

Jonas Fjeldheim Simonsen
Sondre Steinsvik Bakke
Murad Dimen

CyberTest4You: A three-way Model for Evaluating Compliance and General Maturity in IT Security

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Jia-Chun Lin
May 2023

Jonas Fjeldheim Simonsen
Sondre Steinsvik Bakke
Murad Dimen

CyberTest4You: A three-way Model for Evaluating Compliance and General Maturity in IT Security

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Jia-Chun Lin
May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology



CyberTest4You: A three-way Model for Evaluating Compliance and General Maturity in IT Security

Group 120

May 2023

Abstract

Sopra Steira is an internationally established consulting company within digitalization. A part of their job is to help companies comply with local and international frameworks for IT security and privacy. To be able to check to what degree companies comply with these frameworks, it can be used a three-way-model. The goal of this assignment is to create a model like this. The model explains what laws and frameworks an organization has to follow based on their sector of expertise, and then gives a rating based on the organization's answers. The model will also give a rating based on the general maturity of the organization within information security. This maturity rating is based on the established ISO27001 standard, which is among the best standards when measuring and managing information security.

Sammen drag

Sopra Steria er et anerkjent multinasjonalt konsulentselskap innenfor digitalisering. En del av jobben deres er å hjelpe selskaper til å overholde lokale og internasjonale regler og standarder innenfor og IT-sikkerhet og personvern. For å undersøke i hvor stor grad selskapene klarer å overholde disse reglene kan man bruke en såkalt treveismodel. Målet med denne oppgaven er å lage en slik treveismodell. Modellen vil forklare hva slags lover og retningslinjer organisasjonen må følge, avhengig av hva slags sektor den tilhører, og modellen gir deretter en vurdering basert på organisasjonens svar. Modellen vil også gi en vurdering av den generelle modenheten til bedriften sin IT-sikkerhet. Denne modenhetsmålingen er basert på den anerkjente ISO27001 standarden, som er en av de beste standardene for å måle og administrere informasjonssikkerhet.

Preface

It has been a very educational and interesting experience to work on this bachelor project. The assignment we were given by Sopra Steira has been both challenging and fun to work with, and we have learned a lot through the process. Compliance with information security is a big challenge for companies, and we hope our model can make it easier for their clients to be sufficiently compliant, and also get a specific understanding of where the bottlenecks and vulnerable areas are.

We would like to thank the people that have helped us during our thesis. Especially Tea Knudsen from Sopra Steira has been incredibly helpful and answered whatever question we had. Our supervisor Jia-Chun Lin has been extremely helpful as well and gave us great tutorials and general tips on how to write our thesis. We would not manage to complete our thesis without her. We would also like to thank everyone that helped us complete the user evaluation of our model, and Sopra Steira for feedback.

Contents

Abstract	iii
Sammendrag	v
Preface	vii
Contents	ix
Figures	xiii
Tables	xv
List of Listings	xvii
Acronyms	xix
Glossary	xxi
1 Introduction	1
1.1 Background	1
1.2 Project Description	1
1.3 Project Goal	2
1.4 Target audience	2
1.5 Scope and limitations	2
1.6 Project Group	3
1.7 Thesis structure	3
2 Background	5
2.1 General Data Protection Regulation (GDPR)	5
2.2 Information Security Management System	6
2.3 The International Organization for Standardization	6
2.4 ISO27001 Certification	6
2.5 Relevance in modern times	7
2.6 Related work	8
3 Requirements	9
3.1 Functional Requirements	9
3.2 Non-Functional Requirements	9
3.3 Use Cases	10
3.4 Detailed use cases	10
4 Design	13
4.1 System architecture	13
4.2 Flowchart of application	14
4.3 Sequence diagram	16
4.4 Backend	19

4.5	Frontend	22
4.6	Exported Data	24
5	Development	25
5.1	Development model	25
5.2	Documentation	26
5.3	Workflow	26
6	Implementation	27
6.1	Infrastructure	27
6.1.1	Development environment	27
6.1.2	Production environment	27
6.2	Frontend	30
6.2.1	Homepage	30
6.2.2	Sectors	30
6.2.3	About	31
6.2.4	Login interface	31
6.2.5	Testing Center	33
6.2.6	General Maturity Rating Test	33
6.2.7	Display questionnaire results	36
6.2.8	Compare Results	40
6.2.9	Test compliance to legal regulations	43
6.2.10	Display results for legal regulations	46
6.2.11	Admin Panel	47
6.3	Backend	52
6.3.1	Database	52
6.3.2	Login and Session start Process	53
6.3.3	Session check Process	55
6.3.4	Logout Process	55
6.3.5	API	56
6.3.6	JSON file	56
6.3.7	Admin panel backend	58
7	Discussion	63
7.1	Evaluation	63
7.1.1	Overall functional requirements	63
7.1.2	Functional requirements in detail	64
7.1.3	Non-Functional Requirements	67
7.2	User feedback	68
7.3	Approach	72
7.3.1	Problems	72
8	Conclusion	73
8.1	Conclusion	73
8.2	Learning outcome	73
8.3	Further work	75
8.4	Summary	76
	Bibliography	77

A Project Agreement	81
B Project Plan	89
C Project Task	109
D Log	111

Figures

3.1	Use case	10
4.1	High-level design architecture	14
4.2	Flowchart of web interface Questionnaire side	15
4.3	Flowchart of web interface Result display side	16
4.4	Maturity Rating Sequence diagram	17
4.5	legal regulations Sequence diagram	18
4.6	Admin panel Sequence diagram	19
6.1	Server Architecture	28
6.2	Homepage	30
6.3	About interface	31
6.4	Login interface	32
6.5	Testing Center website	33
6.6	General Maturity Rating Test	34
6.7	Section Descriptions	34
6.8	Questionnaire Results	36
6.9	Display User Answers	40
6.10	Compare results interface	41
6.11	Compare User answers	42
6.12	Choose sector starting page	43
6.13	healthcare questions format	44
6.14	Finance questions format	45
6.15	Display legal results finance example	46
6.16	Display legal results Healthcare example	46
6.17	Admin panel interface	47
6.18	Add User interface	48
6.19	Delete User interface	49
6.20	Add Company interface	49
6.21	Delete Company interface	50
6.22	Database Tables	52
7.1	user Friendliness Pie chart	68
7.2	Understandable descriptions	68

7.3	Time spent to complete Security Maturity questions	69
7.4	How understandable were the security framework questionnaire pie chart	69
7.5	healthcare Time to complete	70
7.6	healthcare Understandable	70
7.7	Finance Understandable questions	71
7.8	Finance Time to complete questions	71

Tables

3.1	Questionnaire legal regulations	11
3.2	Questionnaire technical framework	11
3.3	Display compliance	11
3.4	Export data	11
3.5	Add User	12
3.6	See users	12
7.1	Functional Requirements Testing table	64

List of Listings

1	Login validation function	32
2	Looping through the questions	35
3	Read files data code sample	37
4	Percentage Calculation code sample	39
5	Comparison data calculation code sample	42
6	Open and send requests code sample	51
7	Send a delete request code sample	51
8	Code Example for the DB-connection	53
9	Code Example for the authentication	54
10	Code Example for the session check	55
11	Code Example for the log out	55
12	Code Example get questions	56
13	code sample of questions.json file	57
14	code sample of the results	58
15	Add User Query code sample	59
16	Select company code sample	60
17	Search for user code sample	60
18	Display user tabel code sample	61
19	Delete user code sample	61
20	Add company Query code sample	62

Acronyms

2FA Two-factor authentication. *Glossary: 2FA*

API Application Programming Interface. *Glossary: API*

CSS Cascading Style Sheets. *Glossary: CSS*

GDPR General Data Protection Regulation. *Glossary: GDPR*

GUI Graphical user interface. *Glossary: GUI*

HTML Hyper Text Markup Language. *Glossary: HTML*

ISMS Information Security Management System. *Glossary: ISMS*

ISO International Organization for Standardization. *Glossary: ISO*

JS JavaScript. *Glossary: JavaScript*

JSON JavaScript Object Notation. *Glossary: JSON*

PHP Hypertext Preprocessor. *Glossary: PHP*

Glossary

- LaTeX** Is a markup language especially suited for scientific documents. 26
- 2FA** Is an identity and access management security method that requires two forms of identification to access resources and data.. 7
- API** Is a set of definitions and protocols for building and integrating applications.. 35, 56
- Bootstrap** Open source CSS framework for front-end web development. 22, 30, 31
- CSS** Is a style sheet language that is used to describe the look and formatting of web page. 22, 23, 30, 31, 33
- GDPR** is a European Union-wide data protection framework. ix, 5–7, 76
- GUI** User interface with graphical icons for interacting with devices. 1–3, 10, 20, 22, 75
- HTML** Is the standard markup language for creating Web pages. 22, 23, 30, 31, 33
- ISMS** set of policies and procedures for managing sensitive data within an organization. 6
- ISO27001** is the international standard for information security.. iii, v, 1, 6, 8, 9, 23, 33, 36, 43, 64, 66, 74, 76
- JavaScript** Is a scripting language for creating dynamic web page content. 22–24, 31
- JSON** Is a lightweight data-interchange format. 11, 24, 35, 36, 40, 43, 52, 56, 58, 66, 72
- PHP** General purpose scripting language based on web development. 20, 21, 30, 31, 33, 53, 59

Chapter 1

Introduction

In this chapter, we will cover the general background of the project, what the project consists of, and what the end goal of the project is. Further, we will describe who the target audience is, and what scope limitations have been applied.

1.1 Background

The client for this project is Sopra Steria [1] an international IT-consultant firm that offers consulting services to other organizations regarding IT security, innovation, and sustainability. They are a highly recognized and desired workplace and have been awarded for being Norway's greatest workplace several times. Sopra Steria has given us the task of developing a model for organizations to check their compliance with certain security frameworks and legal regulations.

1.2 Project Description

Sopra Steria has given us the assignment of developing a so-called "three-way model". It is called this because the model is split into three different parts. The model should have a sector that displays an overview of what rules and regulations a company has to follow based on what services they provide. It will then give a rating of how compliant an organization is to the currently existing regulations. In the final part, the model will analyze the current general IT security procedures of the organization. This part is universal for all sectors and will be based on the ISO27001 standard. The test will then use the answers from the company to give a general maturity rating of the company's information security.

We are free to use any technology as we would like to create the model, as long as it is functional. It is however recommended to use technology that is easily available. It should also contain a GUI to simplify the interaction with the model.

1.3 Project Goal

As described in the project description, the goal of this project is to develop and design a functioning three-way model that tests the compatibility with current regulations as well as compliance in regard to security frameworks. It should have a functional GUI that is self-explanatory and easy to use. The model must also include relevant frameworks and regulations in detail, to make sure the users get an accurate and helpful evaluation. The model should be reusable in the future, and able to be modified according to different needs. It should be possible for Sopra Steria (or someone else, if required) to be able to modify the model to be able to do an evaluation of companies within other sectors or different frameworks. The goal is that it also should be possible to do this without much technical knowledge.

We would also like our model to be flexible and possible to be tested from anywhere. By this, we mean that the user should be able to use the model wherever there is an internet connection. The user should also be able to compare test results from the model to different dates. This enables the user to easily measure improvements after changes and improvements have been applied. The end goal of our model is to create a website which is called CyberTest4You so that the users find it helpful.

1.4 Target audience

The target audience for this project is clients/companies that are interested in improving or testing their compliance with regulatory bodies or general IT security standards.

1.5 Scope and limitations

Due to the limited time of the project, and to prevent scope creep, the model will only cover two different sectors. These two sectors are healthcare and finance. This is because it can take a lot of time and work to gather relevant information about what compliances and current legal regulations the sectors need to follow. We realize that focusing on several other sectors would be too time demanding, but as we described in the project goals, this is something that can be modified later according to the requirements of the companies. For example, if they would like to add more sectors.

1.6 Project Group

The group consists of three members all studying Digital Infrastructure and Cyber security at The Norwegian University of Science and Technology (NTNU). The members and their group roles are below.

- **Project leader:** Sondre Bakke
- **Log leader:** Murad Dimen
- **Minute Leader:** Jonas Simonsen

We also have external roles in the supervision of the project in the form of:

- **Sopra Steira representative:** Tea Knudsen
- **NTNU Supervisor:** Jia-Chun Lin

1.7 Thesis structure

- **Chapter 1- Introduction**
Project description- information about the project, who the members are, and the project goal and description.
- **Chapter 2- Background**
Introduction to important legal areas as well as Information management Security Systems and their background.
- **Chapter 3- Requirements**
The requirements of our model and GUI
- **Chapter 4- Design**
Design of the model/application, including how it is hosted
- **Chapter 5- Development process**
The choices we did in terms of the development model and standards
- **Chapter 6- Implementation**
Information about the GUI and tools we used to develop and deploy the model
- **Chapter 7- Discussion**
Discussion about choices made during the project and user feedback on what can be improved in the future
- **Chapter 8- Conclusion**
Conclusion of the thesis. Also a discussion about what further work can be done on the model or the thesis itself.

Chapter 2

Background

In this section, we will describe certain background themes for the assignment and give some descriptions of each of them.

2.1 General Data Protection Regulation (GDPR)

GDPR is EU-wide legislation of how data should be processed and handled. It is very important for businesses to comply with the legislation. If they fail or have inadequate policies surrounding GDPR, the fine could be enormous. The fine can be up to 20 million euros or 4 % of the global turnover of the company within the preceding financial year. [2].

Organizations that need to comply with GDPR have several rules in order to maintain user privacy and secure data. The rules only apply to personal data about individuals, and they do not govern data about companies or any other legal entities [3].

Individuals also have several rights that should be respected and maintained. GDPR includes the right for individuals to have their personal data deleted, which means a company has an obligation to do so unless it is one of the following cases[4]:

- The personal data the company/organization holds is needed to exercise the right of freedom of expression
- There is a legal obligation to keep that data
- For reasons of public interest (for example public health, scientific, statistical, or historical research purposes)

If data is processed unlawfully it must be deleted, according to GDPR. This also extends to data collected from minors.

Although GDPR is a big and important part of modern information security and data protection, it is also one of the most common regulations that companies

violate. This can lead to huge economical sanctions and loss of reputation, which is why it is important to get a general understanding of GDPR.

2.2 Information Security Management System

An Information security management system (ISMS) is a framework of policies and procedures for managing system data systematically [5]. It is the framework an organization uses to handle its security and risk management. ISO27001 is a framework within ISMS.

Why an organization would want to base its information security on specific frameworks is twofold. One reason is that it will be easier for all employees to know their role if an attack or leak happens. The ability to safeguard and secure information assets is critical. A ISMS is therefore a way for organizations to set up a solid security framework that regulates how the organization systematically can secure their resources [6].

2.3 The International Organization for Standardization

The International Organization for Standardization or ISO is an organization that has created international standards within different fields. It is a worldwide association of national standardization bodies with 165 member countries, which involves technical experts and committees that develop these standards. [7]. In this thesis, we will focus on their information security standards (ISO27001) and best practices.

2.4 ISO27001 Certification

ISO27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization [8]. It is designed to be universal across organizations and different sectors. ISO 27000, 27001, and 27002 are international standards that are receiving growing recognition and adoption. They are referred to as the “common language of organizations around the world” for information security. With ISO27001 companies can have their ISMS certified by a third-party organization and then show their customers evidence of their security measures [9].

To become ISO certified an external auditor needs to verify the internal policies regarding information security. An additional point is for external partners, governments, and potential customers to know that the organization takes information security seriously and that the information the users/customers give to the organization will be protected in a secure manner.

2.5 Relevance in modern times

The assignment we have chosen is a relevant topic for companies and society in general, now more than ever. There are several reasons for this. The main reason is that governments and local legislations are taking GDPR and other frameworks within information security more seriously than they did years ago. Most governments and organizations are becoming more aware of the serious threat poor information security can have on societies, and why it is important. This is one of the reasons why the sanctions for having poor information security standards have become higher and could lead to great losses for companies. Both economically and for their reputation.

One example of this is the dating app Grindr. In 2020 the Norwegian Consumer Council filed a complaint against them, and at the end of 2021, the Norwegian Data Protection Authority decided to impose a fine of 6.5 million euros [10]. Grindr was found guilty of handling and selling the personal data of its users without their consent. Some of this data includes GPS location, IP address, gender, age, and device information [10]. Even Google had problems related to GDPR, and at the beginning of 2019, they got a fine of 50 million euros. This fine was imposed by the French data protection authority called CNIL [11]. CNIL argued that Google did not obtain the necessary user consent to gather personal info and use this for ad-related purposes. This illustrates that even big and well-established companies can have trouble following and complying with both international and local regulations.

There have also been several incidents related to a lack of sufficient compliance in local Norwegian companies. Even small ones can be targets for coordinated cyberattacks, so it is important that also they have well-implemented standards both regarding privacy and cybersecurity.

SATS, which specializes in fitness centers is another example of a company that got fined by the Norwegian Data Protection Authority. They were fined 10 million NOK, and it was mostly related to mismanagement of personal data and violation of GDPR compliance [12]. Governmental institutions can also be affected. Some examples are the Norwegian parliament hack in 2020 or Toten municipality at the beginning of 2021. The Norwegian parliament was fined 2 million NOK because of their lack of basic security mechanisms 2FA [13]. Toten municipality was affected by ransomware, which is malware that usually encrypts or threatens to publish personal/sensitive data unless a ransom is paid. The total loss because of the attack was estimated to be around 35 million NOK [14]. Toten also got a fine of 4 million from the Norwegian Data Protection Authority for lack of IT- security.

This is the biggest fine that was ever given to a Norwegian municipality.

These are all examples of why it is important to have secure IT standards. While it is impossible to be 100 % secure against cyberattacks or mistakes/leaks, it is possible to greatly reduce the risk and the damage. ISO27001 is designed to help companies greatly reduce this risk, and also to limit the damage if an attack or leak already has happened. It is also considered to be a standard that is generally respected and among the best possible security practices within the industry.

