RQ3.

1) Eliciting internal requirements and creating a security assurance case (Artefact Development): Our first goal in this iteration was to understand the internal needs of the company to allow us to create SAC. We started the second iteration by conducting two more interviews with the same people we interviewed at the end of the first iteration (CTO and a developer) from the organization. We made sure to understand possible usages of SAC for the company. We also asked questions to get an overview of the company's current structure and how they assure that their products are secure. The main goal of the interviews was for the researchers and interviewees to get a shared understanding of how SAC should be constructed and later used.

The next step after we understood the internal and external needs of the company, was to get in touch with the QA/RA manager of 1928 Diagnostics in order to receive company's risk analysis, software architecture, and software design specification documents. These documents helped us get an overview of their system. We later extracted the security related parts of the system to a new document and used it to create a SAC for a part of their system.

Once we had the document with the security relevant features, we used that together with the data we gathered at the start of iteration two and from the first iteration to create a security assurance case covering the transfer of bacterial DNA samples from the users to the cloud service.

We presentented the proposed security assurance case through interviews where the goal was to evaluate the final artefact and make sure the organization representatives had the correct understanding of the artefact. Feedback from the interviews in the end of this iteration helped us to update and finalize the SAC. Additionally it helped us to construct the guidelines.

At the end of the iteration after the SAC had been evaluated, we created guidelines that can be used as a starting point for cloud-based medical software service organizations when constructing security assurance cases. The guidelines are derived from the SAC we created for 1928 Diagnostics and based on our learning experience during our study.

2) Conducting interviews to collect data for creation and evaluation of the SAC (Data Collection): At the start of the second iteration we conducted two interviews with the practitioners from the previous iteration to collect data regarding internal needs in order to create SAC. Appendix D contains the defined questions.

The interviews were semi-structured similar to the iteration and were also hosted online through Zoom and recorded with consent of the interviewees. The interviews lasted about 30 minutes and we started with presenting the practitioners with a more detailed example of SAC as seen in Appendix E.

After creating the SAC we conducted two more interviews with three people to evaluate the artefact. One interview was with the QA/RA manager of 1928 Diagnostics and another one was an interview with two developers at the same time. Similar to the interviews at the start of the iteration, they were semi-structured, hosted and recorded through Zoom. The developers we interviewed were knowledgeable with the technical aspect of the company. The evaluation questions that are listed in Appendix H, were asked to understand the usefulness of the SAC and to make sure it was in alignment with the company's system.

3) Analyzing the collected data from the company to create and then improve the SAC (Data Analysis): For analyzing the data from the first interviews in this iteration we used the same data analysis method and defined themes from the previous iteration. Before conducting the interviews we divided the questions we came up with into the four themes identified previously. Once the interviews were conducted, the data was transcribed and divided into the themes as seen in Appendix F.

To analyze the evaluation data we collected at the end, we used the same method but defined new themes before the interviews. The evaluation questions were divided into the following five themes:

- **Correctness:** How much the SAC actually reflects the architecture and the applied security mechanisms in the company.
- **Quality:** Making sure the case is understood by the company and useful for them.
- **Value:** Whether the case (and similar ones) would be valuable to show a certain level of security in the product, and in this case, who would be interested and why.
- **Generalization:** If the case can be used to derive guidelines for creating SAC for other products within the company but also in the domain.
- **Challenges:** How the cases will be maintained and who will take responsibility to create and update cases. Integrating these steps, in the current company process.

For the final interviews of the iteration we followed the same procedures as done for the previous interviews, we transcribed the gathered data with the same transcription tool. Once all the raw data was transcribed, we read through the transcribed data and systematically code the data under the identified themes as seen in Appendix I.

IV. Results

A. First iteration - identification of external needs

To answer our RQ1, our final artefact from iteration one is presented in Table I. We present the best practices found in the standards and the company's white paper. Each practice refers to which standards they belong to.

The relation between the practices and SAC was not explicitly mentioned in the analyzed documents, therefore, we identified the relation between the SAC and the presented security requirements. We indicated whether using SAC to present compliance with the practices were beneficial or implicitly mentioned in the standards. The presented security requirements in Table I are specific to cloud-based software service providers.

The standards implicitly state that operating procedures should be documented and available to all stakeholders [18]. Using SAC it is possible to show the argumentation and evidence on how logging and monitoring has been applied by the company [18] [19]. Having a SAC available is also useful as a document to the company's stakeholders.

SAC will be beneficial to show that a medical software

TABLE I
ARTEFACT 1 NEEDS AND REQUIREMENTS FOR CREATING SAC IN A MEDICAL SOFTWARE SERVICE ORGANIZATION

Needs	Description	SAC	Reference
Logging	System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.	Implicit	ISO 27002 [18] & 27018 [19]
Monitoring	Security features are monitored automatically and through planned internal audits to detect and mitigate actual or track potential vulnerabilities and both actual and potential intrusions.	Implicit	ISO 27002 [18] & 27018 [19]
Backup	Appropriate backups should be taken and retained in accordance with a backup policy.	Beneficial	ISO 27002 [18], 27018 [19] & HIPAA [20]
Training	Programmers should be training regularly in best coding practices that help to ensure security. e.g, define security requirements, Heed compiler warnings.	Beneficial	ISO 27002 [18] & 27018 [19]
Redundancies	IT facilities should have sufficient redundancy to satisfy availability requirements.	Beneficial	ISO 27002 [18] & 27018 [19]
Encryption	All connections between users and web servers need to be encrypted using HTTPS/TLS, which means that no other person or entity can read or change the information exchanged. All stored user data, including sample files and database should be encrypted.	Implicit	ISO 27002 [18] & 27018 [19]
Accessibility control	All the servers are Protected by stateful packet inspection firewalls, with only necessary services allowed. Offer tight control sharing, only specific users can access data. Changes in user permissions that are initiated automatically by the information system and those initiated by an administrator.	Beneficial	ISO 27002 [18] & 27018 [19]
Firewalls	Uses strict stateful network firewalls to protect all servers, including those processing confidential user data.	Implicit	ISO 27002 [18] & HIPAA [20]
HIPAA compliance	Follow the rules established by HIPAA for the implementation of IT and software security controls. These requirements are important in order to protect personal health information.	Beneficial	HIPAA [20]
Records retention	Customers should have the ability to delete data and reports when no longer needed or when patient or donor consent is revoked. Customer data are stored until deleted by the customer, providing complete control over record retention and destruction. Project Administrators can lock projects to prevent accidental deletion of any files by anyone other than the project Administrators.	Beneficial	ISO 27002 [18] & 27018 [19]

TABLE II
ARTEFACT 1 CHANGES AFTER EVALUATION IN THE FIRST ITERATION

Item	Change	Reason
The practice Cryptographic controls	Removed	Based on feedback P2 - "I don't think having encryption and Cryptographic controls as separate makes sense."
The relationship between SAC and needs.	Added	To increase understandability
Reference to standards	Added	To increase understandability

service organization that operates on the cloud is in compliance with the minimum HIPAA requirements such as having firewalls and backup. The ISO 27002 [18] standard and HIPAA [20] that contain the backup requirements state to ensure that all information and software can be recovered. Using a structured argument-evidence body as SAC can be beneficial to show that the backup requirement has been met.

For a company to be compliant with the ISO 27002 [18] as well as HIPAA [20], the organization should ensure that the network provider manages security networks by using firewalls. SAC can be used to provide justification to regulatory agencies that these solutions are implemented in a system. SAC will contain evidence and argumentation to indicate that the organization has fulfilled the security networks requirements.

The first version of the document was used as a starting point for the final artefact. We evaluated it by interviewing the company to make sure the proposed practices cover the external requirements that the company needs to fulfill. We analyzed the data from the interviews by following thematic analysis method which helped us to update and improve the artefact. The result of the complete analysis is in Appendix C. The changes to the original draft of the artefact can be seen in Table II while the first version of it can be seen in Appendix G.