2.6 Related work

We have not been able to find a lot of related work to our thesis, but some students from NTNU have finished a thesis that is somewhat similar to our assignment. The thesis is called "RSCCI: A User-Friendly Web Application for Evaluating Company Security Regulations and Cloud Security".

The main focus of this thesis was security in the cloud, but it is also relevant for our thesis, especially because cloud security is a big part of general information security and how companies store data. These students also created a website that enables companies to test their compliance with ISO27001 standards, but it only uses internationally known standards and not local Norwegian regulations like our model. Their model is also more technical than our model because it measures the company's cloud security through live dynamic analysis. This is not something our model does, because it would be very hard and take a lot of time to implement for every annex in the ISO27001 standard. It would however be something that possibly could be implemented in the future to test some parts of the ISO or regulation compliance.

Chapter 3

Requirements

This section addresses the functional and non-functional requirements for the proposed solution, taking into consideration the set of requirements provided by Sopra Steira. In light of the flexibility granted by Sopra Steira in the attainment of the project objective, additional requirements to ensure optimal functionality has been added.

3.1 Functional Requirements

To determine the functional requirements of our proposed solution, we used the task description and in-depth consultations with Sopra Steira to develop the functionality.

1. The model should check what sector and services the organization operates in.
2. The model should display what laws and regulations an organization is required to follow.
3. The model should check compliance with current regulations.
4. The model should check the organization's general information security standards.
5. The model should test the organization's human resource policy, and access to data that is granted to employees and contractors.
6. The model should be able to display to what degree a company complies with the ISO27001 standard.
7. The model should be able to export the results as data.

3.2 Non-Functional Requirements

Nonfunctional requirements are requirements that must not be included but are logical to include in order to improve the overall usability and accessibility of the model. Typically non-functional requirements are related to usability, flexibility,

performance, interoperability, and security [15]. The non-functional requirements for the application are as follows:

1. Usability: The goal of the creation of the model is to make it easy to use.
2. Compatibility: The GUI must be compatible with major operating systems and internet browsers.
3. Performance: The GUI should load each page relatively quickly without much delay.
4. Security: The website should follow modern security methods so 3rd parties will not gain unauthorized access.
5. Reliability: The service should be able to run effectively with minimum amounts of downtime.

3.3 Use Cases

This section will go into depth about what actors will make use of our application.

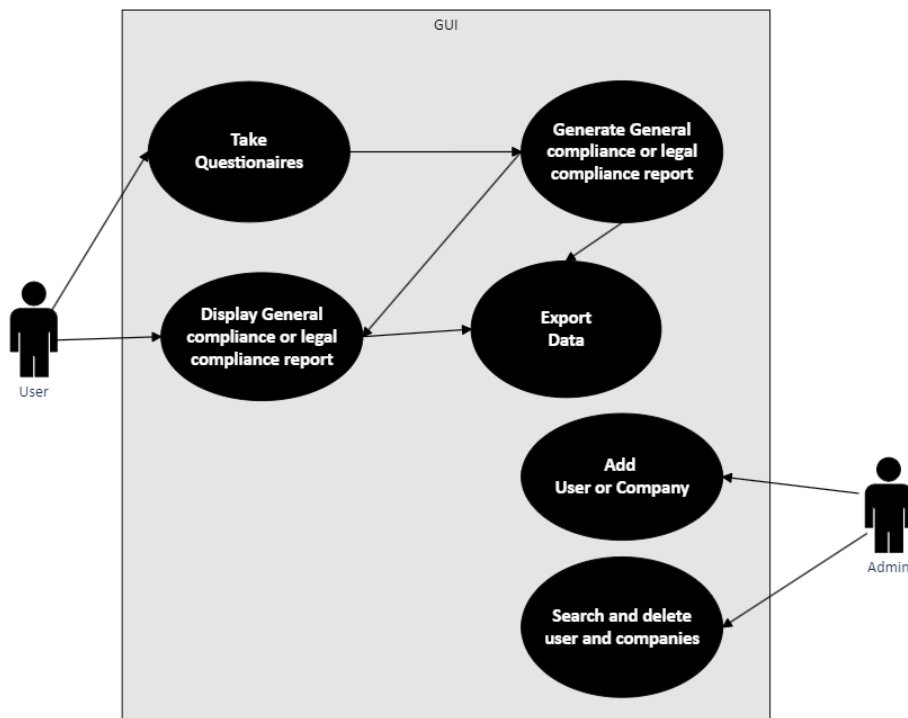


Figure 3.1: Use case

3.4 Detailed use cases

In the tables below we will describe in detail the use cases found in Figure 3.1.

Table 3.1: Questionnaire legal regulations

<p>Use Case name: Questionnaire legal regulations</p> <p>Purpose: Gain information to give users advice on their ability to follow regulatory standards</p> <p>Actor: User</p> <p>Requirement:</p> <p>Description: The user starts the questionnaire to check compliance with current regulations</p>
--

Table 3.2: Questionnaire technical framework

<p>Use Case name: Questionnaire technical framework</p> <p>Purpose: Gain information to give users advice on their compliance</p> <p>Actor: User</p> <p>Requirement: Be logged in to an account with permission to take the questionnaire</p> <p>Description: The user answers a questionnaire to check compliance with a technical framework as well as best practices.</p>

Table 3.3: Display compliance

<p>Use Case name: Display compliance</p> <p>Purpose: To give users a visual presentation of their compliance</p> <p>Actor: User</p> <p>Requirement: Be logged in and have taken the questionnaire</p> <p>Description: The user can get a visual representation of their compliance, and where their compliance is insufficient.</p>
--

Table 3.4: Export data

<p>Use Case name: Export data</p> <p>Purpose: Give the company the ability to export their information so they can display it in what format they would like, and also have their results stored locally</p> <p>Actor: User</p> <p>Requirement: Be logged into an account with permission to take the questionnaire, and also to have completed the questionnaire</p> <p>Description: The user exports their data from questionnaires into a readable format (JSON), this data can be displayed on our web page, or through other programs of their choice</p>

Table 3.5: Add User

Use Case name: Add User

Purpose: To give users access to the service

Actor: Administrator

Requirement: To have an account with administrator privileges

Description: An administrator of the system adds a user so they can take the questionnaire and get the functionality of the website.

Table 3.6: See users

Use Case name: See users

Purpose: To see who has access to the service and who has used it

Actor: Administrator

Requirement: To be logged into an admin account

Description: An admin displays the users who have access to the service.

Chapter 4

Design

In this chapter, we will explain the model architecture and the different components and tools used in its development. These include the database, graphical user interface, charts, and data exports. A detailed explanation of each of these components will be provided, highlighting their respective functionalities and roles in the model's overall design.

4.1 System architecture

To facilitate the understanding of the model we have created a comprehensive high-level system architecture that explains the different stages involved in the user questionnaire process and then the report delivery. This architecture aims to enhance the understanding of the model and its various components.

High level design

The following architecture diagram illustrates the high-level design for evaluating an organization's compliance with ISO 27001 or the legal compliance in the sector that the organization belongs to.

We assume that the user already has logged into the system, they will be able to select a specific compliance test to evaluate the degree of compliance within their organization. when the user completes the questionnaire, a report will be generated and installed on the user's local machine. This report can be used later in the next steps.

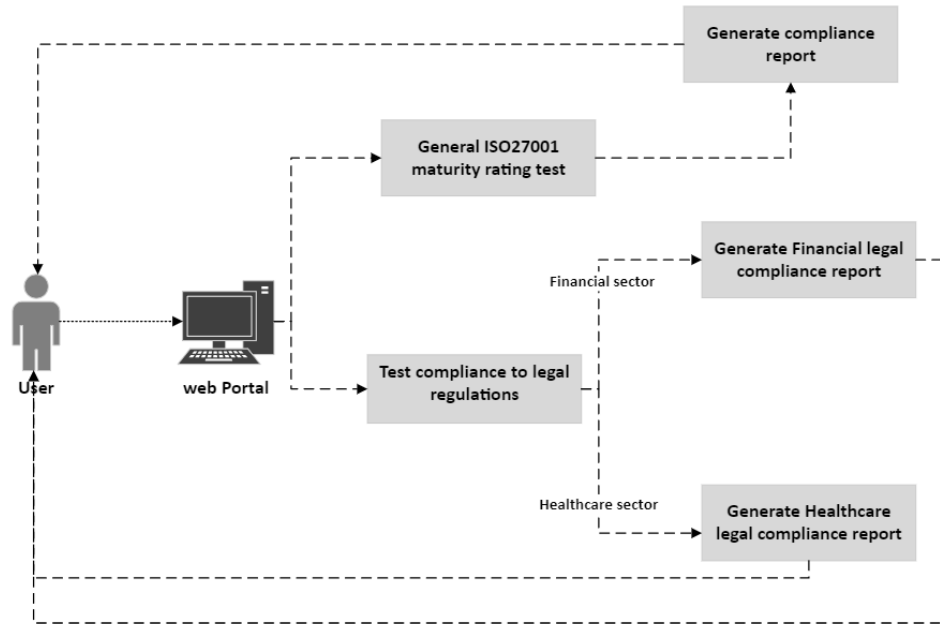


Figure 4.1: High-level design architecture

4.2 Flowchart of application

In this section, we will explain the flowchart of our application. This will show the sequential activities that the user will take during the interaction with our model. We have divided the flowchart into two different graphs to facilitate understanding of the model. The first graph will illustrate the activities involved in completing the questionnaires, while the second will illustrate the activities related to displaying the report's results. The next two sections aim to present a comprehensive visualization of the process users will follow when engaging with our application.

Flowchart of Questionnaire

The following graph illustrates the steps that the user will take for assessing the compliance degree of an organization to the security standard, to achieve an overall compliance evaluation the users have to first select a specific test within the model and they have to answer all questions to receive the compliance report. To determine the legal compliance degree, the user is required to first choose the sector that they want to assess. Then, they have to answer all the sector questions in order to receive the compliance report for that particular sector.

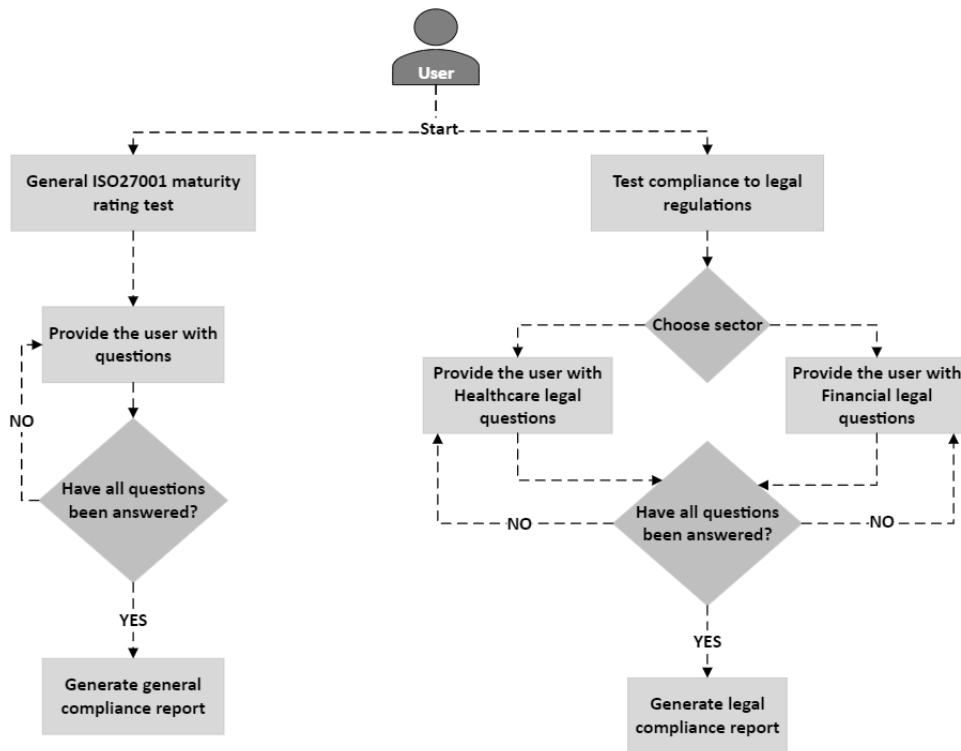


Figure 4.2: Flowchart of web interface Questionnaire side

Flowchart of displaying questionnaire results

The following graph illustrates the sequence of activities required for users to visualize report results in charts. Prior to generating charts, users must first complete a questionnaire to receive a report. Additionally, in order to compare general compliance, users need to possess two different reports, enabling them to make meaningful comparisons.

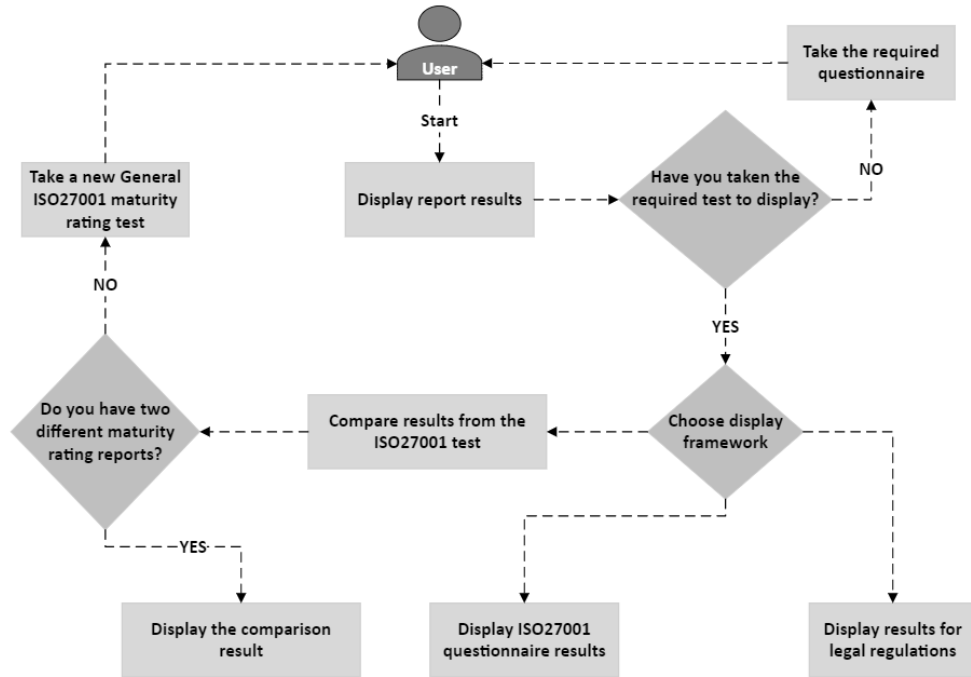


Figure 4.3: Flowchart of web interface Result display side

4.3 Sequence diagram

In this section, we will explain the sequence diagram of our model and we will demonstrate the interactions of different components within the system. The graphs will visually show how these components work together to accomplish and achieve a specific function.

To enhance comprehension and facilitate a comprehensive understanding of the model, we have divided the sequence diagram into three primary diagrams.

Maturity Rating and displaying Sequence diagram

The following sequence diagram presents the interaction between users and the various components within our model for assessing the organization’s compliance degree to security standards. As well as it shows the interaction required to analyze the data within the report file and present the report in the form of charts to the user with either a compliance degree or a comparison report.

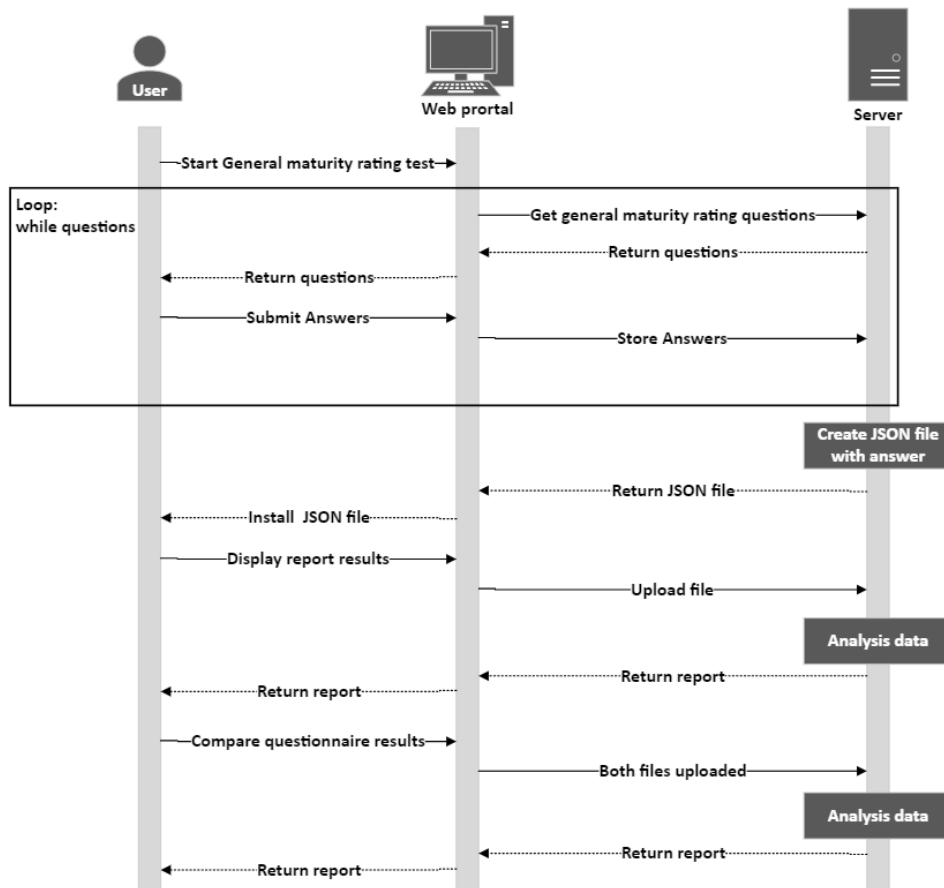


Figure 4.4: Maturity Rating Sequence diagram

Legal regulations and displaying Sequence diagram

The following sequence diagram illustrates the interaction between users and the different components within our model, specifically showing the process of assessing an organization's compliance degree with legal regulations based on the organization's sector and the services it provides, and then analyzing the report data and present it in the form of charts.