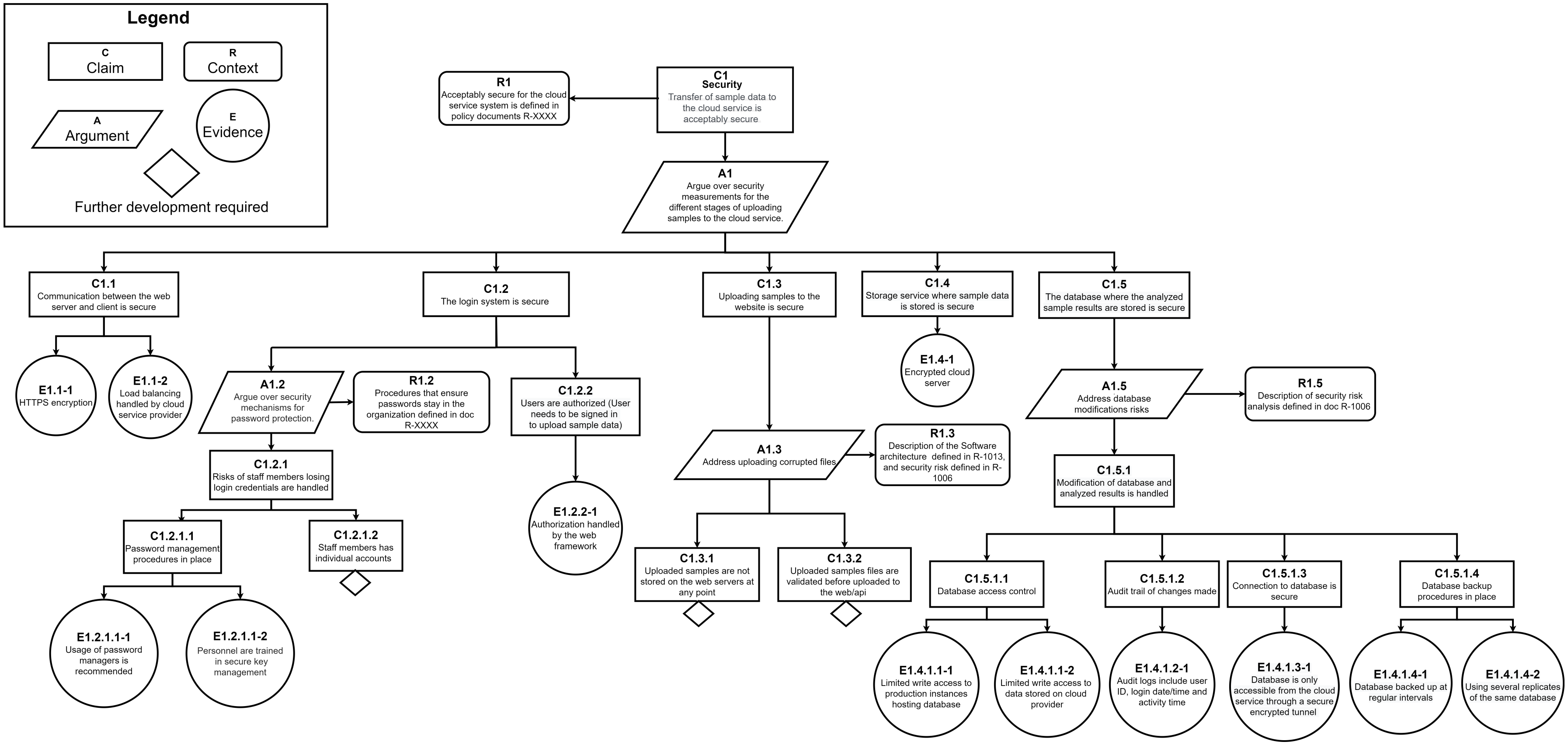

Legend
C
Claim
R
Context
A
Argument
E
Evidence
Further development required
R1
Acceptably secure for the cloud service system is defined in policy documents R-XXXX
C1
Security
Transfer of sample data to the cloud service is acceptably secure
A1
Argue over security measurements for the different stages of uploading samples to the cloud service.
C1.1
Communication between the web server and client is secure
C1.2
The login system is secure
C1.3
Uploading samples to the website is secure
C1.4
Storage service where sample data is stored is secure
C1.5
The database where the analyzed sample results are stored is secure
E1.1-1
HTTPS encryption
E1.1-2
Load balancing handled by cloud service provider
A1.2
Argue over security mechanisms for password protection.
R1.2
Procedures that ensure passwords stay in the organization defined in doc R-XXXX
C1.2.2
Users are authorized (User needs to be signed in to upload sample data)
C1.2.1
Risks of staff members losing login credentials are handled
C1.2.1.1
Password management procedures in place
C1.2.1.2
Staff members has individual accounts
E1.2.1.1-1
Usage of password managers is recommended
E1.2.1.1-2
Personnel are trained in secure key management
E1.2.2-1
Authorization handled by the web framework
A1.3
Address uploading corrupted files
R1.3
Description of the Software architecture defined in R-1013, and security risk defined in R-1006
C1.3.1
Uploaded samples are not stored on the web servers at any point
C1.3.2
Uploaded samples files are validated before uploaded to the web/api
E1.4-1
Encrypted cloud server
A1.5
Address database modifications risks
R1.5
Description of security risk analysis defined in doc R-1006
C1.5.1
Modification of database and analyzed results is handled
C1.5.1.1
Database access control
C1.5.1.2
Audit trail of changes made
C1.5.1.3
Connection to database is secure
C1.5.1.4
Database backup procedures in place
E1.4.1.1-1
Limited write access to production instances hosting database
E1.4.1.1-2
Limited write access to data stored on cloud provider
E1.4.1.2-1
Audit logs include user ID, login date/time and activity time
E1.4.1.3-1
Database is only accessible from the cloud service through a secure encrypted tunnel
E1.4.1.4-1
Database backed up at regular intervals
E1.4.1.4-2
Using several replicates of the same database

Fig. 4. Created SAC in iteration 2 covering transfer of sample data to the cloud service

TABLE III
THE CLOUD SERVICE SYSTEM'S SECURITY FEATURES MAPPED TO ARTEFACT 1 AND CIA

Need	Security feature(s)	CIA
Accessibility control	- Login/register system - Users need to be signed in to upload/download data - Authorization provided by the web application framework - Set user permission depending on work role needs - Disallow editing of results (every export is write protected) - Limit write access to data stored on cloud providers - Limit access to production instance hosting database and code	Confidentiality, Integrity
Encryption	- Usage of https certificates - To provide secure connections from the web client to the server, HTTP over TLS is used, commonly abbreviated HTTPS. (Files containing data are sent over HTTPs) - Access to production databases is handled through ssh-keys or equivalent.	Confidentiality, Integrity
Backup	- Implement procedure for backing up databases at regular intervals. - Implement having regular practice sessions for restoring database backups.	Availability, Integrity
Logging	- Every time we show a result or generate an export we shall include sample id, submission date, run date and user.	Nonrepudiation
Redundancies	- Use a service provider with high availability to store sample sequences and that automatically notifies its administrators when the service is down - Samples are not stored on the web servers at any point, but instead the storage API is utilized directly - Implement protection against ddos attacks - The REST API is used to directly upload samples from the client's computer.	Availability
Training	- Enforce usage of password managers and have trained personal secure key management. - Each staff member shall have an individual account to limit the impact of lost credentials.	Confidentiality, Integrity

B. Second Iteration - creation of the security assurance case

Our second iteration aimed to answer our RQ2 and RQ3. We created a security assurance case which covers the transfer of samples to the cloud service. Our artefact is presented in Figure 4. The security assurance case was constructed by following the graphical notation called Goal Structuring Notation (GSN) [7].

The SAC consists of claims made about the system in a given context, followed by arguments supporting the top-level claim. Claims are broken down into sub-claims which are associated with evidence that is used to justify the claims. The different notations/shapes can be seen in the legend of Figure 4.

The SAC starts with the top claim C1 (**transfer of sample data to the cloud service is acceptably secure**), the claim is associated with a context. The aim of the context is to define the scope, where the claim has to uphold. In this case, what acceptably secure means is defined in the company's policy documents.

The selection of the top-claim was based on the company's internal needs that we identified in the interviews at the beginning of the iteration. The remainder of claims, arguments and evidence that are presented in the SAC was based on the company's risk analysis, software architecture, and software design specification documents we received from the QA/RA manager of the company.

We analyzed the documents we received and extracted the security related parts of the system into a new document called system analysis. The reasoning behind creating a new document was the size of the system, it would take more time than available for the thesis to create security assurance cases covering the whole system. Having a system overview, assets that are threat targets and dataflow of the system in the system analysis document simplified the process of creating SAC for us, instead of having to go through multiple large documents to find information, we had one with all the security relevant information about the system in one place. The system analysis document was used to map the identified security features of their system to the best security practices described in artefact 1. To evaluate the value of each security feature we related each feature to one/or more of the three concepts of the CIA triad model [22], this can be seen in Table III. The three concepts confidentiality, integrity, and availability of the CIA triad are considered to be the most crucial components of information security [22].

For the first argument A1 in Figure 4, we defined our strategy by looking at the different system views and security mechanisms that were specified in the software architecture document, we found the different stages for uploading samples to the cloud service. In order to justify the top-claim that

TABLE IV
ARTEFACT 2 CHANGES AFTER EVALUATION IN THE SECOND ITERATION

Item	Description	Change	Reason
Claim C1 - Transfer of the patient's data to the cloud service is acceptably secure	Changed to "Transfer of sample data to the cloud service is acceptably secure."	Modified	Based on feedback P1 - " Yes, it doesn't have to necessarily be called the patient's data because what we're running analysis on is bacteria. So in the perfect case, it's not patient data. actually bacteria data. I'm thinking just data or sample data."
Diamond notation	Added a diamond beneath claims that were missing evidence to indicate that this needs further development.	Added	Based on feedback P1 - "One idea can be that you can have a dashed circle under or something that indicates that, here's something missing. So then this could be also used as kind of a gap analysis to identify weaknesses. And gaps in the argumentation, so a dash line indicating that we need more claims here. This is just an example."
Evidence E1.4.1.3-1 - Connection to database is made through ssh-keys	Changed to "Database is only accessible from the cloud service through a secure encrypted tunnel."	Modified	Based on feedback P2 - "I mean yes we use a secure connection, but it's a database that is not accessible, none of the ports are open actually. So what we use is a tunnel, it's a cloud service provider tool that helps us to tunnel through the server without opening any open ports, which means literally nobody can ssh into it. I guess you could say something like: 'Secure encrypted tunnel or reversed tunnel'".
Evidence E1.1-2 - Protection against ddos implemented	Changed to "Load balancing handled by cloud service provider"	Modified	Based on feedback P2- "So I also realized, the protection against DDOS, we had this implemented in the past but the product we were using we couldn't keep using. Right now we have it in the load balancer in the cloud service provider itself, but we were using a DDOS service provider in the past but we don't use it anymore because of HIPAA compliances. It's not that it's not implemented, we can use it when needed but now we don't have this like this DDOS service provider layer. I guess DDOS is very specific, but could be something like traffic load instead."
Evidence E1.2.1.1-1 - Enforced usage of password managers	Changed to "Usage of password managers is recommended"	Modified	Based on feedback P3 - "For example password manager is not enforced, we have told people this is a good thing to use. But we don't check if people actually use it. It's recommended."
Claim C1.2.2 - Users are authorized (User needs to be signed in to upload /download data)	Changed to "Users are authorized (User needs to be signed in to upload sample data)"	Modified	Based on feedback P3 - "Small detail in C1.2.2, you mention download data. The user is actually not able to download samples, they are able to download results of the samples like graphs and pictures."
Claim C1.4 - Storage service where sample data is stored is secure	Added a new claim, which is a stage that was missing. Added between C1.3 and C1.4, the previous C1.4 is now C1.5 and all associated boxes have been updated accordingly.	Added	Based on feedback P2 - "I would say, yes. I agree that those four things are consistent. I guess in between C1.3-C.1-4, is probably the point P3 mentioned that uploading samples to the website is secure, but we also wanna say the storage after uploading the samples are encrypted or secure. Right, because that is a different step from the database, consider it like a file server because we have huge files. If you wanna add it, it's stored in a cloud server, because I think it's fairly separated from the database and the web server. "

the transfer of sample data to the cloud service is acceptably secure, we argued over the security measurement in the identified stages and divided them into sub-claims.

Each claim is associated with a strategy that has been used to develop the arguments supporting the top-level claims. In other words, the strategy helps to clarify the approach used for creating the claim.

A security assurance case breaks claims into subclaims, each of which is broken into yet another level of subclaims until the step to the actual evidence that supports that subclaim is reasonably small [7]. For example as the claim C1.2.1 "Risks of staff members losing login credentials are handled" is broken down to two sub-claims, which are C1.2.1.1 "Password management procedure in place" and C1.2.1.2 "Staff member has individual accounts", which then are associated with one or more evidence to justify the claim C1.2.1.

Claims with a diamond beneath indicates that further development is required to fully elaborate the claim-argument-evidence substructure [7]. In the SAC there is no evidence related to the claims C1.2.1.2, C1.3.1 and C1.3.2, however this does not necessarily suggest that the company fails to satisfy this claim or has not implemented it in the system. Due to the limited time frame of our research we decided to allocate more time to breaking down only some of the claims into further detail, the chosen claims were based on the data from the interviews and on the level of information and value that was identified for each security feature from Table III.

At the end of the second iteration, we evaluated the first draft of the SAC by interviewing three people from the company. One of the interviewees works as QA/RA manager at the company and the two others as developers. The questions that were asked during the interviews lead to in-depth answers that provided us with the person's opinions on the topics based on their expertise in their particular field of knowledge. The data from the interviews were analyzed and the result can be found with their corresponding themes in Appendix I.

P1 mostly discussed and gave feedback regarding the value, challenges and quality of the case. P1 being the QA/RA manager, could not help us with the technical correctness of the case. P2 and P3 both being developers and aware of the technical details regarding the system, gave us feedback regarding the correctness of the case and helped us update the SAC to make sure it was aligned with the company's system.

Based on the data we gathered and analyzed from the interviews, we updated and finalized the artefact. Table IV contains all the changes that were made to the artefact (SAC) after evaluation while the first draft of the SAC can be found in Appendix J.

C. Derivation of the guidelines

At the end of iteration two, we developed guidelines that can be used to create security assurance cases. The guidelines are specific to cloud-based medical software organizations and based on the steps we followed to construct a SAC for 1928 Diagnostics and our learning experience throughout the two iterations. The guidelines are presented below as following:

Elicitation of requirements:

- The first artefact we created can be used by cloud-based medical software organizations to make sure the external security needs and requirements are fulfilled. Mapping the external needs in the artefact to the company's internal needs can simplify the creation of SAC, when selecting claims, arguments and evidence.
- It is beneficial to divide the whole system into subsystems such as functions or components that can be used as a top level claim, especially in large and complex systems such as medical software. The selection of the top-level claim should be based on the company needs and values. For example, the selection of the top claim C1 in our SAC was based on the high value the company puts on ensuring their customers' privacy.
- Arguments and claims can be extracted from a cloud-based medical software company's documents such as software architecture and software design specification documents, asset analysis documents, while evidence can be found in threat analysis documents, risk analysis, code reviews and test results etc.

Elicitation of requirements and Evaluation:

- To create a SAC in the medical software domain it is important to have an understanding of the system, any documents regarding security of the system are useful to study. Gathering information from individuals such as developers that are knowledgeable about the system is also useful. Use any valuable resources available. In our case gathering data from people in the company helped us to create a more accurate SAC that was more aligned with their system because there had been changes to the system which was not updated in the documents.

Modeling:

- Using strategies in SAC is optional, but we highly recommend it because it allows the reader to understand the approach that an argument is going to take [7]. The phrasing of strategies is crucial, it decides how subclaims will be elaborated.
- Using identifiers for the claims, arguments and evidence in the SAC improves communication between stakeholders and understandability for anyone reading the SAC, because it allows referencing to certain elements easier. Especially for software companies in the medical domain since the stakeholders background varies to a large extent. For example at the company we conducted our study, bioinformaticians and developers work together.

Evolution and Modeling:

- The absence of evidence should be clarified to the reader, as it might indicate further development is required or security measurement missing. For example in our case, we added a diamond notation under claims without evidence to indicate that these claims require further development based on feedback from the company. This can be useful to identify missing security features which can be crucial for medical software companies.

The guidelines has been classified into four different categories: Elicitation of requirements, Evaluation, Evolution and Modeling. The classifications describes in which part of the SAC creation and for what reason the guidelines are used.

V. Discussion

In this section we discuss the most important and interesting finds, by presenting every artefact that was created in the iterations and discussing how they relate to the research questions. The last part of the section makes suggestions for further work and acknowledges the study's limitations.

A. RQ1

The answers to the question *What are the needs and the requirements for creating SAC in a cloud-based medical software service organization?* were found and developed as an artefact in the first iteration.

The first draft of the artefact consisted only of two columns which were the **need** and **description**. To increase the understability of the artefact and make it clear that these needs are general to any company in the same domain, we added two more columns which were **SAC** and **reference**. The reference column shows in which standard the need can be found. The addition of the SAC column was inspired by the work of Mohamad et al. [28], it describes how each listed need relates to SAC whether using SAC to show usage of need was beneficial or mentioned implicitly in the standards.

Additionally to avoid redundancy, we removed the listed need **Cryptographic controls** based on a suggestion from P2. These improvements were necessary to increase the understandability of the artefact and to support the creation of

SAC.

The artefact which is presented as Table I in Section 4 highlights needs that are specific to cloud-based medical software service organizations, which should be followed by the companies to ensure a secure system. The needs that are recommended by the standards ISO 27002 [18] and ISO 27018 [19] such as logging, monitoring and encryption are general to any cloud-based software. While the ones found in HIPAA [20] are more specific to any organization handling healthcare data.

B. RQ2

To answer the research question *What does a prototypical SAC in a cloud-based medical software service organization look like?* were partly found in the first iteration but mainly being developed and improved in the second iteration. The security assurance case was developed during iteration two based on data gathered from iteration one and two.

The selected case (**transfer of sample data to the cloud service is acceptably secure**) for the SAC prototype was based on P1's definition of a secure product. The SAC artefact as seen in Figure 4 in Section 4 was built based on Table III. Due to time constraints only some claims were broken down into more detailed levels, these claims that were selected were evaluated based on their relation to CIA as seen in Table III.

During evaluation of the SAC some of the practitioners suggested to provide more detailed information in the evidence part, while others recommended to keep the abstraction level. We decided to keep the level of the abstraction since it would be understandable by all stakeholders, not just the technical stakeholders, which can improve comprehension amongst the key project stakeholders [27]. Another suggestion was to add a diamond notation under claims missing evidence, to clarify that this claim requires further development. We applied this suggestion to the prototypical SAC, since it improves the understandability of the SAC and is also a part of the GSN notions [5]. The technical practitioners also helped us with the correctness of the SAC, based on their feedback we updated many parts of the artefact to make sure it was aligned with the company's system.

During our study company representatives confirmed that having security assurance shown in a graphical structure like SAC would be beneficial to improve communication regarding security between stakeholders, but also useful for new developers to find their way around the system [27].

Table III which is seen in Section 4 was developed to cover the internal needs of the company, it gives an overview of the security features the company has implemented. The identified security features were mapped to the needs described in Table I from the first iteration, combining the external and internal needs was done to support the creation of the SAC prototype.

C. RQ3

The answer to the final research question *Which guidelines for creating security assurance cases should cloud-based medical software service organizations follow?* is based on the results from the first and second iteration. The guidelines are derived from the steps we took to create a security assurance case for a cloud-based medical software service organization.

During our research, we found that before creating the SAC, it is important to take into consideration who the stakeholders for the SAC are and how the creation and maintenance of SAC will fit into the process. The level of detail that goes into a SAC depends on the stakeholder. From practitioners' feedback we learned that technical stakeholders such as developers were interested in more detail while stakeholders with managerial roles were more interested in an abstract level of SAC.