This diagram does not have a comparison step for this particular stage, the comparison function is only for the General maturity rating stage.

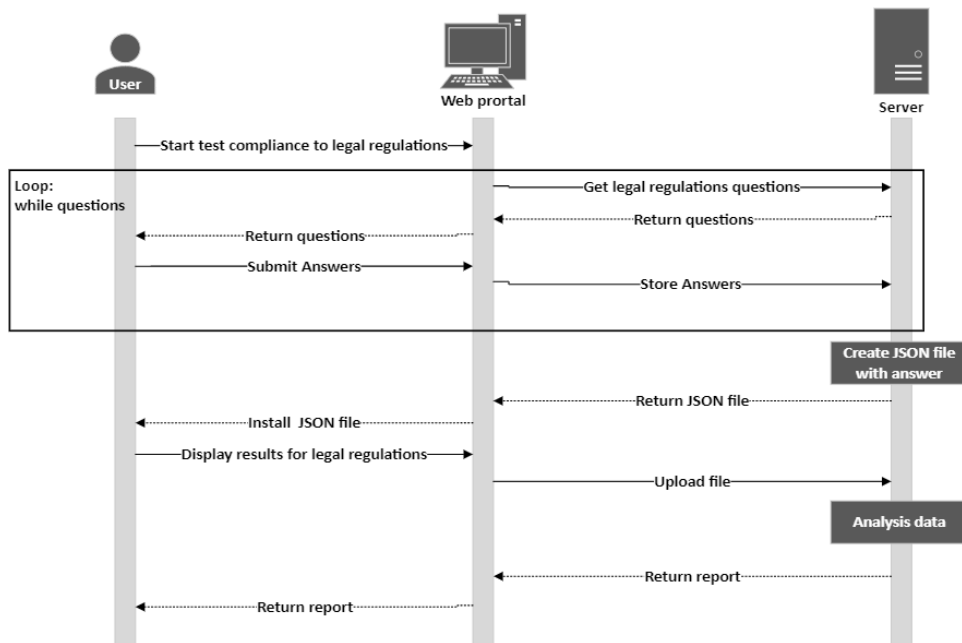


Figure 4.5: legal regulations Sequence diagram

Admin panel Sequence diagram

The presented sequence diagram illustrates the interaction between administrative users and various components within our model. It specifically shows the process involved in adding new users and companies to the system database, as well as conducting searches and deletions. These processes require administrative privileges to successfully execute them.

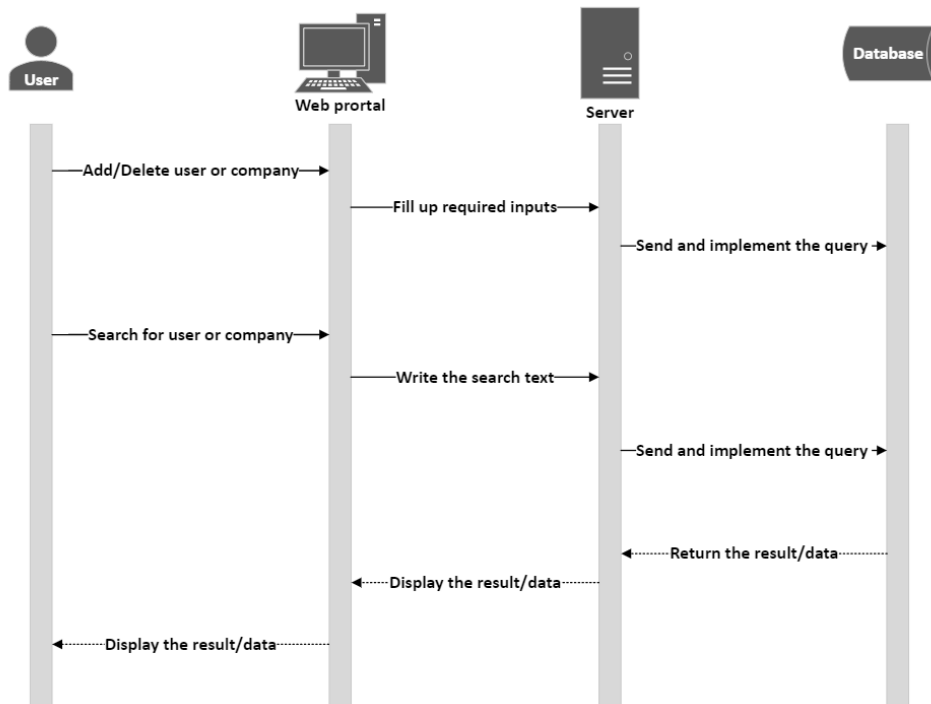


Figure 4.6: Admin panel Sequence diagram

4.4 Backend

The backend is a critical component of any project, and the selection of tools, programming languages, and implementation strategies must be carefully considered. It is imperative that the project team engage in thorough discussion and agreement on these matters as resetting and re-implementing the backend can result in significant delays in project delivery. Our project team has leveraged best practices gathered through our research and study to reduce development time and construct a resilient and dependable backend model.

LAMP stack

To run the website and all functionality a LAMP stack is utilized. The key points in a LAMP stack go by the letters. L stands for Linux the operating system, A for Apache the web server, M for MySQL the database server and P for PHP the programming language. All four of these technologies are open-source, which means they are community maintained and freely available for anyone to use [16]. The main reason to use a LAMP stack is to save time and efficiently create the model. Another reason is to give Sopra Steira the ability to easily utilize the model and make modifications to it. This is easier by using software that is open-source and commonly used. Below we will discuss choices for why different aspects of the stack were chosen and a bit of information about the different technologies.

Linux

The application is designed to run on any ordinary operating system, but for our project, we found Linux to be the most appropriate. For this project, we have decided to use the Ubuntu 20.04.6 LTS (Focal Fossa) version of Linux. The reasons behind the use of Linux/Ubuntu are as follows:

1. Open-source [17].
2. Free to use [17]
3. Widely used: Linux powers 37% of global websites, and of that percentage, 35.9% is Ubuntu [17]. Supported in the developer community for this reason.
4. As Ubuntu server has no GUI only a command line interface it's also resource effective.
5. Previous experience- the use of Linux and Ubuntu has been done previously during education at the university.

As such the configuration for the server setup planned means we plan to run the server as headless. Headless since the server will have no external peripherals and would be controlled over the cloud [18].

Apache

Apache is an open-source HTTP server for UNIX and Windows [19]. It is flexible, easy to set up, and has a big user base [20]. It is widely supported by end users and has a well-documented hosting section. This enables any issue that appears to be easily researched and eliminated. It is also free to use.

MySQL

To manage the log-in data to the model we use the open-source database management tool MySQL [21]. MySQL, which is the most popular Open-Source SQL database management system, is developed, distributed, and supported by Oracle Corporation [22]. The benefits of using it are that it is both powerful and versatile and at the same time free to use. In addition to the other benefits, it is also widely used by a magnitude of organizations within separate fields. An example of a massive organization using MySQL is Meta, which is the company behind Facebook [23].

PHP

PHP is a general-purpose and server-side scripting language that plays an important role in the development of web application components [24]. PHP has gained a lot of popularity among developers due to it being an open-source programming language, user-friendly, easily incorporated with other programming languages, and having a lot of highly useful functions, including database connectivity. PHP also offers a range of frameworks that can be instrumental in streamlining project development processes [25].

Load balancer - Haproxy

As a load balancer for the project, Haproxy was used because of its versatility and robustness. Haproxy is a popular load balancer designed for high-traffic websites and is the de-facto standard open-source load balancer [26].

The load balancing algorithm that is used is Round Robin. Round Robin is a common way of balancing the incoming network traffic among multiple servers. The traffic is routed through every available server with the goal of distributing the workload evenly across all servers. Round Robin is different from other load balancing methods in that it assumes that all the servers have the same hardware to handle the load, this is why it is the most efficient to use servers that have as similar hardware as possible when using Round Robin [27].

To maintain a consistent connection with the database, sticky sessions also called session persistence will be designed from the get-go [28]. Sticky sessions are used to maintain information about what server the original request came from and maintain it. The method used to store the session in this application is by using cookies in the browser to remember what server the client established contact with.

4.5 Frontend

The frontend is the visual representation the user has when interacting and navigating the model. We designed the frontend with simplicity in mind. The model does however have a lot of text, and it can be a challenge to display this text in a clean and sophisticated manner. These are the tools that helped us design the user interface of the model.

Bootstrap

To design the GUI we used the open-source and ready-made library of Bootstrap. Bootstrap is one of the most popular front-end frameworks and open-source projects in the world [29]. Bootstrap has several pre-built design elements and allowed us to easily start the development of the web page. The Bootstrap framework is built on HTML, CSS, and JavaScript [30]. However, it extends the functionality of these by also adding other variables and functions.

The use of Bootstrap allows developers to be able to develop easier and not waste a lot of time on unknown commands or functions. This is because they do not have to write elements from scratch. Bootstrap is used by a total of 21.2 percent of every website in the world [31]. In other words, it is a very popular tool. Another reason for this is that it is very easily adapted to the display on different devices and applications. Mobile devices are becoming more and more popular, so every serious web page should be aesthetic to view regardless of what type of screen it is displayed on. Bootstrap makes this simple.

HTML

(HTML) is a widely adapted language used for writing and designing web pages. HTML is however not a programming language, but a markup language [32]. This means that it is a system for identifying and describing the various components of a document such as headings, paragraphs, and lists [32]. There are two main versions of HTML that are used today. These are HTML 4.0 and 5.0. In our model, we used HTML5 because it is the latest version and it has several advantages. Some of these advantages include better performance, more cross-platform compatibility, and improved accessibility [33].

Because HTML is not a programming language, it is not required to have any set programming skills in order to utilize it. HTML is known for being beginner-friendly and easy to use. Because it is the go-to standard for creating web pages [34], it is also easy to find additional information and resources if needed. We realized that with the combined use of Bootstrap, JavaScript, CSS, and other web development technologies we would be able to create a well-designed and functional model. HTML also has the advantage that it is easily viewed on different devices, which enables users of the model to also be able to complete the test

through mobile devices. This adds more convenience.

The main function of HTML in our model is to structure and design the content. It is a bonus that the user-friendliness of HTML allows us or users of the model to easily redesign it.

CSS

(CSS) is a style sheet language that is used to describe how the content of a web page should look. Visual effects like fonts, colors, background images, spacing, layout, and so on are controlled using CSS [32]. Our goal is to make the model user-friendly, and proper use of CSS will help to achieve that. We have designed and used CSS so text is easy to read, and the layout is clean and easy to use. It is also possible to design and publish websites using only HTML [32], but the use of CSS adds more professionalism and flexibility.

JavaScript

JavaScript is the standard scripting language for modifying and adding behaviors to web pages [32]. It is popular because of the versatility it enables, along with a great set of plugins and tools which is compatible with JavaScript. It is also relatively easy to use, especially for those that already know certain programming languages. It can be used for a variety of functions, and some of the most common examples are form validation, interactivity, client-side data storage, or server-side programming. Form validation was the main use of JavaScript in the model.

Chart.js

Simple yet flexible JavaScript charting library for the modern web [35]. It is open-source and supports up to 8 different graph types. It is used in our model to display the compliance organizations have towards regulation or the general ISO27001 certification.

4.6 Exported Data

We wanted the data that gets downloaded after the user has completed the tests to be intractable with other software. This is in order to add more options and flexibility for the user. A lot of companies use different programs in order to read and display data. The goal is that they will be able to download a JSON file that can be read in a program of their choice, but it will also be a function to read it on the website.

JSON

JSON is a "lightweight data-interchange format. It is easy for humans to read and write. It is also easy for machines to parse and generate" [36]. JSON is commonly used to exchange data between platforms. It is based on a subset of JavaScript, but it is not required to know JavaScript to be able to use it [37].

Chapter 5

Development

5.1 Development model

Through our thesis, we used an incremental development model. All of the students are familiar with or have previously worked with different sorts of development models, for example, Kanban or Scrum. These two are very popular, but we did not find them to be optimal for both writing the thesis and completing our model. Kanban is popular because it is a very lean and agile development model, which is also simple and flexible. This again can help to resolve bottlenecks and improve the workflow [38]. We did however find Kanban to be a little too unstructured for our preferred way of developing. Scrum is another agile model, which is more focused on iterative and incremental development than Kanban. We acknowledge that Scrum most likely would also be an efficient development model for our thesis, however, we did not have much experience in working with this model, so using it was too unpredictable.

We would also prefer to have an even more flexible approach than what Scrum enables. It is hard to estimate exactly how long the implementation of different parts of the model will take. If something is more challenging than the other parts, it will be beneficial to complete this part before starting the next. Because of the fixed Spring lengths that are commonly used in the scrum model, it is likely to be somewhat less flexible to changes or eventual delays. If we knew exactly what had to be done from the beginning, and had more experience in creating something like this, the scrum model would be likely to be used instead.

Because we believe we would have to continuously work on and improve our three-way model, a standard incremental development model makes sense. This way we can regularly check and modify our model according to feedback from Sopra Steria or our supervisor. There is also a lot that has to be done when we are creating the model, and by breaking the project into smaller parts, we can make it more manageable and approachable. Some disadvantages of an incremental development model are that it can be less predictable compared to other models. This is one of the disadvantages of choosing an agile model. It will also require

a lot of regular communication and updates between the team members, but we are confident the team will handle this.

5.2 Documentation

Report writing

The report writing of the project was done through \LaTeX . Working on the assignment with \LaTeX has several advantages. It enables everyone in the group to work together in real-time on the document and makes cooperation easier. The Template used was provided by NTNU[39], which is the default template for writing a thesis.

Source code

The source code of the project was stored through Github so we could collaborate on the development of the GUI. Github has over 100 million developers from across the world [40]. Usage of the service is therefore widespread across the globe and has all the functionalities a Git repository should have.

Link to our Github repository:

<https://github.com/Bachelor2023Gr120/ProgramKode>

Meeting notes

Notes were taken during or after each meeting with the supervisor or Sopra Steria. This enabled us to remember answers to any questions or tips for improvements.

5.3 Workflow

Communication

We mainly used the free-to-use VoIP and instant messaging platform Discord to communicate internally within the group. For communication with the supervisor either from the university or Sopra Steira we either used Teams for calls or email for written communication. Every group member was expected to meet at every agreed-upon meeting unless they had notified the group of their absence.

Development

The version control system as well as the collaborative tool Git were used to track progress on the development of the application. Git is a free and open-source distributed version control system designed to handle everything from small to very large projects with speed and efficiency [41]. It is lightweight, easy to understand, and efficient.

Chapter 6

Implementation

In this chapter, we will provide a detailed description of the implementation of our model components, including the interface, database, questionnaires, and charts. We will explain the programming languages utilized in the various components and present a sample of the code. This chapter will provide an in-depth understanding of our model's technical aspects, offering a comprehensive overview of its different components and functionalities.

6.1 Infrastructure

This section covers the development and delivery environment used during the creation of our application. What choices were made and configuration of said environments.

6.1.1 Development environment

During the development period of the project the way it was done was with utilizing local hosting with the development programs git, phpMyAdmin and XAMPP. Git as a collaborative tool, phpMyAdmin to manage local MySQL databases and XAMPP to virtualize the LAMP stack used during production. XAMPP supports all the modules in the LAMP stack on a local computer.

6.1.2 Production environment

A easy, reliable and cost effective solution for production environment was using NTNU's virtualization-platform. It came with no extra expenses for either Sopra Steira or the group, and it gave the group plenty of resources to manage and host the application for user testing. The university's virtualization-platform runs OpenStack, which the team members previously have worked with. This way we avoided using time to learn another platform for hosting applications.

Server Setup

Figure 6.1 illustrates the server architecture, and it consists of the following components:

- **Load Balancer:** A load Balancer runningnng Haproxy. All webservers run the same configuration and have the same capacity so running the Round-Robin algorithm.
- **Webservers:** Webservers running Apache server
- **Database:** A database server running MySQL server. Connected to the other webservers so data is synchronised between them.

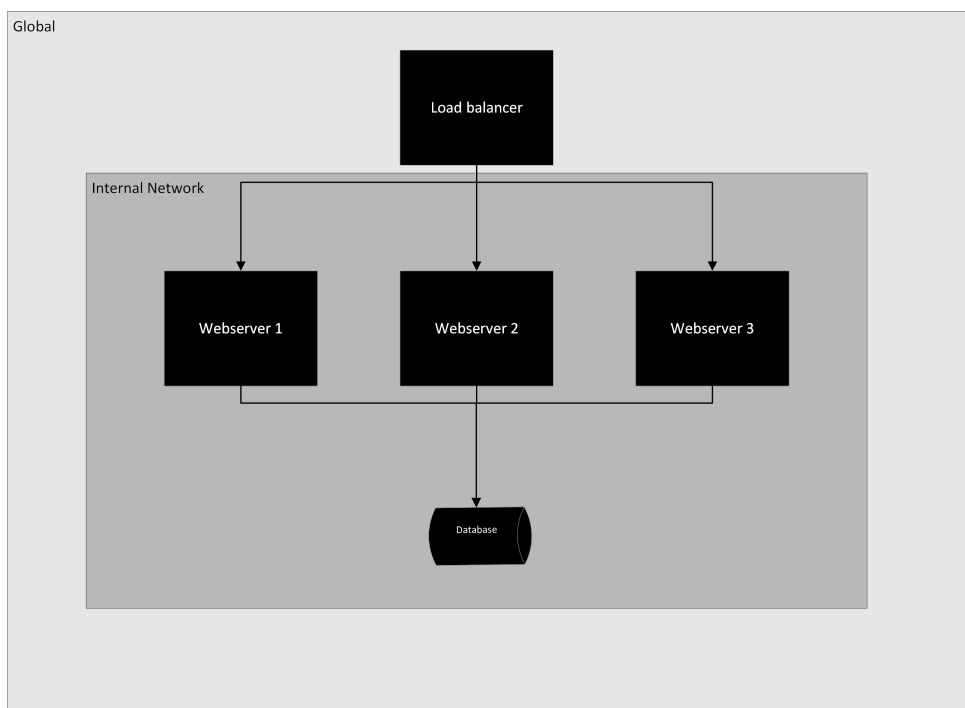


Figure 6.1: Server Architecture

Security

Below are a few different aspects to how the security of our production environment are set up.

- **Network**

To gain access to our website configuration you need to either be physically present at a certain location or virtually with a use of a VPN. This secures the application with the requirement that you are present at the university or have access to a VPN so you can virtually be present.

- **Port restriction**

Outside access to the application gets limited to only the port running the application. Port 80 in this case as we did not have access to a SSL certificate and for a potential future full release it would be opened up to traffic from port 443 [42].

- **Secure Shell**

Use of Secure Shell or SSH is required to gain access to system resources and to be able to change configuration. The Secure Shell (SSH) Protocol is a protocol for secure remote login and other secure network services over an insecure network[43]. It works by exchanging keys and to gain access you require a verifiable key. Without one the connection between computers will be denied.

All of these tools combined creates a safe production environment where users that have not been cleared for access should be incapable of modifying the configuration while also gaining access to the website.

6.2 Frontend

This section covers the front-end of the model, encompassing the interface, and a comprehensive clarification of their implementation, as well as the tools used in each of them.

6.2.1 Homepage

The homepage of our model has been designed using PHP, HTML and CSS to provide a simple and user-friendly interface (see Figure 6.3). It also features a navigation bar at the top which has been implemented and designed using the open-source Bootstrap component and CSS, which enables users to interact with the various pages on the website.

The first section of the homepage provides an inclusive overview of information security, explaining the importance of safeguarding sensitive data in any organization. The subsequent paragraph delves into the various sectors that our model covers. Each sector is presented as clickable, which allows users to navigate to the specific sector that his/her organization belongs to.

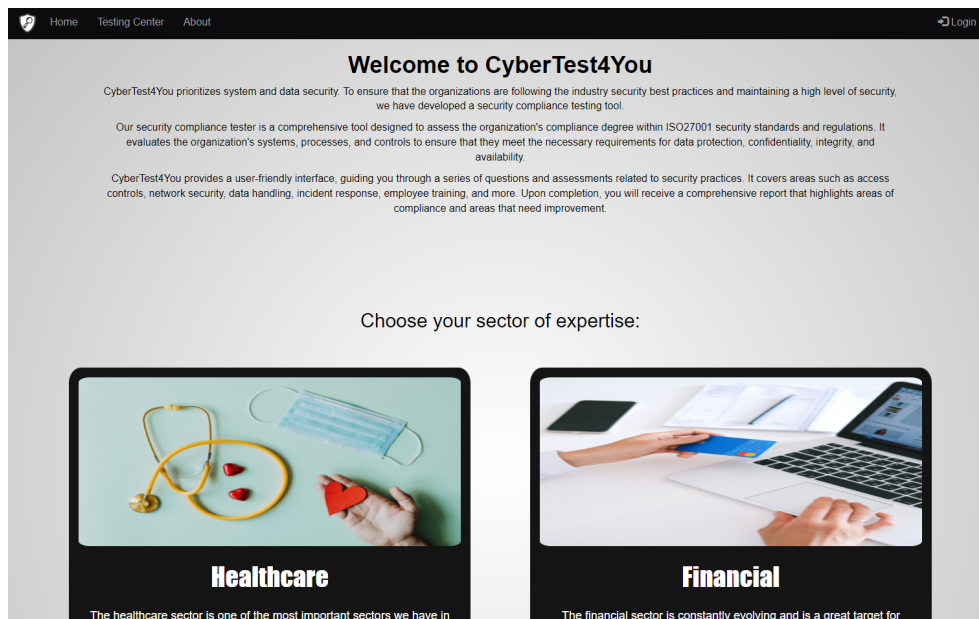


Figure 6.2: Homepage

6.2.2 Sectors

The model will cover only two sectors of expertise, namely healthcare, and finance. Through this interface, users will be able to obtain relevant information re-

garding the laws and regulations that govern their organization's services within these domains. The module serves to provide a comprehensive and efficient means of assessing compliance requirements, with a particular emphasis on the health-care and finance sectors. The sector interface was designed and implemented using PHP, HTML and CSS technologies.

6.2.3 About

This interface (see Figure 6.3) serves to provide overall information about the website and the team responsible for the development of the model, as well as the project owner Sopra Steira[1]. The purpose is to facilitate the user's understanding of the platform.

To the left of the interface, users can find contact information for the development team. This feature enables users to easily get in touch with us if they have any questions or concerns. The interface was designed and implemented using PHP, HTML and CSS technologies here as well.

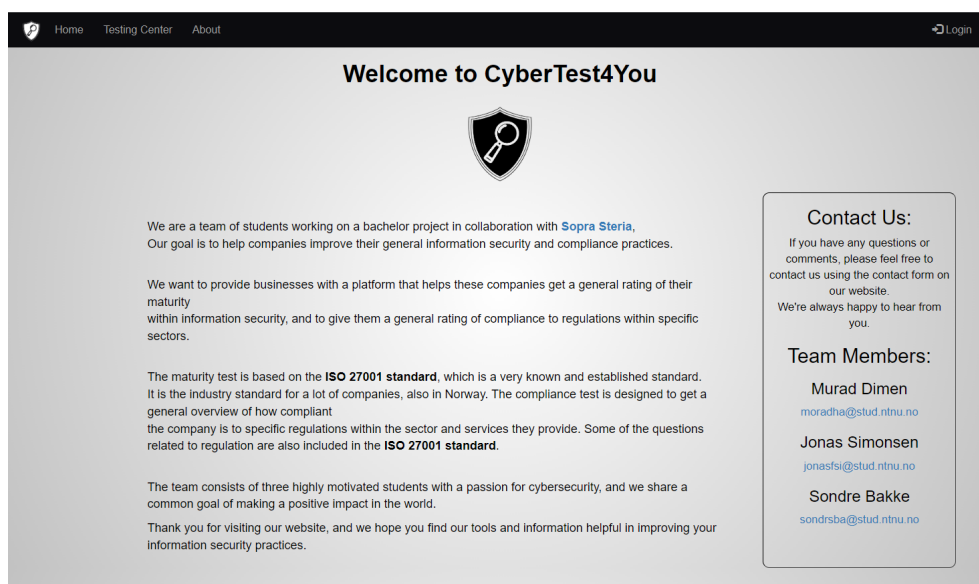


Figure 6.3: About interface

6.2.4 Login interface

The login interface (see Figure 6.4) is a simple design featuring a login form and a text description adjacent to it. The text is to inform users that they should approach the administrator of their organization or the development team to request an account in order to engage with the model. The interface has been developed using HTML, JavaScript, and CSS in addition to the Bootstrap framework to provide a consistent look to the website.

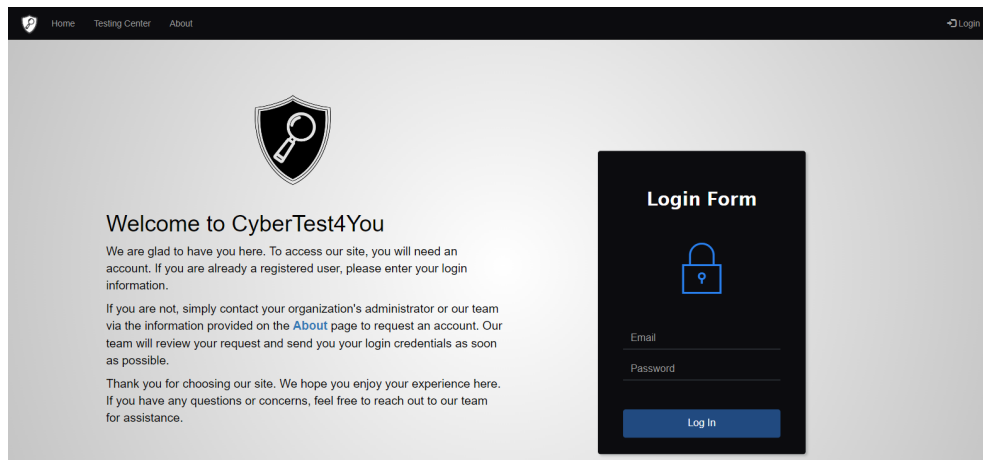


Figure 6.4: Login interface

Furthermore, a validation function has been implemented to identify errors or missing inputs that may occur during the login process and alert users with informative error messages. This robust validation mechanism enhances the usability of the interface and improves the overall user experience.

```
1  function validation()  
2  {  
3      var id=document.f1.email.value;  
4      var ps=document.f1.password.value;  
5      if(id.length==" " && ps.length=="") {  
6          alert("email and Password fields are empty");  
7          return false;  
8      } else {  
9          if(id.length=="") {  
10             alert("email is empty");  
11             return false;  
12         }  
13         if (ps.length=="") {  
14             alert("Password field is empty");  
15             return false;  
16         }  
17     }  
18 }
```

Listing 1: Login validation function

6.2.5 Testing Center

The Testing Center interface (see Figure 6.5) comprises a diverse set of features integrated into the model, providing users with a seamless interaction experience. The interface was designed and implemented using PHP, HTML and CSS technologies. Among its key features, the interface allows users to initiate a "General ISO27001 Maturity Rating Test" which evaluates compliance with the ISO27001[8] standard. The interface also enables users to display the results of the questionnaire and compare them with previously completed assessments. Additionally, users can initiate a test to assess compliance with legal regulations in the health and finance sectors, with the results of these assessments also being displayable. An explanation of each function and its purpose is also provided to ensure users have a clear understanding of how to navigate and use them.

Access to the Testing Center interface requires a verified user account, and successful login authentication is also necessary to commence interactions with the components within the interface. Further elaboration on each of the functionalities and their specific features will be provided in subsequent chapters.

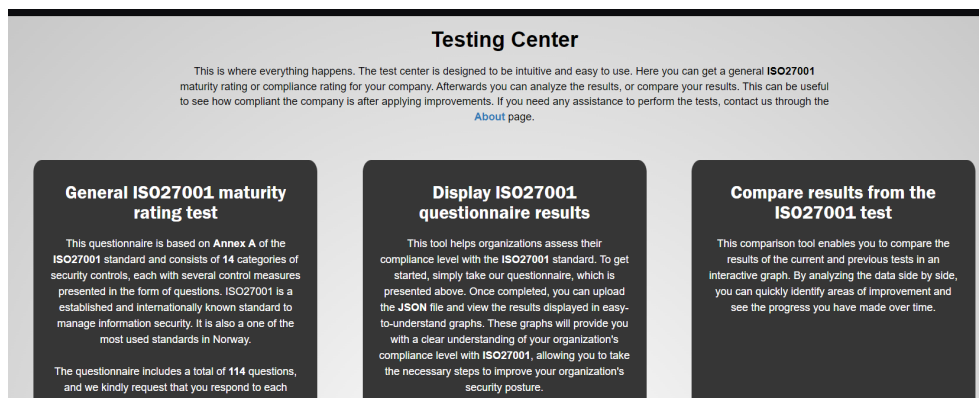
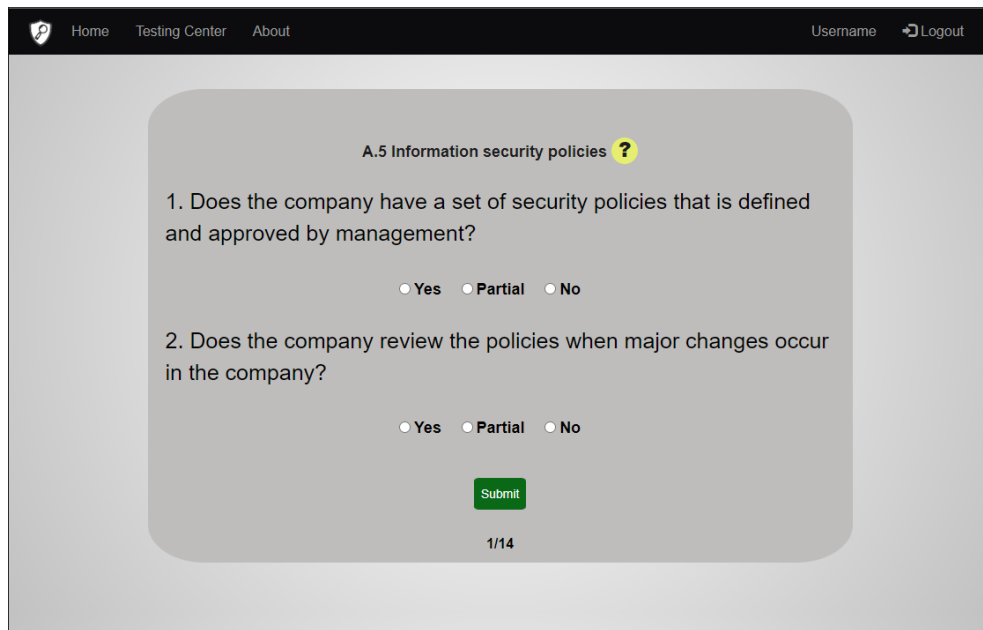


Figure 6.5: Testing Center website

6.2.6 General Maturity Rating Test

The questionnaire page (see Figure 6.6) presents a standardized assessment tool based on Annex A "security controls" of the ISO27001[8] standard. The questionnaire encompasses 14 categories of security controls, with each category comprising a series of control questions. Each category is accompanied by a concise title and description, providing users with a clear understanding of the security control's scope and purpose.



Home Testing Center About Username Logout

A.5 Information security policies ?

1. Does the company have a set of security policies that is defined and approved by management?

Yes Partial No

2. Does the company review the policies when major changes occur in the company?

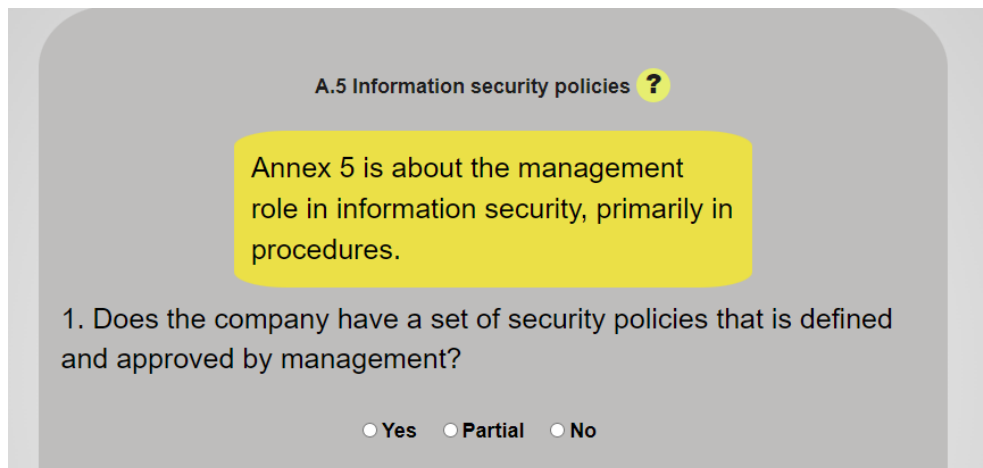
Yes Partial No

Submit

1/14

Figure 6.6: General Maturity Rating Test

To enhance user experience and streamline the questionnaire's content, some categories include sections descriptions, to avoid overwhelming users with excessive text, we opted to utilize hover-over buttons to display the descriptions, as depicted in Figure 6.7. This approach improves user comprehension and provides a user-friendly interface for completing the questionnaire.



A.5 Information security policies ?

Annex 5 is about the management role in information security, primarily in procedures.

1. Does the company have a set of security policies that is defined and approved by management?

Yes Partial No

Figure 6.7: Section Descriptions

The questionnaire operates by retrieving questions stored in a JSON-file using the fetch-API (see code listing 12). The JSON object is initialized, and an iterative process is utilized at the beginning of the Questions() function (see code listing 2) to generate specific elements for each object, depending on its intended function as a question, title or description. This is achieved by invoking the showQuestion() function for each sector and its questions.

```
1 function Questions(questions) {  
2     let userAnswers = {};  
3     for( i=0; i<questions.length; i++){  
4         showQuestion(questions[i]);  
5     }  
}
```

Listing 2: Looping through the questions

The Questions() function (see code listing 2) contains four various functions designed to facilitate the process of displaying the questions, and creating and downloading a JSON file that contains the user responses to the questionnaires.

Firstly, the showQuestion() function creates the necessary elements for each section of the questionnaire. Then, the createQuestionForm(index) function generates a form to display the questions and inputs.

Next, the submitAnswers(e) function detects button click events and verifies if the user has answered all the questions. Afterwards it saves the responses and forwards them to the next function.

Finally, the createJSONFile(answers, Username) function takes the responses and username as parameters and generates a JSON file with the section titles and user responses as content. The file is named by using the user's name and the date the questionnaire was taken, and is automatically downloaded upon completion of the test.

6.2.7 Display questionnaire results

The result page displays the results of the taken questionnaire in graphs to show the degree of compliance the organization has within their compliance towards certification ISO27001[8].

The displayed results interface affords the user the capability of uploading a JSON file (code listing 14), which is downloaded after the user completes the questionnaire. The interface will then present the data of the file in two graphical representations, namely bar charts and doughnut charts. The bar chart illustrates the compliance percentages for each section, while the doughnut chart provides an overview of the total compliance percentages. Each chart utilizes calculation methods to ensure precise and accurate rates. The following paragraphs will elaborate on the calculation methods employed by each chart to extract the compliance percentages.