Another important lesson we learned throughout the research and as a practitioner from 1928 Diagnostics also pointed out, is that the creation and management of SAC's should be integrated in the software development process. Creating and evolving security assurance cases in the software development life cycle (SDLC) can help in finding security requirements and features that need to be developed and focus on what evidence needs to be improved at each stage of the SDLC [7]. Additionally, it would be easier to construct SAC at the beginning of the software development rather than waiting until the system becomes larger and more complex making it harder to gather evidence. For example, we could only create SAC for a part of 1928 Diagnostics system with the given time, because they already have a rather large system. In order to include more details in the SAC and cover a larger part of the system we would have to find more claims and evidences which would require more time.

The guidelines which are found in Section 4 C are specific to cloud-based medical software service organizations, which want to create security assurance cases.

D. Future Work

As stated earlier, the proposed guidelines can be used as a starting point for cloud-based medical software service organizations for creating SAC. Due to time constraints the guidelines were not evaluated, therefore we suggest to validate the guidelines by applying them when creating SAC for cloud-based systems in the medical domain. The results of our study reflects on adoption of SAC in smaller companies, since our study was conducted within a small organization. Future work could be used to expand the scope and include bigger samples in the research, as the interviewees mentioned the usage of SAC might be more useful in larger companies that consist of multiple subteams.

E. Limitations

1) External Validity: The end goal of our study was by studying a small sample size, we would create generalised guidelines that could be used by companies in the cloud-based medical software service domain. Using a judgment sampling method is low cost, convenient, not time consuming and ideal for exploratory research design [23]. However the issue that arises, is that it does not lead to generalized results, since we only take one company's needs into consideration when creating guidelines [23].

Gregory [25] notes that "The outcome of design science research (i.e., the problem solution) is mostly an individual or local solution and the results cannot be readily generalized to other settings".

Being aware of this limitation and taking into consideration that we are not covering the entire population in the domain, we focused on creating guidelines that can be used as a starting point to create SAC for cloud-based medical software service organizations. However users of these guidelines should study the situation and values of the population on which the study was conducted with caution in order to understand to what extent they can generalize the findings [26].

2) Internal Validity: Conducting successful semi-structured interviews is a major challenge, interviews are a resource-demanding data collection method; activities such as planning, conducting and analyzing are time-consuming by nature [24]. There is a risk to induce errors in data collection. For example, if the questions are open-ended but misinterpreted by the interviewees the results will be influenced. The order of the questions asked during the interviews can also have an impact on the result, because it might lead to biased answers.

To mitigate these risks, the questions were prioritized based on the objective of the interview and were timed-boxed to allow full answers for every question. Additionally, we tried to avoid yes or no questions to gain more in-depth information from the practitioners. The interviewees were provided with the questions and interview material in advance, so they could prepare for the interview.

Being two interviewers during the interviews enabled us to listen carefully to what was being said and helped us to ask follow up questions and having deeper discussions with the interviewees which led to us collecting more data [24]. Besides the structure of the interviews, another drawback was the small size of the company, which resulted in the availability of only four different interviewees throughout the two iterations.

However since we conducted a qualitative research this issue was mitigated, because we followed a purposeful sampling technique and not random sampling [15]. The participants we collected our data from are experts within their domains. The interviewees were selected during different parts of the study based on their expertise to make sure we could gather the needed data at the right time of the research process.

3) Construct Validity: Validity of our result depends on the reliability of any measurement instruments used during the research [29]. This being a bachelor thesis and the inexperience of us as researchers might have led to the composition of interview questions that were misinterpreted by the participants. To avoid this issue, we provided the participants with the questions beforehand through email and started off each interview with a brief introduction about the goal of the interview. Beside that, the prepared interview questions were checked with academic supervisors before the interviews to ensure their understandability.

Using an online transcription tool online to convert the recorded audio from the interviews to text, also affects the reliability of our research, because it does not assure accuracy. To mitigate this threat we used the tool as support to manually correct the transcriptions.

VI. Conclusion

This research was an attempt to address the lack of guidelines and examples of SAC available to follow for creating security assurance cases within the cloud-based medical software service domain. By conducting a design science study at a company in the domain, we created a SAC for a part of their system by identifying the company's internal needs and external needs such as standards, regulations, and best practices of cybersecurity in the domain. After evaluating the SAC with practitioners from the company, we created guidelines derived from the SAC. We believe the guidelines coupled with the created SAC will be beneficial for companies in the same domain that are looking to simplify the process of creating security assurance cases for their system.

Acknowledgment

We would like to express our gratitude to our academic supervisors Jan-Philipp Steghöfer and Mazen Mohamad for their effort, availability and guidance throughout the research. Additionally we extend our thanks to our industrial supervisor Robert Engberg and all of 1928 Diagnostics for allocating their resources to this research. We would also like to thank our Co-Assessor Thorsten Berger for his valuable feedback that contributed to this research.

References

[1] D. Klinedinst, J. Land, and K. O'Meara, "2017 emerging technology domains risk survey", CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, Tech. Rep., 2017.

[2] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate", Journal of Cybersecurity, vol. 4, no. 1, p. tyy006, 2018.

[3] T. Moore, "The economics of cybersecurity: Principles and policy options", International Journal of Critical Infrastructure Protection, vol. 3, no. 3-4, pp. 103–117, 2010.

[4] U.S. Food and Drug Administration, "Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and food and drug administration staff", Retrieved May, vol. 1, p. 2014, 2013.

[5] C. B. Weinstock and J. B. Goodenough, "Towards an assurance case practice for medical devices", CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, Tech. Rep., 2009.

[6] S. Smith, M. S. Nejad, and A. Wassyng, "Building confidence in scientific computing software via assurance cases", arXiv preprint arXiv:1912.13308, 2019.

[7] J. Goodenough, H. Lipson, and C. Weinstock, "Arguing security- creating security assurance cases", Build Security in Software Assurance Initiative, 2007.

[8] B. ISO, "Iec 15026—2: 2011 systems and software engineering—systems and software assurance, part 2: Assurance case", Google Scholar. 1

[9] International Organization for Standardization. 2014. ISO 27000 Information Security Management Systems.

[10] European Union. 2016. General Data Protection Regulation (GDPR) 2016/679.

[11] Knoppers, B. M. Framework for responsible sharing of genomic and health-related data.

[12] A. Finnegan and F. McCaffery, "A security argument pattern for medical device assurance cases", in 2014 IEEE International Symposium on Software Reliability Engineering Workshops. IEEE, 2014, pp. 220–225.

[13] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research”, MIS quarterly, pp. 75–105, 2004.

[14] C. A. Olney and S. Barnes, “Planning and evaluating health information outreach projects booklet 3: Collecting and analyzing evaluation data. 2. national network of libraries of medicine, outreach evaluation resource center; 2013.[16 jun 2016]”, 2013.

[15] M. Law, D. Stewart, L. Letts, N. Pollock, J. Bosch, and M. Westmorland, “Guidelines for critical review of qualitative studies”, McMaster University occupational therapy evidence-based practice research Group, 1998.

[16] C. Humphrey and B. H. Lee, The real life guide to accounting research: a behind-the-scenes view of using qualitative research methods. Elsevier, 2004.

[17] V. Vaishnavi and W. Kuechler, “Design research in information systems,”2004.

[18] ISO/IEC 27002:2017, Information technology - Security techniques - Code of practice for information security controls.

[19] ISO/IEC 27018:2014, Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”, International Organization for Standardization ISO, Geneve, 2014

[20] H. C. Assistance, “Summary of the hipaa privacy rule,”Office for Civil Rights, 2003.

[21] D. Firesmith, “Engineering safety-and security-related requirements for software-intensive systems,” CARNEGIE-MELLON UNIV PITTSBURGHPA SOFTWARE ENGINEERING INST, Tech. Rep., 2007.

[22] S. Qadir and S. Quadri, “Information availability: An insight into the most important attribute of information security,”Journal of Information Security, vol. 7, no. 3, pp. 185–194, 2016.

[23] H. Taherdoost, “Sampling methods in research methodology; how to choose a sampling technique for research,”How to Choose a Sampling Technique for Research (April 10, 2016), 2016.

[24] S. E. Hove and B. Anda, “Experiences from conducting semi-structured interviews in empirical software engineering research,” in 11th IEEE Inter-national Software Metrics Symposium (METRICS’05).IEEE, 2005, pp.10–pp.

[25] R. W. Gregory, “Design science research and the grounded theory method: Characteristics, differences, and complementary uses,” in Theory-guided modeling and empiricism in information systems research. Springer, 2011,pp. 111–127.

[26] A. K. Shenton, “Strategies for ensuring trustworthiness in qualitative re-search projects,”Education for information, vol. 22, no. 2, pp. 63–75, 2004.

[27] R. Alexander, R. Hawkins, and T. Kelly, “Security assurance cases: motivation and the state of the art,”High Integrity Systems Engineering Department of Computer Science University of York Deramore Lane York YO105GH, 2011.

[28] M. Mohamad, A. Astrom, O. Askerdal, J. Borg, and R. Scandariato, “Security assurance cases for road vehicles: an industry perspective,”arXiv preprint arXiv:2003.14106, 2020

[29] J. D. Brown, “What is construct validity, ”Available at jalt. org/test/bro8.htm (accessed 10 June 2013), 2000.

[30] E. K. H. Fong and D. A. Wheeler, “A sample security assurance case pattern,” 2018.

[31] P. Kotz e, K. Renaud, K. Koukouletsos, B. Khazaei, and A. Dearden, “Patterns, anti-patterns and guidelines–effective aids to teaching hci principles,”in Inventivity: Teaching theory, design and innovation in HCI, Proceedingsof of HCIEd2006-1 First Joint BCS/IFIP WG13. 1/ICS/EU CONVIVIOHCI Educators’ Workshop, 23-24 March 2006, Limerick, Ireland. Citeseer,2006, pp. 109–114.