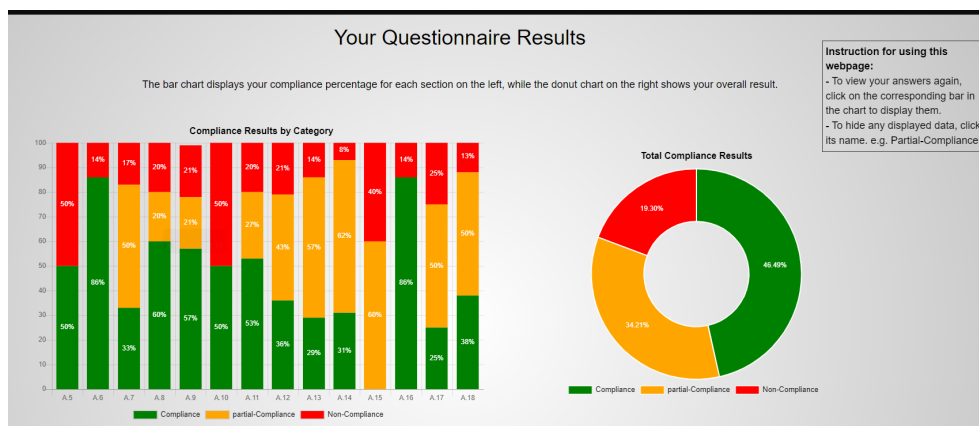


Figure 6.8: Questionnaire Results

After the completion of a successful file-uploading process, the data within the file will be retrieved using the `ReadFileData()` function (see code listing 3). This function is responsible for reading the file contents and parsing it as JSON data. Then, the parsed data is passed as a parameter to the `ResultDisplayChart(data)` function (see code listing 4), which is designed to calculate the percentage and display them later in the form of charts.

```
1 function ReadFileData() {
2     let file = document.getElementById("file").files[0];
3     let fileReader = new FileReader();
4     fileReader.onload = function() {
5         let data = JSON.parse(fileReader.result);
6         ResultDisplayChart(data);
7     }
8     fileReader.readAsText(file);
9 }
```

Listing 3: Read files data code sample

The `ResultDisplayChart(data)` function (see code listing 4) utilizes a collection of variables and arrays to perform calculations and store data. It employs a for loop to iterate through the data, determining the number of answers in each section and assigning it to the variable "numAnswers".

The calculation of percentages for the bar chart involves checking the type of each answer based on its value, it increments the corresponding count variable for each answer type. After the completion of each section, the function calculates the percentage of each answer type by dividing the total count of that type by the total number of answers in the section. The resulting percentage is then multiplied by 100 and pushed to the array for storage. This sequential process is repeated for each section and answer type.

To illustrate, suppose we have 10 questions, of which three responses are valued at 1, and three at 0.5, while the remaining are valued at 0. The compliance percentage would be computed as follows: $\text{compliancePercent} = 3/10 = 0.3$, and the Partial-Compliance percentage = $3/10 = 0.3$, while the Non-Compliance percentage = $4/10 = 0.4$. After applying a multiplication factor of 100, the analysis reveals a compliance rate of 30%, a Partial-Compliance rate of 30%, and a Non-Compliance rate of 40%.

The calculation of percentages for the doughnut chart involves a similar procedure to the calculation of the percentages for the bar chart but with additional considerations. It calculates the total count of each answer type in all sections and stores it in each corresponding variable, as well as the total count of answers, and stores it as "TotalAnswersNum". The process then divides the total count of each answer type by the total number of answers and multiplies the result by 100. These calculated percentages are then stored in an array, which is subsequently utilized to display the data in the doughnut chart.

The stored data in the two arrays are then transmitted to the charts for graphical representation, thereby enhancing the legibility and facilitating the readability of the data.

```
1  for (var sectionNum in data) {
2      var sectionData = data[sectionNum];
3      var numAnswers = Object.keys(sectionData).length;
4      TotalAnswersNum += Object.keys(sectionData).length;
5
6      var numCompliant= 0;
7      var partialCompliant = 0;
8      var noncompliance= 0;
9
10     for (var answer in sectionData) {
11         if (sectionData[answer] == "1") {
12             numCompliant++;
13         } else if(sectionData[answer] == "0.5"){
14             partialCompliant++;
15         } else
16             noncompliance++;
17     }
18
19     var compliancePercent = numCompliant / numAnswers;
20     var partialcompliancePercent = partialCompliant / numAnswers;
21     var noncompliancePercent = noncompliance / numAnswers;
22
23     complianceData.push(compliancePercent.toFixed(2)* 100);
24     partialcomplianceData.push(partialcompliancePercent.toFixed(2)* 100);
25     noncomplianceData.push(noncompliancePercent.toFixed(2)* 100);
26
27     totalCompliant += numCompliant;
28     totalpartialCompliant += partialCompliant;
29     totalNonCompliant += noncompliance;
30
31     totalCompliantPercent =
32         (totalCompliant / TotalAnswersNum) * 100;
33     totalPartialCompliantPercent =
34         (totalpartialCompliant / TotalAnswersNum) * 100;
35     totalNonCompliantPercent =
36         (totalNonCompliant / TotalAnswersNum) * 100;
37         // uses for the section labels in bar-chart
38     labels.push("A." + (i + 5));
39     i++;
40 }
41
```

Listing 4: Percentage Calculation code sample

In order to improve the user experience, we have implemented a feature that enables the retrieval of questions and previously provided answers in case users have forgotten them. Users can now simply click on the bar within the chart to view the section questions and their corresponding answers. This functionality allows users to identify areas of weakness and strength within their organization.

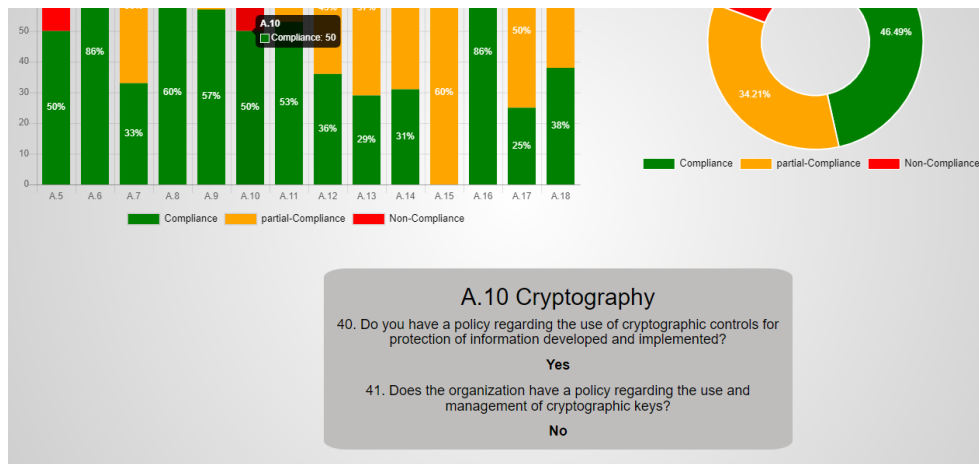


Figure 6.9: Display User Answers

6.2.8 Compare Results

The Compare Results interface has been developed to facilitate the monitoring of enhancements made in the security controls implemented within the organization. This interface provides a visual representation, in the form of a bar chart, that allows for a side-by-side comparison of two different questionnaire results. Its purpose is to provide an efficient means of tracking and evaluating progress made in enhancing security measures.

The interface affords the user the capability of uploading two different JSON files (see code listing 14). After a successful file uploading, the ReadFileData() function is executed, which is similar to the previous function (see code listing 3) but reads data from two different files. The extracted data is then passed as parameters to the CompareData(data1, data2, file1, file2) function (See code listing 5). The file1 and file2 parameters are used to label the bars in the chart and show the file name label under the chart, thereby identifying the corresponding file names.

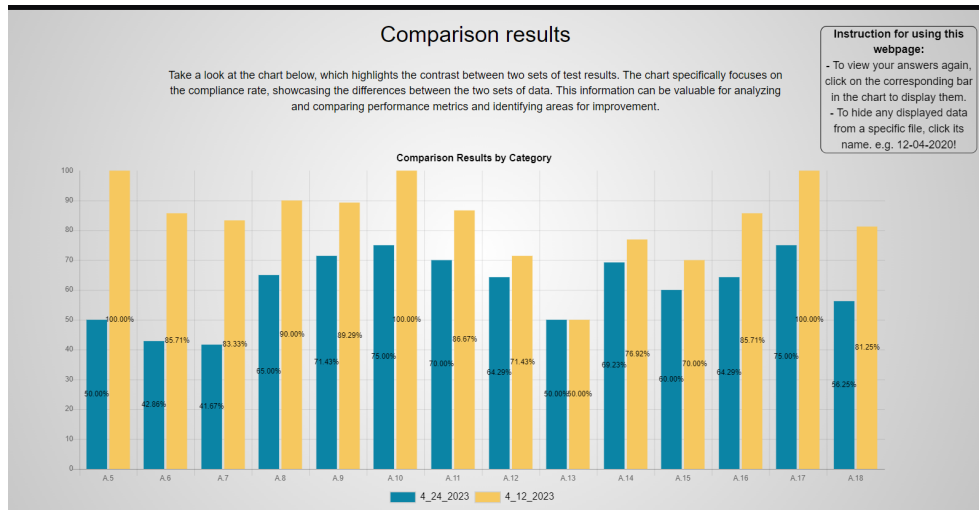


Figure 6.10: Compare results interface

The comparison function is created to evaluate the security enhancements. In this regard, the CompareData() function (see code listing 5) essentially focuses on compliance and partial compliance responses. It analyzes these responses for each section in each file and calculates the percentage of compliance achieved. Through this approach, it is possible to assess the security measures implemented in a comprehensive manner.

To find the compliance percentage, we divide the previously calculated compliance variable by the total number of responses in the corresponding section. We then multiply the result by 100 to extract the percentage. Then, we store the calculated value in an array for later use in visualizing the data in a chart.

The above-mentioned process is implemented iteratively on each section for each file. The calculated values are then stored in their corresponding arrays for each file. The provided code sample (see code listing 5) shows the process for the first uploaded file only. However, the second file takes a similar process and appends the calculated data to the "complianceData2" array.

```

1  for (let section in data) {
2      labels.push("A." + (i + 5)); // uses for the section labels in bar-chart
3      i++;
4
5      let sectionData = data[section];
6
7      let complianceCount = 0;
8      let partialcomplianceCount = 0;
9
10     for (let answer in sectionData) {
11         if (sectionData[answer] === "1") {
12             complianceCount++;
13         }if (sectionData[answer] === "0.5") {
14             partialcomplianceCount++;
15         }
16     }
17     let compliance = complianceCount + (partialcomplianceCount / 2);
18     let compliancePercent =
19         (compliance / Object.keys(sectionData).length) * 100;
20     complianceData.push(compliancePercent.toFixed(2));
21 }

```

Listing 5: Comparison data calculation code sample

Similar to the result display functionality, we have implemented a feature that enables the retrieval of questions and their associated answers for users who may have forgotten them or want to compare. But here it displays the data for each file separately. We have introduced colored boxes (see Figure 6.11) that correspond to the file bars in the chart. To display different section data, users are required to click on the corresponding bars, which triggers the display of the information (see Figure 6.11).

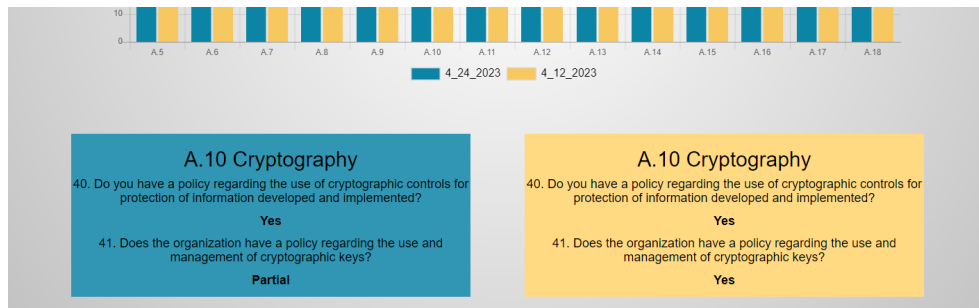


Figure 6.11: Compare User answers

6.2.9 Test compliance to legal regulations

To start the test for checking what information security laws an organization has to follow you get a startup screen after going from workspace. To choose a sector you get a drop-down menu with the added sectors the group has researched.

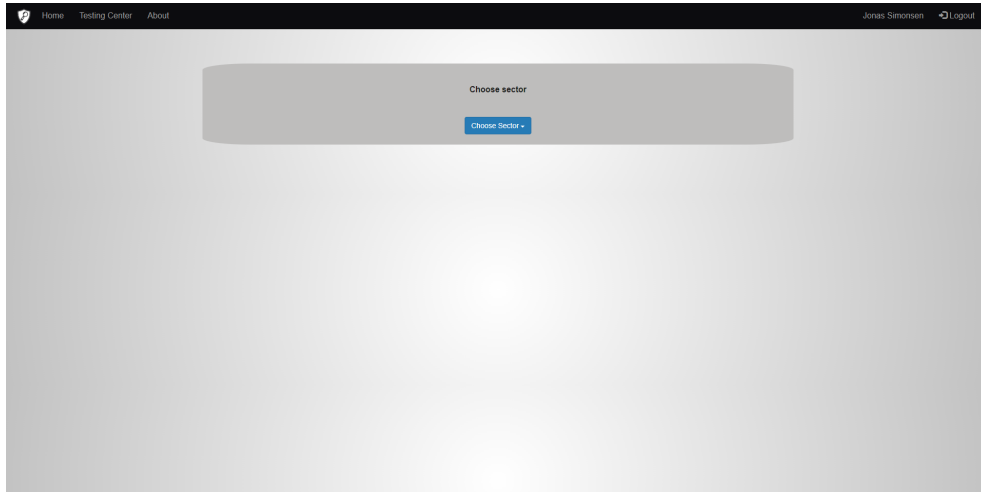


Figure 6.12: Choose sector starting page

The questions within both sectors gets brought out by a JSON file in the same format as done within the ISO27001 questionnaire. What file that it searches for depends on the sector of choice.

Healthcare

It consists of 186 questions regarding the information security regulations within the health care sector. The following figure shows the question format.

1

1. Are all security measures suitable and chosen on the basis of risk assessments?
Relevant laws: GDPR, Section 32 & PjL, Section 22 & HRL, Section 21
 Yes Partial No

2. Does the organisation assess whether it is necessary to implement more comprehensive measures than those described in the Code?
Relevant laws: GDPR, Section 32 & PjL, Section 22 & HRL, Section 21 & FLK, Section 8
 Yes Partial No

3. Do all employees in the organisation undergo continuous training regarding the requirement to fulfil the duty of confidentiality, information security and data protection?
Relevant laws: GDPR, Section 32 & PjL, Section 22 & HRL, Section 21 & FLK, Section 7
 Yes Partial No

4. Does the organisation obtain a confidentiality agreement for each employee?
Relevant laws: PjL, Section 15 and 23 & HRL, Section 22
 Yes Partial No

5. Has the organisation guidelines for the private use of information systems and equipment?
Relevant laws: PjL, Section 23 & HRL, Section 22 & FLK, Section 7
 Yes Partial No

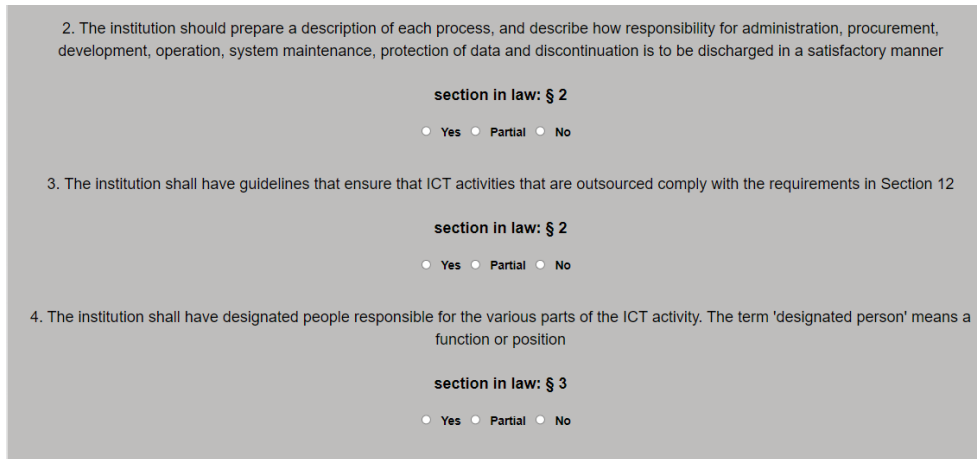
6. Has the organisation established measures which ensure that everyone who is given access to information systems and

Figure 6.13: healthcare questions format

The format is of 10 questions on each page up until you have completed the questions. After it gets finished it downloads a file in the format of healthcare-username-date and redirects you towards where you can see to what degree you comply with the regulations.

Finance

It consists of 19 questions regarding the information security regulations and laws surrounding the financial sector (see Figure 6.14)



2. The institution should prepare a description of each process, and describe how responsibility for administration, procurement, development, operation, system maintenance, protection of data and discontinuation is to be discharged in a satisfactory manner

section in law: § 2

Yes Partial No

3. The institution shall have guidelines that ensure that ICT activities that are outsourced comply with the requirements in Section 12

section in law: § 2

Yes Partial No

4. The institution shall have designated people responsible for the various parts of the ICT activity. The term 'designated person' means a function or position

section in law: § 3

Yes Partial No

Figure 6.14: Finance questions format

The format is of 10 questions on each page up until you have completed the questions. After it gets finished it downloads a file in the format of finance-username-date and redirects you towards where you can see to what degree you comply with the regulations.

6.2.10 Display results for legal regulations

Uses the same functions from the display results from the General Maturity Rating Test, Display questionnaire results. Takes the file created from the questionnaire for legal regulation and allows you to display the information in both a doughnut graph and a stacked bar chart. Below shows two alternative versions of how the website would present itself.

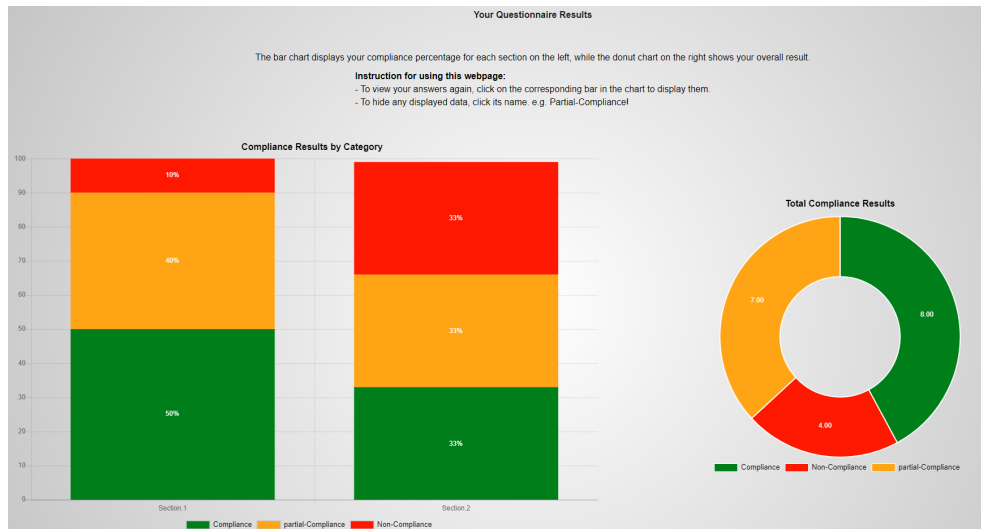


Figure 6.15: Display legal results finance example

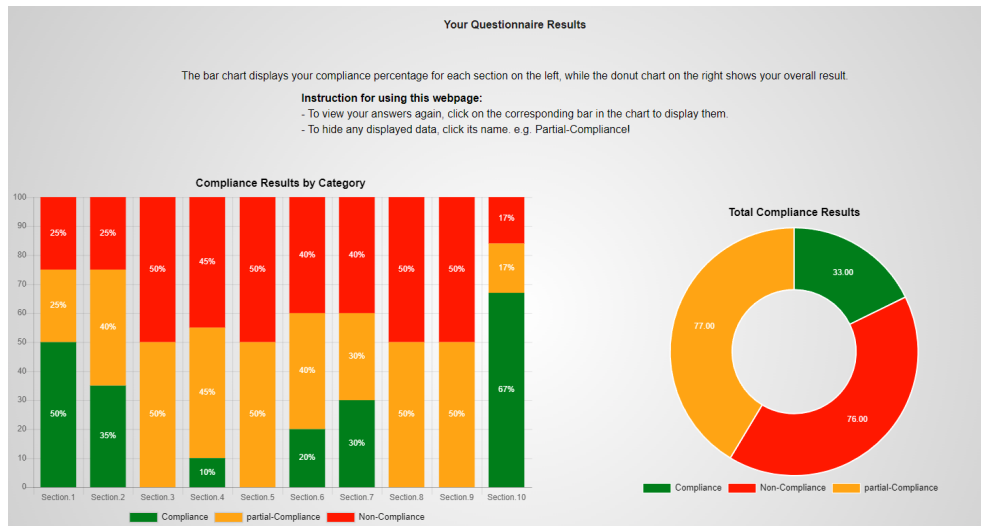


Figure 6.16: Display legal results Healthcare example

As mentioned it runs code established earlier and as such it has functionality that mirrors the other results page. For instance if you click a bar, questions within that part of the questionnaire would be displayed.

6.2.11 Admin Panel

Our website incorporates an administration panel interface (see Figure 6.17) designed to facilitate user and company management. The administration panel uses security measures to ensure that only authorized administrators user can access its features. Once an administrator successfully logs in, a dedicated admin panel button will appear in the navigation bar, providing access to the interface.

The administrative panel interface offers a comprehensive set of controls that enable administrators to manage user accounts and companies within the system. Through a user-friendly interface, administrators can easily add or delete users or companies by simply selecting the corresponding buttons located on the control panel on the left side.

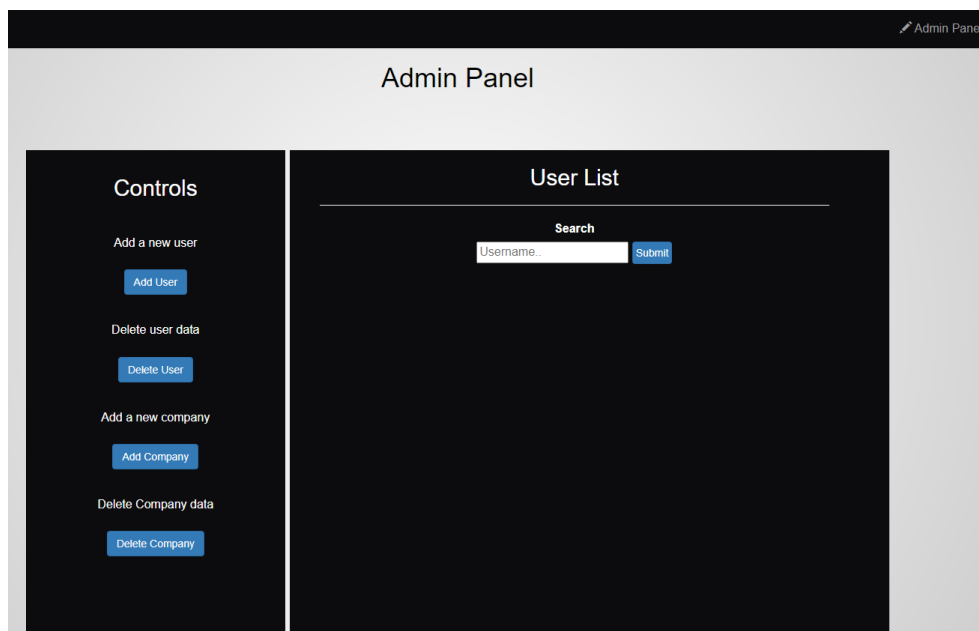


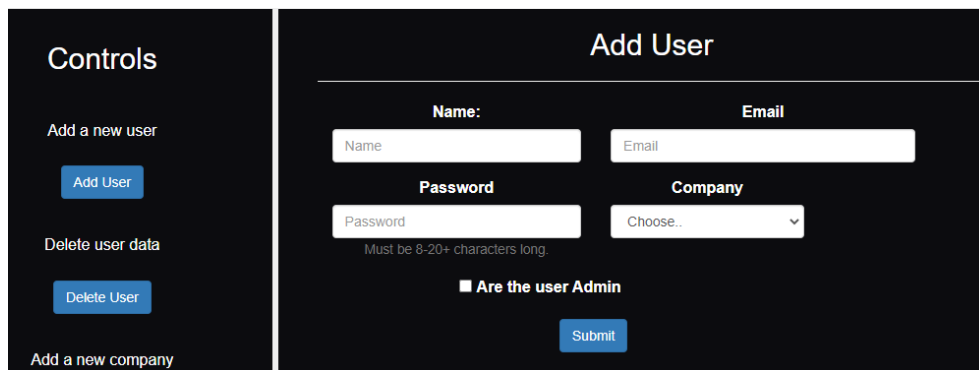
Figure 6.17: Admin panel interface

Admin panel controls

The interface incorporates four essential controls, each of which will be explained in the following sections:

Add user:

Upon clicking the "Add User" button as shown in the figure below, a data input form will appear on the right side of the panel. This form requires the administrator to input the new user account information in order to add a new user to the database. The required fields for data entry include the user's name, email, password and company. The company input is selective because they are limited to the existing companies within the database (see code listing 16). Additionally, there is an optional check button to indicate whether the user should be assigned administrative privileges. It is important to note that the admin check button should be used with care, as it grants significant privileges to the user in the system. All the previously mentioned input fields are mandatory, except the admin check button.



The image shows a dark-themed user interface. On the left, a sidebar titled "Controls" has three buttons: "Add User", "Delete User", and "Add a new company". On the right, a form titled "Add User" is displayed. It has four input fields: "Name", "Email", "Password", and "Company". The "Password" field has a note below it: "Must be 8-20+ characters long". The "Company" field is a dropdown menu with "Choose.." selected. Below the form is a checkbox labeled "Are the user Admin" and a "Submit" button.

Figure 6.18: Add User interface

Delete user:

Upon clicking the "Delete User" button as shown in the figure below, a search bar will appear on the right side of the panel. This search function enables the administrator to search for a specific user by inputting either the complete user name or a partial name. The search function will then retrieve and display all users whose names contain the entered characters. As well as the search functionality accepts an empty search input, which will result in the display of all users existing in the database.

After completing the search and successfully finding the user to be deleted, the administrator will be presented with the "Delete" button in the action column. In order to ensure accuracy and responsibility, an alert message will appear, requesting the administrator's confirmation prior to proceeding with the deletion process. Once the confirmation is given, the identified user will be permanently removed from the database.

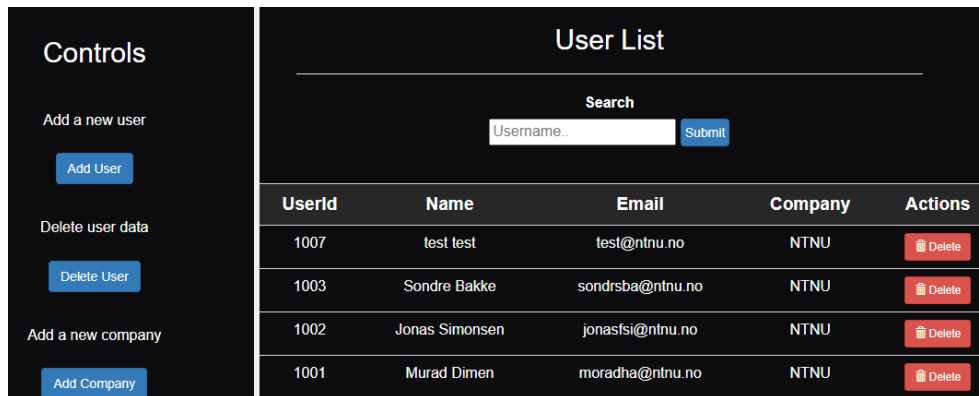


Figure 6.19: Delete User interface

Add company:

The "Add Company" function operates as shown in the figure below is similar to the user-adding function but with a different input form. Upon selecting the "Add Company" button, a form for adding company information will be displayed, requiring the administrator to enter the company name and its website URL. After the addition of a company to the database, its name will become available in the user adds interface, allowing the administrator to select it when needed.

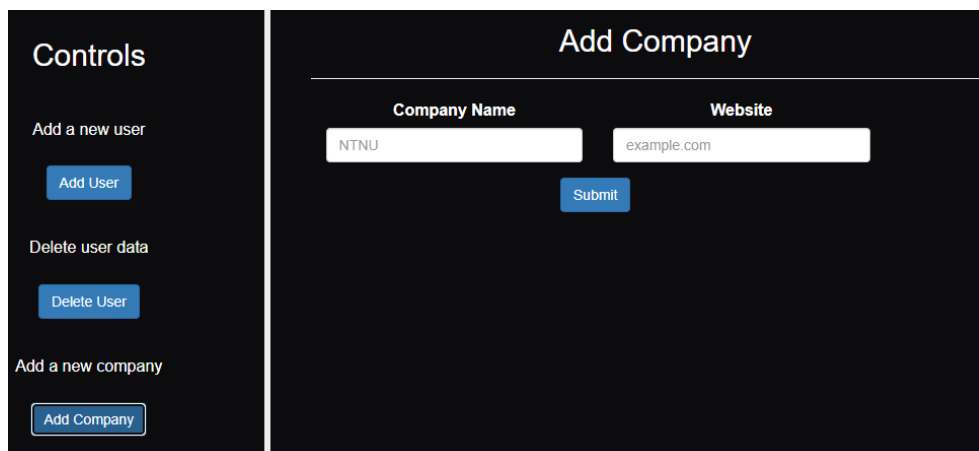


Figure 6.20: Add Company interface

Delete company:

The company deletion function as shown in the figure below operates similarly to the user deletion function. After selecting "Delete company," the current existing companies in the database will be displayed on the right side, as shown in the accompanying figure 6.21. This approach has been implemented and excluded the search bar function due to the uncertain number of companies expected to utilize this platform, with the current list having only two companies.

Similar to the user deletion function, a confirmation alert message will be presented upon clicking the delete button, requesting the administrator's confirmation prior to proceeding with the deletion process.



Company List			
CompanyId	Company Name	Website	Actions
1001	Sopra Steria	www.soprasteria.no	Delete Company
1002	NTNU	www.ntnu.no	Delete Company

Figure 6.21: Delete Company interface

Controls functionality:

On clicking any of the previously mentioned control buttons, the associated function responsible for the corresponding process is invoked. The function facilitates the loading of the required form by utilizing a separate function. In the provided code sample, we see one of the loading functions `loadUserForm()` (see code listing 6), the one responsible for loading the user-adding form. The loading functions initiate an HTTP request upon button click, then opens and send a GET request to the designated file responsible for loading the form and implementing the function.

The mentioned method is used for loading all other forms within the system in the admin panel interface as well. However, each form utilizes a different function. These functions follow a similar pattern by generating an HTTP request upon button click, accessing the relevant file, and loading the form along with its associated functionality.


```
1 function loadUserForm() {
2   var usersListDiv = document.querySelector('.contentList');
3   var xhr = new XMLHttpRequest();
4   xhr.onreadystatechange = function() {
5     if (xhr.readyState === XMLHttpRequest.DONE) {
6       if (xhr.status === 200) {
7         usersListDiv.innerHTML = xhr.responseText;
8       } else {
9         alert('There was a problem loading the form.');
```

Listing 6: Open and send requests code sample

On clicking the delete button associated with either a user or a company displayed in their respective tables, the corresponding deletion function (see code listing 7) is invoked. The function initiates an alert, waiting for confirmation from the administrator. Once confirmed, the system extracts the user or company ID and passes it to the relevant file responsible for executing the deletion query in the database, effectively removing the entity from the database.

The deletion process for companies follows the same functionality as the code sample 7 below but utilizes the company ID instead.

```
1 function DeleteUser(user_id) {
2   if (confirm("Are you sure you want to delete this user?")) {
3     window.location.href = "./controls/deleteUser.php?user_id=" + user_id;
4   }
5 }
```

Listing 7: Send a delete request code sample

6.3 Backend

In this section, we shall explicate the back-end implementation of our model, encompassing the components such as the database, security measures, and the utilization of JSON files. Additionally, we will delve into the database queries used for retrieving and inserting data.

6.3.1 Database

The database of our system currently consists of two tables as depicted in Figure 6.22.

The first table, known as the **user** table stores essential information about the users within the system, and contains six key columns: **user-ID**, **name**, **email**, **password**, **company-ID**, and **admin**. The **user-ID** uses as the session identifier during the login and logout process, while the email and password combination is utilized to authenticate authorized users. Furthermore, the name attribute is employed to assign a specific name to the JSON file generated upon completion of a user's questionnaire. The **company-ID** field uses the purpose of identifying the company to which a user belongs. Lastly, the **admin** column is utilized to define whether a user possesses administrative privileges or not.

While the second table, known as the **company** table stores essential information about the companies within the system and contains three key columns: **company-id**, **company-name**, and **website**. The **company-id** column uniquely identifies each company within the system, while the **company-name** column indicates the name of the respective company. Similarly, the **website** column corresponds to the website associated with the company.

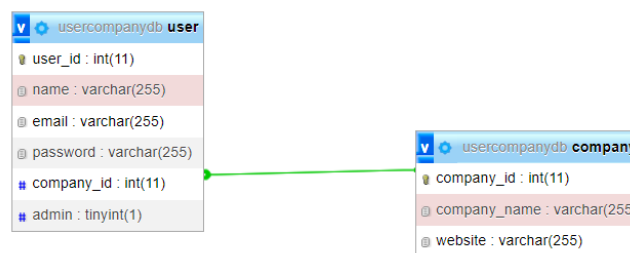


Figure 6.22: Database Tables

To ensure the security and integrity of our system, we have implemented a protocol that mandates users to request account creation or modification from an administrator. Only individuals with authorized administrator access privileges are allowed to create or modify user or company accounts in our system database via the designated administrative panel.