APPENDIX A
EVALUATION QUESTIONNAIRE FOR THE FIRST ITERATION

1.1. What is your role?

1.2. How long have you been working at your current role?

1.3. What's the definition of a secure product for you?

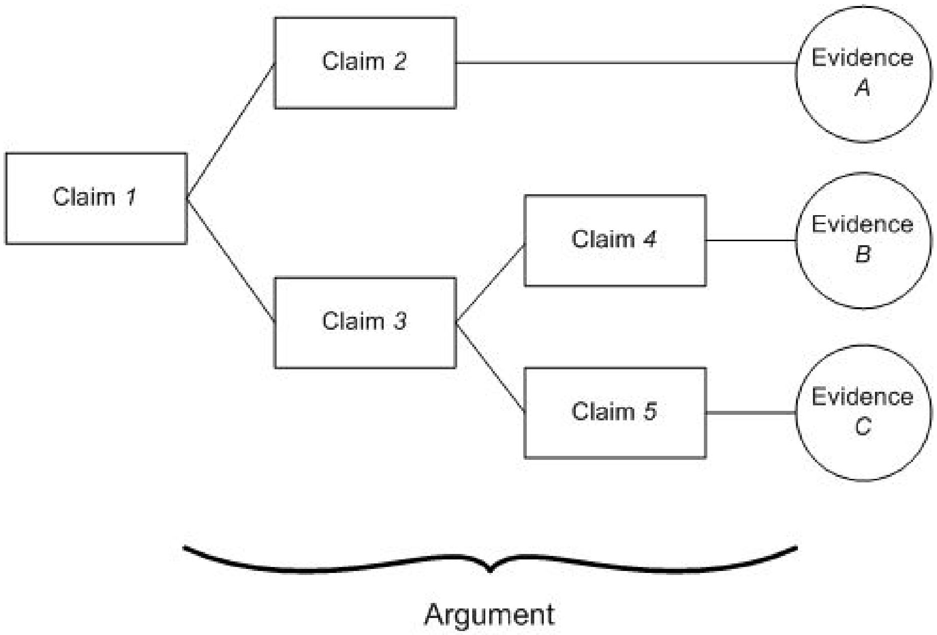
1.4. By looking at the presented artefact, do you think there is anything missing that is in use by your company?

1.5. Do you think there is a need to add more practices and techniques to ensure security?

1.6. Are any of these redundant?

1.7. Would this document be helpful to create SAC?

APPENDIX B
SIMPLE EXAMPLE OF SAC



APPENDIX C
EVALUATION DATA FROM ITERATION 1 DIVIDED INTO THEMES

Theme	Definition	Questions	Answer
Demographic	**Participants' backgrounds and knowledge regarding SAC.**	Q1.1: What is your role?	P1 - “CTO”
			P2 - “Software Developer”
		Q1.2: How long have you been working at your current role?	P1 - “3 years”
			P2 - “3 years”
Values	**Understanding what the participant regards as valuable when it comes to security.**	Q1.3: What’s the definition of a secure product for you?	P1 - “Privacy of data, users shouldn’t be able to access and see data they are not allowed to.”
			P2 - “A secure product in this context would be something that is secure from the entry points by the user, basically through the browser, API and HTTP.”
		Q1.5: Do you think there is a need to add more practices and techniques to ensure security?	P1 - “I don't think we are missing any big areas, but penetration testing could be useful.”
			P2 - “I would need more time to answer that, but to give a blank answer you could always tighten up your security but it would be at the cost of convenience of certain things. Without decreasing convenience, I don't think we should add anything at this point. I think it’s quite good for a service that is run over the web.”
		Q1.6: Are any of these redundant?	P1 - “Monitoring and logging overlaps in some cases, but I think it’s good to keep them separated.”
			P2 - “I don't think having

			encryption and Cryptographic controls as seperate makes sense.”
Structure	**In what way and how the company is taking measurements to assure security and comply with practices before creation of SAC.**	Q1.4: By looking at the presented artefact, do you think there is anything missing that is in use by your company?	P1 - “I think if you have covered what’s in the whitepaper, you have the main things.”
			P2 - “I would need more time to look at it but from what I see, it looks like all the things we are doing and they provide reasonable security.”
Usefulness	**In what way will SAC be useful to the company, who will benefit from it and how can it be used.**	Q1.7: Would artefact 1 be helpful to create SAC?	P1 - “I guess so, but I’m also interested in understanding how SAC could be defined from this.”
			P2 - “From what I have seen, yes. From the definition of SAC you given me, we can create SAC for all of the things mentioned in the document (artefact 1)”

APPENDIX D
DATA COLLECTION INTERVIEW FOR THE SECOND ITERATION

2. a

2.1. As of today, is there any security assurance done in your company? To make sure that a certain product or function is secure.

2.2. If yes, what kind of security assurance do you have in place today?

2.3. If yes on 1, who do you present this security assurance to? Who is interested to know that your product is secure?

2.4. How do you make sure the product as a whole is secure? Is there anyone who does that? (not just different parts like logging, encryption)

2.5. Were you familiar with security assurance cases before looking at the provided example?

2.6. If yes, have you created a security assurance case?

2.7. Do you think encryption and logging requirements would be useful as claims for ensuring security of patients' data?

2.8. Are you compliant with these practices?

2.9. If yes, how do you prove that these practices are in compliance? (do you have a way to show that?).

2.10. For the selected practices, can you provide us with evidence to justify the claims and the sub claims? for example, test reports, tool output etc.

2.11. In which part of the development process these practices are addressed?

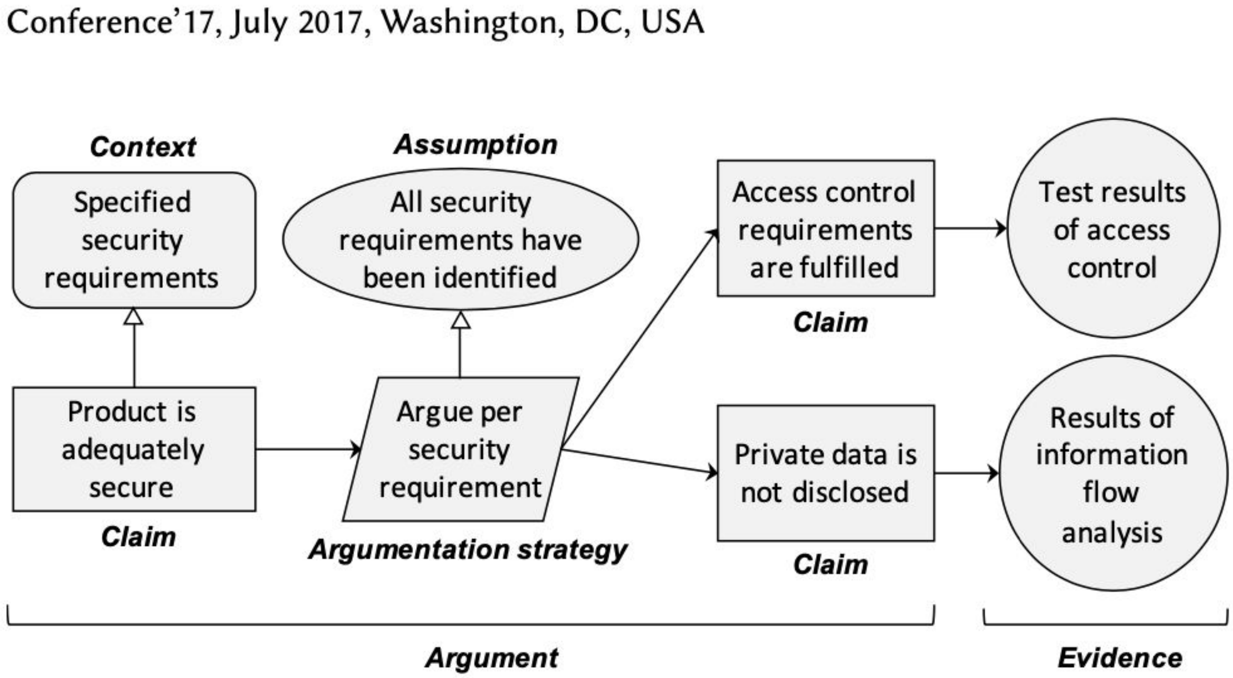
2.12. How can your company make use of SAC?

2.13. Who would use it (roles)? In what way would it help them?

2.14. What would be the benefit of using an abstract SAC? (A less technical detailed SAC, presented in an easier way for someone non-technical to understand, in another words, a low level of details)

2.15. Do you think it's more useful to have 1 SAC for the system as a whole or separate SAC'S for different parts of the system?