6.3.2 Login and Session start Process

Upon successful input of login data by the user (see Figure 6.4), the provided information is then sent for authentication. The authentication first start with establishing a connection with the database via connection methods in connection.php.

```
1 <?php
2     $host = "192.168.1.25t";
3     $email = "root";
4     $password = 'passord';
5     $db_name = "usercompanydb";
6
7     $con = mysqli_connect($host, $email, $password,$db_name);
8     if(mysqli_connect_errno()) {
9         die("Failed to connect with MySQL: ". mysqli_connect_error());
10    }
11    ?>
```

Listing 8: Code Example for the DB-connection

If the connection succeeds the authentication PHP file then sends a MySQL query to the database using the POST method to check if the user exists within it. The query contains the email and password provided by the user. If the user exists in the database, all user data is fetched, and a session is initiated using the user-id, name, and checks if the user is admin. Subsequently, the user is redirected to the workspace interface. However, if the user does not exist in the database, an error message is displayed, and the user is kept on the login page.

```
1 <?php
2 session_start();
3 include('connection.php');
4
5 $email = $_POST['email'];
6 $password = $_POST['password'];
7
8 $sql =
9     "select * from login where email = '$email' and password = '$password'";
10 $result = mysqli_query($con, $sql);
11 $row = mysqli_fetch_array($result, MYSQLI_ASSOC);
12 $count = mysqli_num_rows($result);
13
14 $url = "../Pages/Workspace.php";
15
16 if($count == 1){
17     $_SESSION["user_id"] = $row['user_id'];
18     $_SESSION["admin"] = $row['admin'];
19     $_SESSION["name"] = $row["name"];
20
21     header("Location: $url ");
22 }
23 else{
24     echo "<script>if(confirm('Login failed. Invalid email or password.'))
25         {document.location.href='../Pages/login-form.html'};</script>";
26 }
27 ?>
```

Listing 9: Code Example for the authentication

6.3.3 Session check Process

The session check mechanism plays a vital role in maintaining the security of web applications. It operates by verifying the authentication status of a user attempting to access a restricted interface. If the user is not logged in, the session check redirects them to the login interface and prevents unauthorized access to the interface. This mechanism acts as a gatekeeper, protecting the confidentiality and integrity of the applications.

```
1 <?php
2 session_start();
3 if (!isset($_SESSION["user_id"])) {
4     header("Location: ../Pages/login-form.html");
5     exit();
6 }
7 ?>
```

Listing 10: Code Example for the session check

6.3.4 Logout Process

Upon completing their interaction with the website, users are provided with the option to log out. This functionality is facilitated by the destruction of the sessions that are established when the user initially logs in. Specifically, the logout process entails the resetting of the session variable to an empty value and the subsequent elimination of the pre-existing session. Through this method, users are able to securely terminate their active session on the website.

```
1 <?php
2 session_start();
3 $_SESSION["user_id"] = "";
4 $_SESSION["name"] = "";
5 $_SESSION["admin"] = "";
6 session_destroy();
7 header("Location: ../index.php");
8 ?>
```

Listing 11: Code Example for the log out

6.3.5 API

Fetch API

This code searches for a file named "Questions.json" which contains a collection of questions. If the file is located successfully, the program (code) will display the contents of the file. However, if the file is not found, an error message will be sent to the console.

```
1 fetch('Questions.json')
2   .then( response => {
3     if (!response.ok) {
4       throw new Error(`HTTP error: ${response.status}`);
5     }
6     return response.json();
7   })
8   .then( json => initialize(json) )
9   .catch( err => console.error(`Fetch problem: ${err.message}`) );
```

Listing 12: Code Example get questions

6.3.6 JSON file

In our model, we utilize four distinct JSON files. The first file Ouestions.json, which remains constant and is stored on our system, comprises the questions that we have formulated and utilize to display in the questionnaire. This file is structured in a manner that encompasses various sections, along with questions assigned to each section. In certain sections, we have included additional variables that contain the sub-section title and a corresponding description. The following code sample elucidates the format of the mentioned file.

```
1  [
2    {
3      "section": "WILL CONTAIN THE SECTION TITLE",
4      "sectionDescription": "WILL CONTAIN THE SECTION Description",
5      "questionsList":
6      [
7        {
8          "q": "WILL WILL CONTAIN THE QUESTION "
9        }
10     ]
11   },
12   {
13     "section": " ",
14     "sectionDescription": " ",
15     "questionsList":
16     [
17       {
18         "TipsTitle": "WILL CONTAIN A SUB-SECTION TITLE",
19         "Tips": "WILL CONTAIN A SUB-SECTION DESCRIPTION",
20         "q": " "
21       }
22     ]
23   }
24 ]
25
```

Listing 13: code sample of questions.json file

The second JSON file corresponds to the output that users receive upon completion of the questionnaire. This file has a specific format, which is predefined in the questionnaire function. The purpose of this format is to enable efficient reading and analysis of the data, ultimately resulting in the display of results through the two aforementioned charts Figure 6.8 and Figure 6.10. The following code sample elucidates the format of the mentioned file.

```
1 {
2 {
3   "SECTION TITLE": {
4     "QUESTION-NUMBER": "ITS VALUE/USER ANSWER",
5     " ": " "
6   }
7 }
```

Listing 14: code sample of the results

The section title in the sample is the same title designated in the questions file Code listing [13]. The question number will be to indicated corresponding to the respective question in the section. The question value will be determined based on the user's response, which will be represented by three discrete values: 1, 0.5, or 0. These values correspond to positive, partial, or negative responses, respectively.

The 3rd and 4th versions of the JSON files are based upon the questions.JSON file, except with questions dedicated to the specific sectors rather than a security maturity rating. The number of questions gets done slightly differently by using a loop rather than numbering in the file itself. The questions here are also split into bulks of 10 rather than annexes in security maturity rating.

6.3.7 Admin panel backend

In this section, we will explain the back-end implementation of the administrative panel and its various controls, we will also discuss their respective functionalities. This comprehensive explanation provides a detailed determination of each control's development process. It also aims to show how it has been effectively used to fulfill its intended purpose.

Add user

The add user function begins by presenting a user-friendly form to gather essential information required for creating a new user Figure 6.18. Once the user submits the necessary inputs, the PHP code establishes a connection to the database and proceeds to execute an insert query with the provided values, thereby adding the user to the system. Furthermore, the code verifies the success of the execution, and in the event of failure, it sends alerts with an error message. Finally, the code concludes by closing the established database connection.

```
1 <?php
2 if ($_SERVER["REQUEST_METHOD"] == "POST") {
3     $name = $_POST['name'];
4     $email = $_POST['email'];
5     $password = $_POST['password'];
6     $company_id= $_POST['company_id'];
7     $admin = isset($_POST['admin']) ? 1 : 0;
8
9     $con = new PDO
10         ("mysql:host=192.168.1.25; dbname=usercompanydb','root', 'password');
11
12     $query = $con->prepare
13         ("INSERT INTO user ( `name`, `email`, `password`, `company_id`, `admin`)
14         VALUES ( :name, :email, :password, :company_id, :admin)");
15
16     $query->bindParam(':name', $name);
17     $query->bindParam(':email', $email);
18     $query->bindParam(':password', $password);
19     $query->bindParam(':company_id', $company_id);
20     $query->bindParam(':admin', $admin);
21
22     if ($query->execute()) {
23         header("Location: ../adminPanel.php");
24     } else {
25         echo "<script>if(confirm('Error adding User.'))
26             {document.location.href=' ../adminPanel.php'};</script>";
27     }
28     $con = null;
29 }
30 ?>
```

Listing 15: Add User Query code sample

The add user form has a selective input feature for the company, wherein the administrator is required to choose the company that the new user belongs to. The following code sample (see code listing 16) shows the process of retrieving and displaying the available company names as selectable options. The code first establishes a connection with the database and executes a query to fetch all the existing companies stored in the database. These company names are then presented as options for the user to choose from.

```

1 <label for="inputState">Company</label>
2 <select id="inputState" class="form-control" name="company_id" required>
3   <option value="" disabled selected>Choose..</option>
4   <?php
5     $con = new PDO
6       ("mysql:host=192.168.1.25; dbname=usercompanydb", 'root', 'passord');
7     $query = $con->query("SELECT company_id, company_name FROM company");
8     while ($row = $query->fetch()) {
9       echo "<option value='" . $row['company_id'] . "'>"
10          . $row['company_name'] .
11          "</option>";
12     }
13   ?>
14 </select>

```

Listing 16: Select company code sample

Search for user

The search functionality operates by extracting the text input entered into the search bar by the administrator, then employing it as a query parameter for searching user names in the database. This query involves locating users whose names match the provided text or contain a partial match.

```

1 $query = $con->prepare(" SELECT `user`.*, company.company_name
2 FROM `user`
3 INNER JOIN company ON `user`.company_id LIKE company.company_id
4 WHERE `user`.name LIKE '%$userName%'");

```

Listing 17: Search for user code sample

Upon finding the user, a table will be presented Figure 6.19, displaying all user information. The table will incorporate an action column, affording the administrator the ability to delete a specific user via a delete button.

```

1 while ($row = $query->fetch(PDO::FETCH_OBJ)) {
2     echo "<tr>
3         <td>{$row->user_id}</td>
4         <td>{$row->name}</td>
5         <td>{$row->email}</td>
6         <td>{$row->company_name}</td>
7         <td>
8             <a class='btn btn-danger btn-sm'
9                 onclick=\"DeleteUser($row->user_id)\">
10                <span class='glyphicon glyphicon-trash'></span> Delete</a>
11        </td>
12    </tr>";
13    }

```

Listing 18: Display user table code sample

Delete user

Upon the user deletion button being clicked and the deletion is confirmed by the administrator (see Figure. 6.19), the user ID is then passed to the function to initiate the deletion process as shown in the code sample (see code listing 7).

The code sample below will then establish a connection to the database to execute a deletion query using the passed user ID. Once the query execution is completed, the connection is closed, and the administrator is redirected back to the administrative panel.

```

1 <?php
2     $user_id = $_GET['user_id'];
3     $con =
4     new PDO("mysql:host=192.168.1.25; dbname=usercompanydb", 'root', 'passord');
5
6     $query = $con->prepare("DELETE FROM user WHERE user_id = :user_id");
7     $query->bindParam(':user_id', $user_id);
8
9     $query->execute();
10    $con = null;
11    header("Location: ../adminPanel.php");
12    ?>

```

Listing 19: Delete user code sample

Add company

The addition of a company function operates similarly to user addition. It presents a form that collects the required information for creating a new company Figure 6.20. These input values are then utilized in the query sent to the database. As shown in the code below:

```
1  $query = $con->prepare("INSERT INTO company (company_name, website)
2      VALUES (:company_name, :website)");
3
4  $query->bindParam(':company_name', $company_name);
5  $query->bindParam(':website', $website);
```

Listing 20: Add company Query code sample

Search for company

The search company functionality works similarly to the user searching, but here we don't provide a search bar, the search functionality is activated by clicking the Delete company button in the control section. Upon clicking a query will be executed to retrieve all existing company data from the database. The retrieved data is then displayed in the company table (see Figure 6.21).

Delete company

The functionality for deleting a company operates similarly to the deletion of a user, utilizing the company ID as a parameter in the query to the database.

Chapter 7

Discussion

In this chapter, we will discuss the work and decisions we made during the project. We will look closer at what the group did well, but also what parts could have been improved. Any changes during development are also mentioned here.

7.1 Evaluation

In this section, we will go over to what degree our application complied with previously established requirements. We will see results from user testing as well as the internal tests in regard to how compliant the website is with the functional requirements.

7.1.1 Overall functional requirements

In this section, we will cover to what degree the application complied with the functional requirements set in the "requirements" chapter. Table 7.1 below shows the way both internal and external testers saw our fulfillment in regard to functional requirements. Internal testing was done by the team throughout the whole development process. We continually checked that the website and the functions were working as intended. The external testing was done by Sopra Steria and other friends/students that we sent out forms to. The feedback from friends/students is just from the interface of the model and the general readability of the text because they are not qualified to review the questions.

Table 7.1: Functional Requirements Testing table

Functional Requirement	Internal testers	External testers
1: The model should check what sector and services the organization operates in.	Passed	Partly Passed
2: The model should display what laws and regulations an organization is required to follow	Passed	Passed
3: The model should check the compliance to current regulations	Passed	Passed
4: The model should check the organizations general information security standards	Passed	Passed
5: The model should test the organization's human resource policy, and access to data that is granted to employees and contractors	Passed	Passed
7: The model should be able to display to what degree a company complies with the ISO27001 standard.	Passed	Passed
8: The model should be able to export the results as data.	Passed	Passed

7.1.2 Functional requirements in detail

Requirement 1: Check what sector the organization is in

The applications fulfillment regarding functional requirement 1 is decent. Due to the limitations of the assignment we only used two sectors. It is however easy to add more sectors in the future if needed. It is easy for the user to choose the correct sector or service they specialize in through CyberTest4You. In the future, it could also be possible to predetermine the correct sector/service for the company, so they only have access to the correct ones, but this is not something we added in this version of the model.

Requirement 2: Display what laws and regulations an organization is required to follow

This requirement was followed, however, it could have been made clearer exactly which laws should be followed. In the future, the model could also give specific feedback based on the answers of the users for each question. For instance, if a company within healthcare does not have multi-factor login as a requirement, they can get specific improvements that they should apply in order to be compliant.

Also when the user completes the questionnaires related to sectors, it could have been more convenient if it displayed a list of the laws/regulations the user failed to follow after the test is completed. The way the website works now is more clunky, but it is still possible to see what laws are not compliant by looking at the results in the "display results" tab. We would have tried to implement this solution if we had more time.

Requirement 3: Compliance to current regulations

It was somehow confusing as to what laws and regulations specifically we should add to the model. This model covers local Norwegian laws within healthcare and finance, however, in a lot of sectors (like finance), the institutions have to follow regulations that are made by international organs (like the European Union) which is valid for many countries in Europe. Many of the local laws are just versions of these laws, and it is hard to distinguish them from international laws.

If we were to add every IT law or regulation related to an advanced sector like finance or similar it would take ages to not only gather all the information but also for the user to complete the test. This is why we only added the "Regulations on the use of Information and communication technology" developed by the Norwegian Ministry of Finance - because they differed from EU laws. This law is the most important related to information security in finance locally in Norway, and it was also intended for several financial institutions [44].

In the future, the model should be clearer as to exactly which regulations each institution must follow, but getting an overview of this is a difficult task. Regulations can also be different for specific companies within sectors. Insurance companies might for instance have different regulations they have to comply with than banks. A solution to this could be to change the "sectors" part of the model with specific institution-based laws. For example let the user choose between "hospital", "bank", "nursing home" etc.

The regulations related to the healthcare sector were easier to create because we could use information from "The Norm", which is an industry standard in the healthcare sector. This standard has an overview of all the regulations institutions in healthcare has to comply with. It is developed by several organizations within the healthcare sector [45]. This standard also has specific questions related to who is answering. The questions will be different if an IT-administrator that is responsible for information security answers compared to a manager. This is something our model is lacking and is something we would implement if we were to create a model like this again.

We also noticed that many of the regulation laws were similar to the ISO27001 standard. This means that some companies would be fully compliant as long as they were compliant with the ISO27001 standard. In that case, it would be unnecessary to complete both questionnaires.

This requirement passes, but there is definitely room for improvement.

Requirement 4: The model should check the organization's general information security standards

The model does check the organization's general information security standards through ISO27001. This standard is a great way for companies to get a general overview of their maturity regarding information security, which was a part of our assignment from Sopra Steria.

Requirement 5: Test the organization's human resource policy, and access to data that is granted to employees and contractors

The model maps an organization's human resource policy and checks if they protect its internal data. It does this both through the ISO27001 test and the compliance test. This point in the functional requirement passes.

Requirement 6: Display to what degree a company complies with the ISO27001 standard

The model does display to what degree a company complies with the ISO standard. It also gives an overview of what degree it complies with every individual question.

We also had "partially compliant" as an alternative answer to the questions. The only negative related to this is that in certain questions can be hard for the company to know what they should do in order to become fully compliant. In a future version of the model, this would be improved because it would also include detailed instructions to become compliant.

Requirement 7: Able to export the results as data

The model is able to export the results as data. The JSON file is a common file format, and it is also possible to convert it to other file formats (like excel). In the future, it could be possible to add a function in the model so the user can choose which format to download the file. This way it would be possible to view or edit the file in whatever program the user is comfortable with.

7.1.3 Non-Functional Requirements

The general non-functional requirements for the project were fulfilled as follows:

- **Usability**
The feedback the group got back in regards to how easy to use the application means the fulfillment of this non-functional requirement was fulfilled, but there is room for improvement.
- **Compatibility**
As the tools used during the creation, testing, and production of the application are commonly used during web development as well as supported by modern browsers this point passes. Also capable of running on mobile browsers.
- **Performance**
The performance of the application has not been reported as an issue. No noticeable delays have been noticed during product testing and since the application runs on widely used modules performance is also not likely to decrease any meaningful amount.
- **Security**
This point is lacking to some degree because a digital certificate has not been implemented on our platform. It can however be implemented in the future since all tools used are compatible with using the encrypted version of HTTP.
- **Reliability**
The reliability of the model is maintained by running several servers in a load balancer and having automatic bash scripts on each server running to make sure the application is running. Any updates to the tools used for reliability should not hamper any performance as they are widely supported.

7.2 User feedback

The user feedback received during the testing of the application was performed by fellow university students and Sopra Steira. Below we will display some graphs in regard to how users found the different aspects of the website.

User Friendliness

Below shows two pie charts on how user-friendly users found our website.

How user friendly do you find the user interface of the application?

9 svar

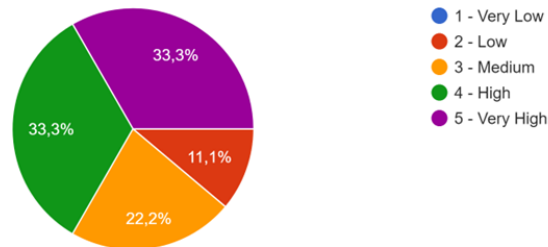


Figure 7.1: user Friendliness Pie chart

How easy did you find the text descriptions in the application?

9 svar

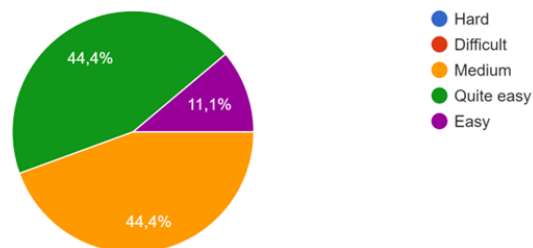


Figure 7.2: Understandable descriptions

The pie chart in Figure 7.1 shows that generally users find the UI of the application user-friendly. Figure 7.2 also shows that most of the testers find the descriptions provided to be a mix of "easy" and "medium" difficulty to understand. Some testers had some comments in areas where they would improve the UI or where they had issues with it. Those include:

- Being able to start the legal questionnaire from the sector information pages.
- chunky interface
- Too much text.

Time spent completing the security framework questions?

The following figure shows the time spent for completing the security framework questions.