APPENDIX E
DETAILED EXAMPLE OF SAC [28]



Conference’17, July 2017, Washington, DC, USA

Context
Specified security requirements
Assumption
All security requirements have been identified
Access control requirements are fulfilled
Test results of access control
Claim
Product is adequately secure
Argue per security requirement
Private data is not disclosed
Results of information flow analysis
Claim
Argumentation strategy
Claim
Argument
Evidence

APPENDIX F
DATA COLLECTION INTERVIEW FROM ITERATION 2 DIVIDED INTO THEMES

Theme	Definition	Questions	Answer
Demographic	**Participants' backgrounds and knowledge regarding SAC.**	Q2.5: Were you familiar with security assurance cases before looking at the provided example?	P1 - “No I haven't seen it before, but it’s reasonable that you provide claims and then evidence of the claims. ”
			P2 - “Not in this particular format, no.”
		Q2:6 If yes, have you created a security assurance case?	P1 - “-”
			P2 - “-”
Values	**Understanding what the participant regards as valuable when it comes to security.**	Q2.3: If yes on 2.1, who do you present this security assurance to? Who is interested to know that your product is secure?	P1 - “I would say mainly any auditor that looks at specific certifications, maybe customers as well.”
			P2 - “”

		Q2.7: Do you think encryption and logging requirements would be useful as claims for ensuring security of patients' data?	P1 - “I think the claim should be, if you don't have the right credentials, you shouldn’t be able to see any information and encryption is the method that we are trying to enforce that claim”
			P2 - “When it comes to logging, be extra careful. Encryption is fine, but when we are logging we make sure we have filters built into the program and drop certain things, we don’t log everything. If anything is personally identifiable we don't log those, it can be in the database. Not everyone has the permission to view the logs in our cloud service, it’s only people who have access that can see it.”
Structure	**In what way and how the company is taking measurements to assure security and comply with practices before creation of SAC.**	Q2.1: As of today, is there any security assurance done in your company? To make sure that a certain product or function is secure.	P1 - “Not documented in the same fashion as in a SAC, but yes we have some.”
			P2 - “I know we have done enough tests of the process of getting different certifications. The question is a bit vague and open, so my answer will be a bit vague. Ofcourse, yes we do regularly check that we are secure, but this is done inhouse, we do it as developers. However we don’t schedule it, except if a certificate requires it. Otherwise all of these security decisions are baked in during development.”
		Q2.2: If yes on 2.1, what kind of security assurance do you have in place today?	P1 - “For example one of them is Audit trail for HIPAA compliance, to make sure users are only looking at data they are allowed to look at. We get trails of what data users are looking at and store them up until 200 days.” “Another example is that we have encryption for all traffic both in transit (sending data) and at REST (storing data), all the files are encrypted. When any operations are performed on the infrastructure, we use encrypted channels”.
			P2 - “”
		Q2.4: How do you make sure the product as a whole is secure? Is there anyone who does that?	P1 - “There is no single person in charge of that, but we have one guy in the developer team who does most of the infrastructure stuff. It’s a common effort when we are setting it up, making sure we follow the best practices and have a reasonable amount of security.”
			P2 - “We don’t have a separate person assigned for this, so it’s kind of baked into the development process. We start out with a base of what we think is secure, like all the

			TLS stuff, encryption stuff, making sure the passwords are not easily guessable, using the right libraries and all that kind of stuff. For example if there are new places for user input, we make sure to sanitize it. A lot of the stuff is really hand in hand with the development. If we see something isn't secure, we fix it. It's not scheduled per say, but it's always there."
		Q2.8:Are you compliant with these practices?	P1 - "Yes I think so."
			P2 - "In general yes, but if you would like me to be really really sure, i'd need more time to look through it."
		Q2.9:If yes on 2.8, how do you prove that these practices are in compliance? (do you have a way to show that?)	P1 - "No, not really."
			P2 - "So, I would give you an example, when we had to certify for CE, HIPAA, one person usually drives it. Then we go through each of the points (requirements in standards) and we ensure that we are running it, kind of like a drill and check off stuff in the list"
		Q2.10: For the selected practices, can you provide us with evidence to justify the claims and the sub claims? For example, test reports, tool output etc.	P1 - "I think that's the main reason we are doing this thesis work, because we don't have that. By defining the claims and need for evidence, we can generate those evidence. It's not something we have upfront."
			P2 - "I think to answer that, you have to give me an exact format of what you are looking for, in terms of logging and monitoring I think we can satisfy that, there should be no problem. We could do a test run for you, like a random sample so you can see there is logging, there is monitoring."
		Q2.11: In which part of the development process these practices are addressed?	P1 - "In the development of the infrastructure."
			P2 - "In the 3 weekly sprints of development process"
Usefulness	**In what way will SAC be useful to the company, who will benefit from it and how can it be used.**	Q2.12: How can your company make use of SAC?	P1 - "Definitely would be useful to understand what claims we have and guide us towards evidence as output."
			P2 - "I think it will be very beneficial because it will be something that is gonna be like a manifest, something that you can test against, you can check against. Because right now like I said, a lot of these things are based on experience, and we might have written some stuff down somewhere. But this is gonna be

			more structured. So it’s gonna add structure and a checklist sort of a thing.”
		Q2.13: Who would use it (roles)? In what way would it help them?	P1 - “In terms of development, it’s gonna be useful to know what the requirements for different certifications are in terms of security.”
			P2 - “The dev team, but the product dev team more than the dev team, it would be a good bullet list to check against.”
		Q2.14: What would be the benefit of using an abstract SAC? (A high level structure, less technical/detailed)	P1 - “I’m not sure, but it would be less clear that the evidence you provide is actually fulfilling that abstract claim.”
			P2 - “I think the abstract cases would make more sense for business owners, product owners and probably customer base. But maybe it’s not gonna be as useful directly, because when you are doing security you wanna be as precise as possible in my opinion because that's how you get good security. Abstract cases are very good for convening what we do rather than how we do it, but when you want to give something to the product team to get that checkmark, you wanna be precise and even get into what possible algorithms to use for certain certificates.”
		Q2.15: Do you think it’s more useful to have 1 SAC for the system as a whole or separate SAC’S for different parts of the system?	P1 - “I would say different, with different focus. The division into user privacy. For example one user is authenticated and is able to look at data in the system but they shouldn't be able to look at other people's data. I think this is a very different case from any other random person trying to break into a system and they shouldn't be able to see any information. The claim and evidence for these cases would be very different.”
			P2 - “Should be different for different scenarios, having just one makes it more generic. I guess it depends on what level of detail you wanna get into.”

APPENDIX G
ARTEFACT 1 FIRST DRAFT

External requirements for SAC to ensure the security for cloud services provider	
Practice	**Description**
Logging	System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.
Monitoring	Security features are monitored automatically and through planned internal audits to detect and mitigate actual or track potential vulnerabilities and both actual and potential intrusions.
Cryptographic controls	There should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.
Backup	Appropriate backups should be taken and retained in accordance with a backup policy.
Training	Programmers should be training regularly in best coding practices that help to ensure security. e.g, define security requirements, Heed compiler warnings.
Redundancies	IT facilities should have sufficient redundancy to satisfy availability requirements.
Encryption	All connections between users and web servers need to be encrypted using HTTPS/TLS, which means that no other person or entity can read or change the information exchanged. All stored user data, including sample files and database should be encrypted.

Accessibility control	All the servers are Protected by stateful packet inspection firewalls, with only necessary services allowed. Offer tight control sharing, only specific users can access data. changes in user permissions that are initiated automatically by the information system and those initiated by an administrator.
Firewalls	Uses strict stateful network firewalls to protect all servers, including those processing confidential user data.
HIPAA compliance	Follow the rules established by HIPAA for the implementation of IT and software security controls. These requirements are important in order to protect personal health information.
Records retention	Customers should have the ability to delete data and reports when no longer needed or when patient or donor consent is revoked. Customer data are stored until deleted by the customer, providing complete control over record retention and destruction. Project Administrators can lock projects to prevent accidental deletion of any files by anyone other than the project Administrators.

APPENDIX H
EVALUATION QUESTIONNAIRE FOR THE SECOND ITERATION

2.16. Is the structure of the security assurance case clear? (*the order and how its broken down: claims - arguments - evidence, with reference to context*)

2.17. Are the notations understandable?

2.18. Do you think the SAC is self-explanatory?

2.19. What do you think about the case we selected (top-claim function)? Is it important to your company to have this part of the system shown in a structured way?

2.20. Do you think there are details missing in the SAC? If yes, in which part?

2.21. Would this SAC be helpful to show that the company has security in place, to different stakeholders?

2.22. Can you think of any other use cases for the SAC?

2.23. Do you think the first level of the claims 1.2,1.3,1.4, are consistent with the first argument?

2.24. Are the claims well constructed and aligned with company claims?

2.25. Do you think the arguments are understandable?

2.26. Do you think this SAC can be used as guidelines to create more SACs for other parts of your system?

2.27. Do you think companies within the same domain can use this SAC as guidelines to create SAC for their products?

2.28. Would the creation and maintenance of SACs be a part of the development process? If so, in which part?

2.29. Who would be responsible to create and maintain SACs?

2.30. Are all the presented evidences implemented in your system?

2.31. Does the provided evidences justify the claims being made?

2.32. By looking at the presented artefact, do you think it’s aligned with your system?

APPENDIX I
EVALUATION DATA FROM ITERATION 2 DIVIDED INTO THEMES

Theme	Definition	Questions	Answer
Correctness	**How much the SAC actually reflects the architecture and the applied security mechanisms in the company.**	Q2.19: What do you think about the case we selected (top-claim function)? Is it important to your company to have this part of the system shown in a structured way?	P1 - " Yes, it doesn't have to necessarily be called the patient's date because what we're running analysis on is bacteria. So in the perfect case, it's not patient data. actually bacteria data. I'm thinking just data or sample data. So it's not really wrong that you say patient data. It's so it's not only DNA data. So it's sample data. I think. Yeah, it would be good. From my aspect, I like the idea of visualizing, visualizing this kind of information. From the claim and going down to the evidence a structured manner. "
			P2 - "Yeah I think so, it's one of the core parts. It is a reasonably good claim to work on, security wise. "
			P3 - "Yeah definitely, this is one of the questions that come from customers when it comes to security."
		Q2.20: Do you think there are details missing in the SAC? If yes, in which part?	P1 - ""
			P2 - "I think the steps are fairly, at least for the second level of claims C1.1-C1.4, they are fairly broad enough. I guess you can always dig down and find individual steps, but those four definitely cover. Even when I quickly looked at it 2 hours ago, I think the main steps are covered." P2 - Like P3 said, it depends on the level of detail. It is not mentioned for example file storage or blob storage, only database storage is mentioned. But there is more than that. So for example C1.3.1 if samples are not stored in web server. Where are they stored? But the claims are correct, they are not stored on the web server and the files are validated.
			P3 - "I mean of course since you have only looked at the system for a short while, there are some detailed stuff missing in the whole picture and if we start to add those, maybe it will come up and even change the first level. So I am not sure, but it doesn't talk much about how we store the samples, it mentions we don't store them on the web server which is true but we store them at other places that are encrypted and all that might be pretty important and if you want to divide it up to claim, it maybe boils up all the way to first level. "
		Q2.23: Do you think the first level of the	P1 - " Yeah, I understand but this something more technical, you can ask P2 and P3 to get the answer. "
			P2 - "I would say, yes. I agree that those four things are

		claims 1.2,1.3,1.4, are consistent with the first argument?	consistent. I guess in between C1.3-C.1-4, is probably the point P3 mentioned that uploading samples to the website is secure, but we also wanna say the storage after uploading the samples are encrypted or secure. Right, because that is a different step from the database, consider it like a file server because we have huge files. If you wanna add it, it’s stored in a cloud server, because I think it’s fairly separated from the database and the web server. ”
			P3 - “-”
		Q2.24: Are the claims well constructed and aligned with company claims?	P1 - “”
			P2 - “There was one, the one I thought wasn’t correct was E1.4.1.3-1, which is the connection to the database that is made through SSH keys. I mean yes we use a secure connection, but it’s a database that is not accessible, none of the ports are open actually. So what we use is a tunnel, it’s a cloud service provider tool that helps us to tunnel through the server without opening any open ports, which means literally nobody can ssh into it. So I guess yeah, we don’t really connect to database in that sense, our application connects to the database using a tunnel and that’s about it. We can do external backups, we never have to log in to the server. The claim is true, but the evidence is something else I guess you could say something like: ‘Secure encrypted tunnel or reversed tunnel’. I think most of the other things look okay. We could walk through all of them actually” P2- “So I also realized, the protection against DDOS, we had this implemented in the past but the product we were using we couldn't keep using. Right now we have it in the load balancer in the cloud service provider itself, but we were using a DDOS service provider in the past but we don't use it anymore because of hipaa compliances. It’s not that it's not implemented, we can use it when needed but now we don't have this like DDOS service provider. I guess DDOS is very specific, but could be something like traffic load instead.”
			P3 - “For example password manager is not enforced, we have told people this is a good thing to use. But we don’t check if people actually use it. It’s recommended.”

			P3 - “Small detail in C1.2.2, you mention download data. The user is actually not able to download samples, they are able to download results of the samples like graphs and pictures.
		Q2.30: Are all the presented evidences implemented in your system?	P1 - “”
			P2 - “So I guess, those were the main things that P3 mentioned. But also the limited access to the production database, it is in fact correct but the limited means that only our application gets to write, nobody else has permission. The writing process is a very difficult path. That means there is no write access to people no whatsoever, only application. It’s easy to read out but extremely difficult to write. ”
			P3 - “Yeah so except the ones we mentioned, the SSH case, password manager and ddos protection.”
		Q2.32: By looking at the presented artefact, do you think it’s aligned with your system?	P1 - “”
			P2 - “Yeah I agree” Final comments - “I guess to add to that, we are a small team and small company, so in some sense this knowledge is fairly compressed in a small team, which is the benefit of a small team. But I think this would be extremely useful in other places where there are sub-teams, each working in their own little bubbles. So having one of these to verify end-to-end that your system is secure, so I think in those cases it would be extremely useful to have this kind of SAC. I can see very good benefits, regardless of the level of details”
			P3 - “Yes, I am actually quite impressed. How did you dig up all this information?” Final comments - “For me it was the first time I looked at things like this, I must say I kind of liked it, it’s easy to follow and gives quite good information.”
Quality	**Making sure the case is understood by the company and useful for them.**	Q2.16: Is the structure of the security assurance case clear? (the order and how its broken down: claims - arguments - evidence, with reference to context)	P1 - “Yeah, for sure. But, I'm just struggling a little bit with understanding and how this document should be used in relation to other documents and how it fits in the process. So that means we have to create these kinds of documents and we need to keep them updated. And I think it's very beneficial to have a graphical structure. Something, you know, like a visualization I think is a very good thing. But then for, for example, should, the links to the evidence be even more explicit. So for example, if we look at E1.2.2-1, so should that be even more specific to the actual evidence that it's actually handled in the web framework? should it be connected to the actual function?. I think the structure is there, but you can then argue if the references should be more detailed. I liked the structure very much, it's very clear what is the evidence and the requirements with the claims and the arguing. I'm just a bit

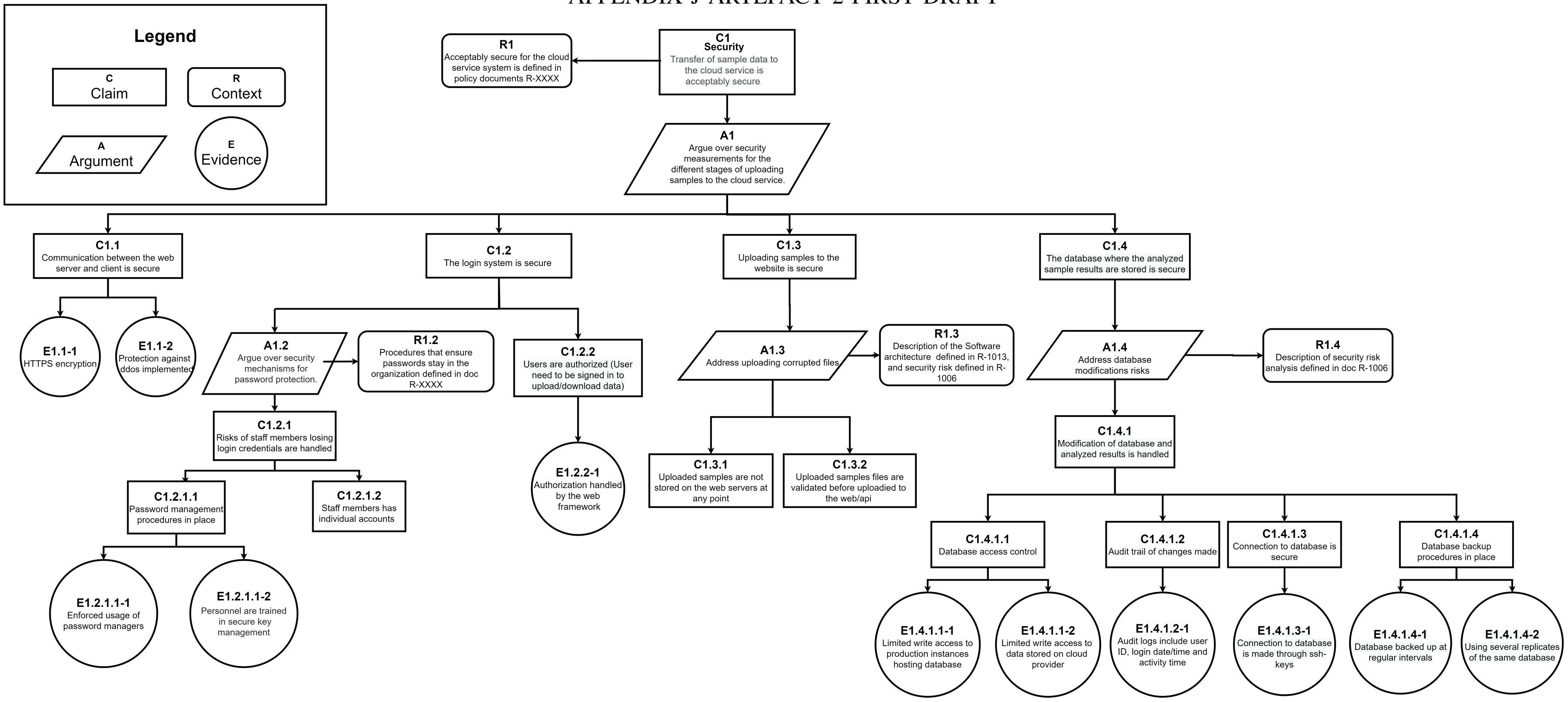
			struggling with how we fit this today and that's not really up for me to answer. It's more along the lines of, of the development team and how they see this document. from a quality perspective. From my perspective, I think it's beneficial, but I think also that this information should be also available through the regular requirements documents. Something that we don't really have. This is a way, so let's say that we don't have full documentation of our product, but then we focused on security because it's so important. So then we decide to go with this method of documenting our approach to security. But then we have to make sure everybody on board uses this method for documenting our approach for example toward security.“
			P2 - “Yes, it’s fairly clear at least with the framework. Makes sense with the things in the legend, when I look at it.”
			P3 - “I also agree it’s clear, even without seeing anything like this before. It was easy enough to follow.”
		Q2.17: Are the notations understandable ?	P1 - “ yeah yeah, for sure. ”
			P2 - “One thing I find interesting about this flowchart is that it only has possibility for a happy path, in the sense we made a claim, this is how we argue and this is how the claim was verified. Of course in this case it works, and why it’s SAC but what if it didn’t work, how would you represent that in this graph? Let’s say personnel aren't trained in secure key management. It’s what I don’t see in this graph.” P2 - “I don't know how SAC exactly works, but I was thinking if you could add a color layer, then you can represent those things. Red or green for evidence.”
			P3 - “Yeah, you could see the symbols and distinguish stuff, but I don't know exactly what you mean with the argument for example.”
		Q.2.18: Do you think the SAC is self-explanatory ?	P1 - “ I can definitely, I understand it.with the legend is everything's really clear. You would need some contextual background information. So are there several security cases. Are they complete or not? you know, things like that, which is not visible in the figure. I don't think that's a problem, I mean, it's very self explanatory. One idea can be that you can have a dashed circle under or something that indicates that,here's something missing. So then this could be also used as kind of a gap analysis to identify weaknesses. And gaps in the argumentation, so a dash line indicating that we need more claims here.This is just an example.”
			P2 - “At least the way I see it, you are building up a case and with that it makes sense. But I guess it comes back to that idea, the case not covering the absence of certain things, is what I miss. But when I look at it it’s obvious that

			we have this point and we are trying to prove that this point is valid with all the evidence.”
			P3 - “I think it’s clear and you can follow, but something to make it even better. Would be a short description of what SAC is and maybe go through for these things in the legend. Max 1 paragraph for each describing what it is”
		Q2.25: Do you think the arguments are understandable?	P1 - “”
			P2 - “I think it’s fairly understandable, this is the thing does SAC require the argument to be extremely precise or not, I guess like the login system is secure, you could really build a lot on that. You could go down to for example what hashing algorithm you are using. I guess otherwise arguments are understandable, but yeah they don't define the level of detail I am supposed to go in.” P2 - “Like address uploading corrupted files, right? Like take, for example, there's so many ways to, to possibly think about corrupted files, like intentional corruption, network corruption, you know, like just accidental corruption. For example we accept text files that are zipped. It's a particular kind of text file called fasta and one could actually just wrap, like what you say, zip, some other files and upload it. I mean, we do some very basic validation, but the thing is the, the moment our, our queue picks up the work, it will fail because clearly when the job starts at stuff it fails, but we do not do like deep validation of a, you know, hundreds of types of file in the browser because you know, it's not reasonable to get the browser stuck doing that.” P2 - “But otherwise they are good, they are quite understandable for sure, but they don't tell me what level of detail I am supposed to act on”.
			P3 - “Not much I wanna add to that, I agree with P2.”
		Q2.31: Does the provided evidences justify the claims being made?	P1 - “”
			P2 - “Yes, I mean I guess I would say yes, my hardest part of digesting SACs has been that for claims, we dont show the absence of bugs. It only shows what we have done.” P2 - “So yes sorry to answer your question, yes it does but I have a problem with this framework, that’s all. But I guess that’s how you design threat scenarios, you assume the level of the things you wanna deal with and beyond that isn’t covered, so makes sense.”
			P3 - “I agree with P2, I also could add so much more details maybe not showing here, of course it's hard to fit all the bits and pieces to this, yeah. On a high level of evidence it’s good I would say.”

Value	**Whether the case (and similar ones) would be valuable to show a certain level of security in the company, and in this case, who would be interested and why.**	Q2.21: Would this SAC be helpful to show that the company has security in place, to different stakeholders?	P1 - “yes, I think that could be one way of using it. Depending on what the stakeholder is, I think it would be more of the technical stakeholder because if I wouldn't want to show this to customers, I wouldn't want to show it to sales for example. Just the reason being that you don't want to show, I mean this is quite a lot of information about the system that you might not show them. I think if you want to present information towards sales or towards customers, it's more along the lines of like a white paper. But for the technical team and for quality and things like that, I think it's a very good document, but it needs to be put into its place in the process. because you don't want to have just another document, you want to have something that feels its purpose. ”
			P2 - “We talked a bit last time about this, but I think different stakeholders have different interests in how deep you want to go, define the level of detail. Overall I think this is great to probably present to non-technical leaderships and non-technical teams, it’s okay. But if you present to technical teams, then I for example would ask to put more detail in this, like every single step. It would take a long while though, because we would go through every single thing. But otherwise I think it is good.”
			P3 - “Yeah I kind of agree, it depends on the stakeholders, for a customer they probably don’t wanna look at this, but for some authority that is approving us, they would maybe want to see something like this.” P3- “If a customer really wanted to see this, they could and some customers are actually that interested in details, but most of them are not I guess, it’s not like sales material sales people would bring with them.”
		Q2.22: Can you think of any other use cases for the SAC?	P1 - “”
			P2 - “Yeah so, it is a good framework for thinking, on that I definitely agree. But the level of detail depends on every person who cares.
			P3 - “I guess we are also stakeholders but for developer to developer communication it could also help, for a new comers to find their way around the system and also just to show ‘I am working on this high level security feature on the product, this is a way to prove that I am thinking about all the security issues.’”
Generalization	**If the case can be used as**	Q2.26: Do you think this SAC can be used as	P1 - “Yeah, yeah, for sure. Of course you could.”

	guidelines to create SAC for other products within the company but also in the domain.	guidelines to create more SACs for other parts of your system?	P2 - “Yes, of course.”
			P3 - “Yeah the quick answer is yes, it’s possible.”
		Q2.27: Do you think companies within the same domain can use this SAC as guidelines to create SAC for their products?	P1 - “”
			P2 - “Yeah, and I guess that’s where the difference between being general enough and specific enough makes the difference ” P2 - “But it might change some on the lower levels of the SAC, because people maybe don't use the same stuff, like in the claims people maybe don't use web framework or database for example.”
			P3 - “Yeah I guess, it’s not for a particular product, I guess anyone could use this.”
Challenges	**How the cases will be maintained and who will take responsibility to create and update cases. Integrating these steps, in the current company process.**	Q2.28: Would the creation and maintenance of SACs be a part of the development process? If so, in which part?	P1 - “”
			P2 - “Like the level of detail that is here, doesn’t change that often. So I guess it’s one off thing that is gonna be like architecture stuff, design. Then it kind of is stale in some sense ”
			P3 - “I guess this is a tricky question, it’s of course really nice to have this. It gives a lot of information, but it also takes a lot of effort to both create and maintain, so I guess it’s important to value the effort against what it actually gives back. Documentation that is made to be used on a regular basis, is gonna find it’s way of being used in the process regardless who is responsible for it. I think just putting this to a person, it becomes a weird thing to maintain, but instead if you can flip it over and kind of make it something useful to drive team decisions, then it’s gonna find a much better home otherwise it’s just a chore.”
		Q2.29: Who would be responsible to create and maintain SACs?	P1 - “”
			P2 - “Yeah I think like documentation that tries to cover these kinds of things, it’s easy to do it the first time, than after that unless it's a clear path for the usage of it on some kind of regular basis it usually doesn’t work out.”
			P3 - “So I guess it depends on who the main target of the SAC is, who the stakeholder is. As said earlier for communication between developers it’s good but then you need more detail and developers should maintain it. If it’s more for regulatory stuff, then someone like P1 (quality manager) but of course he can’t answer all of these questions on his own.”

APPENDIX J ARTEFACT 2 FIRST DRAFT


Legend
C
Claim
R
Context
A
Argument
E
Evidence
C1
Security
Transfer of sample data to the cloud service is acceptably secure
R1
Acceptably secure for the cloud service system is defined in policy documents R-XXXX
A1
Argue over security measurements for the different stages of uploading samples to the cloud service.
C1.1
Communication between the web server and client is secure
E1.1-1
HTTPS encryption
E1.1-2
Protection against ddos implemented
C1.2
The login system is secure
A1.2
Argue over security mechanisms for password protection.
R1.2
Procedures that ensure passwords stay in the organization defined in doc R-XXXX
C1.2.2
Users are authorized (User need to be signed in to upload/download data)
E1.2.2-1
Authorization handled by the web framework
C1.2.1
Risks of staff members losing login credentials are handled
C1.2.1.1
Password management procedures in place
C1.2.1.2
Staff members has individual accounts
E1.2.1.1-1
Enforced usage of password managers
E1.2.1.1-2
Personnel are trained in secure key management
C1.3
Uploading samples to the website is secure
A1.3
Address uploading corrupted files
R1.3
Description of the Software architecture defined in R-1013, and security risk defined in R-1006
C1.3.1
Uploaded samples are not stored on the web servers at any point
C1.3.2
Uploaded samples files are validated before uploadied to the web/api
C1.4
The database where the analyzed sample results are stored is secure
A1.4
Address database modifications risks
R1.4
Description of security risk analysis defined in doc R-1006
C1.4.1
Modification of database and analyzed results is handled
C1.4.1.1
Database access control
C1.4.1.2
Audit trail of changes made
C1.4.1.3
Connection to database is secure
C1.4.1.4
Database backup procedures in place
E1.4.1.1-1
Limited write access to production instances hosting database
E1.4.1.1-2
Limited write access to data stored on cloud provider
E1.4.1.2-1
Audit logs include user ID, login date/time and activity time
E1.4.1.3-1
Connection to database is made through ssh-keys
E1.4.1.4-1
Database backed up at regular intervals
E1.4.1.4-2
Using several replicates of the same database