How long did it take to complete the Security maturity questions? (in minutes)
9 svar

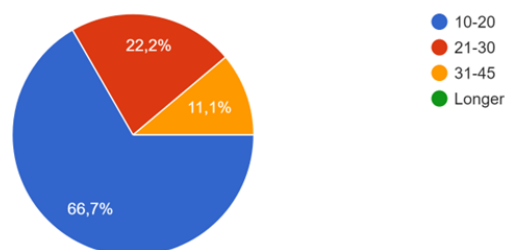


Figure 7.3: Time spent to complete Security Maturity questions

How understandable was the security framework questionnaire?

It is important for users to understand the questions asked during the questionnaire. An important note is who the test is designed for, and simplistic questions may not be enough to determine if organizations comply with the framework.

Was the Security Maturity Questionnaire questions understandable?
9 svar

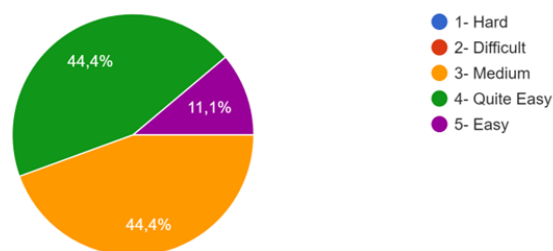


Figure 7.4: How understandable were the security framework questionnaire pie chart

The response to the questions asked during the testing shows that the users that took the test had no issues with them. They in a sizable majority found the answers easy to understand.

Healthcare

Healthcare of the two sectors was by far the one with the most thorough regulations.

How long did it take to complete the Healthcare regulation questions? (in minutes)
8 svar

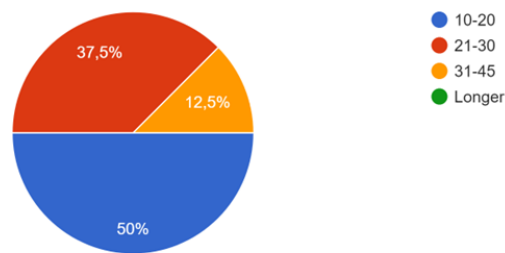


Figure 7.5: healthcare Time to complete

Did you find the questions in the Healthcare questionnaire understandable?
8 svar

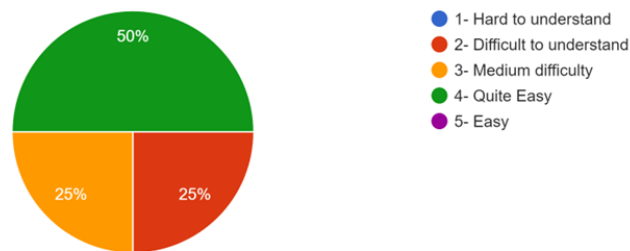


Figure 7.6: healthcare Understandable

The results of user feedback as seen in figures 7.5 and 7.6 show that users generally found the questions to be on the easier side.

Finance

Finance regulations also got above-average ratings in terms of how easy it was for users to understand the questions. However, it is the one questionnaire with the most mediocre user feedback. It may be a suggestion that for future improvements to the model, the finance part will get different questions. The results from Figures 7.7 and 7.8 also show that it is the test the users spent the least amount of time on.

Did you find the questions in the financial questionnaire understandable?

8 svar

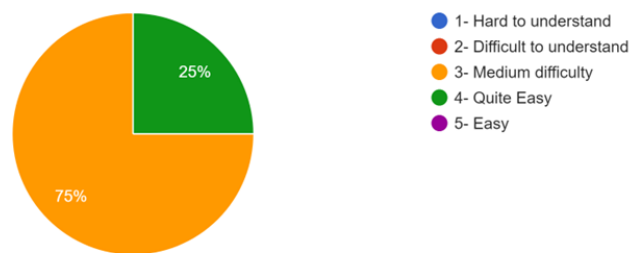


Figure 7.7: Finance Understandable questions

How long time did you use to complete the "financial" questionnaire?

8 svar

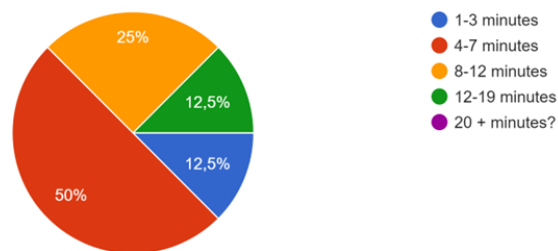


Figure 7.8: Finance Time to complete questions

7.3 Approach

During the creation of the project, we were given a lot of freedom in regard to how the project was to be completed by Sopra Steira. We quickly came to the conclusion that developing a website for the model fit the requirements.

7.3.1 Problems

User testing

- As the people user testing the model requires some background knowledge in regards to using the model, getting people with said knowledge has been challenging.

Development

- **Programming languages:** During our studies developing web pages have not been a major part of the curriculum. Naturally inserting yourself into different programming languages takes time.
- **Charts:** The challenge we faced during the development of the model was finding the appropriate tool to effectively demonstrate the report. It took considerable effort and time to find the solution for this task.
- **JSON file:** The challenge we faced was determining the most appropriate method for storing user answers. We successfully implemented and formatted the sections in a JSON file, although it required significant time and effort to arrive at the appropriate approach.
- **Component interactions:** The challenge of integrating various components and ensuring their interaction to achieve the required functionality.

Chapter 8

Conclusion

8.1 Conclusion

As stated in Chapter 1, this project's goal was to design and create a model where organizations can check their compliance with security frameworks and legal regulations. We were given a lot of freedom from Sopra Steira on how to complete the assignment and fulfill the requirements of the model, and it has been a challenging and educational experience.

8.2 Learning outcome

This section of the report will cover what we learned overall during the project. It covers what we have learned in general, but also about specific parts of the project.

General

In general, no team members had much experience developing a model of this scope. We have all worked in groups before, but it has been mostly smaller and not as demanding projects. Working on the model could sometimes be a frustrating experience, especially when the code does not work as intended, or it seems impossible to find the information you are looking for. Because we did not have experience in creating a product from scratch, it could be hard to know the best approach. We are not used to having this much freedom, because assignments we have completed are usually more straightforward, and you have to follow a general recipe in order to finish the project.

To our understanding, there are also not many that have made a model like us, and especially not a model that is meant for the Norwegian market like ours. This also made it harder to know the best approach to creating the model. In hindsight, we could possibly have been a bit better at using our supervisor and contact from Sopra Steria more efficiently to hear if our approach and tools we used were the

most logical.

Overall it has been very fun and we have learned a lot. We also think that this model is something that could help organizations, and it can also definitely be useful for consulting services like Sopra Steria.

Thesis writing

As this is our first bachelor project we had quite the learning experience writing such an advanced report, especially in an environment like \LaTeX . It took some time to get used to the \LaTeX formatting and make sure all our figures and paragraphs were correctly sized and placed. Formatting the document can take a lot of time, and we should have prioritized doing this more during the project than toward the end.

Information Security Standards and legal regulations

During the creation of the project, we learned what being compliant with several information security frameworks meant. In particular, we learned in detail about what was required for the ISO27001 standard and what steps were required to become certified.

As we already wrote in the "discussion" chapter, it can be very overwhelming to know every information security law or regulation related to a sector. It is also very important to get this correct because if a law or regulation is forgotten, it can lead to devastating consequences for the company. If we were to make another model, it could have been beneficial to work together with a lawyer or someone else that specializes in IT security in the relevant sector, in order to create the model as detailed and correct as possible.

Teamwork and Communication

During the creation of the application, we learned how to do teamwork where members would work on different subjects in an incremental development model. We had to communicate a lot, and a continual delegation of workload was required. Some members of the team were more focused on the technical aspect of the model, while others worked with regulations and general text. We would change this depending on where the workload was required. We worked and communicated mostly digitally, which worked fine, but there were some situations it could have been easier to communicate and work together physically.

Software Development

Software development has not been a major part of the study program. Because of this, no group members had a lot of experience developing this. We did mostly choose beginner-friendly and highly documented tools for development, which helped us a lot.

8.3 Further work

In this section, we will go over what work can further be done to either the model, GUI, or report. There are a lot of parts of the model that can be improved, and several possible improvements have already been mentioned in the report.

Sectors and user roles

- Adding more sectors so companies within other fields will have the ability to check their compliance. A lot of companies have confusing regulations, and having a broader model with a bigger variety of sectors would add a lot of usability. As also mentioned in the "discussion" chapter, it could be more logical to not add sectors, but specific questionnaires for the specific institution. This would however depend on the sector. In the healthcare sector, most institutions have to follow the same laws and regulations.
- The questions in our model are made for whoever is in charge of IT security. Because other roles (manager, data processor, etc) also are relevant to be fully compliant, the questionnaires should have different subsections where employees with different roles and responsibilities can give their answers.

User Interface

There are definitely improvements that can be made to the user interface, and our user test also displays this.

- It should be possible to enter the legal/regulation questionnaire directly from the relevant sector. At the moment you have to first read general info about the sectors on the homepage, and manually go to the "testing center" part of the model in order to start the compliance test.
- Adding more languages to the GUI so it becomes more user-friendly. For now, our model is only in English, and it could possibly make more sense to have the model in Norwegian, or at least have the option to change the language. This is because the model is made for local Norwegian regulations, and it makes sense that Norwegian companies would perform the tests.
- Some parts of the user interface also have a lot of text. This can become overwhelming for the user, so these parts should be made shorter. It could also be more use of images to illustrate points and better formatting with the black boxes in the "testing center".

Frameworks

- Making the model capable of testing information security towards more frameworks. Although ISO27001 is among the top international standards for testing IT security, there are also other frameworks that can be helpful. This includes the NIST cybersecurity framework or GDPR. If the model were able to test against these instead of ISO27001, it can be helpful. However, a lot of these frameworks cover almost the same sections as ISO27001.

Results

- The model should give a rating of each question based on what importance they have in the ISO questionnaire. The model is now designed as if every question counts the same amount towards the compliance rating, but the reality is that some annexes are more important than others. These should give a better compliance rating compared to others.
- The model should have the ability to give specific recommendations based on the answers from the users. For now, the model just gives a rating of "yes", "no" or "partially" if the company is compliant. Getting a recommendation of exactly what the company needs to implement can be very helpful.

Questionnaire from user evaluation

- We did not get as many user evaluations from actual companies within the sectors as we had hoped for. Some further work can be done to get more user evaluations from them and change the model according to their needs.
- We could have performed the user evaluations earlier than we did, in order to have more time to make improvements to the model. We had a lack of time in the last couple of weeks of the project to implement all the changes that we would like to. Here we could have some better time management. We failed to follow our Gantt chart as carefully as we had hoped.

8.4 Summary

Overall it has been a very interesting and fun experience. We have learned a lot, not only academically, but also about teamwork and how to develop a product from scratch. We also think that models like the one we created will only become more popular among organizations. Cybersecurity is becoming more and more important, but many organizations still have a long way to go in order to become as protected as possible.

Bibliography

- [1] S. Steira. 'Sopra steira.' (), [Online]. Available: <https://www.soprasteria.no/> (visited on 13/02/2023).
- [2] G. Fines. 'Gdpr fines.' (), [Online]. Available: <https://gdpr.eu/fines/> (visited on 23/02/2023).
- [3] E. Commision. 'Gdpr fines.' (), [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en/ (visited on 23/02/2023).
- [4] E. Commision. 'Do we always have to delete personal data if a person asks?' (), [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en (visited on 23/02/2023).
- [5] J. Dutton. 'What is an information security management system (isms)?' (Aug. 2023), [Online]. Available: <https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2> (visited on 14/02/2023).
- [6] R. Alavi, S. Islam and H. Mouratidis, 'A conceptual framework to analyze human factors of information security management system (isms) in organizations,' in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas and I. Askoxylakis, Eds., Cham: Springer International Publishing, 2014, pp. 297–305, ISBN: 978-3-319-07620-1.
- [7] T. Holtebekk. 'Iso.' (), [Online]. Available: <https://snl.no/ISO> (visited on 20/03/2023).
- [8] ISO. 'Iso/iec 27001:2013.' (), [Online]. Available: <https://www.iso.org/standard/54534.html> (visited on 20/03/2023).
- [9] G. Disterer, 'Iso/iec 27000, 27001 and 27002 for information security management,' *Journal of Information Security*, vol. 2013, pp. 92–100, 2013.
- [10] L. M. N. Eguia, 'Snatched up by advertising partners: Norwegian dpa fines grindr for lack of consent over third-party data sharing,' *Eur. Data Prot. L. Rev.*, vol. 8, p. 289, 2022.

- [11] O. Tambou, 'Lessons from the first post-gdpr fines of the cnil against google llc,' *Eur. Data Prot. L. Rev.*, vol. 5, p. 80, 2019.
- [12] M. Melkild. 'Opprettholder sats-bot på 10 millioner kroner.' (), [Online]. Available: <https://www.finansavisen.no/tjenester/2023/02/08/7983872/datatilsynet-oppretholder-sats-bot-pa-10-millioner-kroner?zephrossoott=Kwh6LN> (visited on 08/02/2023).
- [13] J. Hildrum. 'Stortingets administrasjon vedtar ikke milliongebyr etter dataangrep.' (), [Online]. Available: <https://e24.no/norsk-oekonomi/i/JxwKw8/stortingets-administrasjon-vedtar-ikke-milliongebyr-etter-dataangrep> (visited on 14/02/2023).
- [14] D. Kessel and A. B. Larsen. 'Hacket kommune får 16 millioner kroner i statsstøtte.' (), [Online]. Available: <https://www.nrk.no/innlandet/ostre-toten-kommune-far-16-millioner-kroner-i-statsstotte-etter-dataangrep-1.15776277> (visited on 28/02/2023).
- [15] L. Chung and J. C. S. do Prado Leite, 'On non-functional requirements in software engineering,' *Conceptual modeling: Foundations and applications: Essays in honor of john mylopoulos*, pp. 363–379, 2009.
- [16] A. W. Services. 'What is a lamp stack?' (), [Online]. Available: <https://aws.amazon.com/what-is/lamp-stack/> (visited on 09/04/2023).
- [17] J. Wallen. 'Ubuntu server: A cheat sheet.' (), [Online]. Available: <https://www.techrepublic.com/article/ubuntu-server-the-smart-persons-guide/> (visited on 14/03/2023).
- [18] I. Wigmore. 'Headless server.' (), [Online]. Available: <https://www.techtarget.com/whatis/definition/headless-server> (visited on 14/03/2023).
- [19] A. H. S. Project. 'Apache http server project?' (), [Online]. Available: <https://httpd.apache.org/> (visited on 09/04/2023).
- [20] R. Giaquinto. 'What is apache and what does it do for website development?' (), [Online]. Available: <https://www.greengeeks.com/blog/what-is-apache/> (visited on 09/04/2023).
- [21] R. B. 'What is mysql: Mysql explained for beginners.' (), [Online]. Available: <https://www.hostinger.com/tutorials/what-is-mysql> (visited on 15/03/2023).
- [22] MYSQL. '1.2.1 what is mysql?' (), [Online]. Available: <https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html> (visited on 15/03/2023).
- [23] H. Lee and P. Nayak. 'Migrating facebook to mysql 8.0.' (), [Online]. Available: <https://engineering.fb.com/2021/07/22/data-infrastructure/mysql/>.
- [24] PHPnet. 'What is php?' (), [Online]. Available: <https://www.php.net/manual/en/intro-what-is.php/> (visited on 09/04/2023).

- [25] K. Chris. 'What is php? the php programming language meaning explained.' (), [Online]. Available: <https://www.freecodecamp.org/news/what-is-php-the-php-programming-language-meaning-explained/> (visited on 09/04/2023).
- [26] haproxy. 'Description.' (), [Online]. Available: <https://www.haproxy.org/> (visited on 13/02/2023).
- [27] avinetworks. 'Round robin load balancing definition.' (), [Online]. Available: <https://avinetworks.com/glossary/round-robin-load-balancing/> (visited on 14/02/2023).
- [28] Traefiklabs. 'What are sticky sessions?' (), [Online]. Available: <https://traefik.io/glossary/what-are-sticky-sessions/> (visited on 14/03/2023).
- [29] getbootstrap. 'Historyofbootstrap.' (), [Online]. Available: <https://getbootstrap.com/docs/4.0/about/history/>.
- [30] techtarget. 'Bootstrap.' (), [Online]. Available: <https://www.techtarget.com/whatis/definition/bootstrap> (visited on 10/03/2023).
- [31] w3techs. 'Usage statistics and market share of bootstrap for websites.' (), [Online]. Available: <https://w3techs.com/technologies/details/js-bootstrap> (visited on 10/03/2023).
- [32] J. N. Robbins, *Learning web design: A beginner's guide to HTML, CSS, JavaScript, and web graphics*. " O'Reilly Media, Inc.", 2012.
- [33] A. K. Ratha, S. Sahu and P. Meher, 'Html5 in web development: A new approach,' *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 3, pp. 551–554, 2018.
- [34] B. Lawson and R. Sharp, *Introducing html5*. New Riders, 2011.
- [35] Chart.js. 'Chart.js.' (), [Online]. Available: <https://www.chartjs.org/> (visited on 13/03/2023).
- [36] jsonOrg. 'Introducing json.' (), [Online]. Available: <https://www.json.org/json-en.html>.
- [37] L. Bassett, *Introduction to JavaScript object notation: a to-the-point guide to JSON*. " O'Reilly Media, Inc.", 2015.
- [38] P Klipp, 'Getting started with kanban,' *Amazon Digital Services*, 2014.
- [39] N. Salvesen. 'Thesis template ntnu.' (), [Online]. Available: <https://www.overleaf.com/latex/templates/thesis-template-ntnu/kpybjxchxnm> (visited on 29/01/2023).
- [40] T. Dohmke. '100 million developers and counting?' (), [Online]. Available: <https://github.blog/2023-01-25-100-million-developers-and-counting/> (visited on 14/03/2023).
- [41] git. 'Git –local-branching-on-the-cheap?' (), [Online]. Available: <https://git-scm.com/> (visited on 14/03/2023).

- [42] R. T. Fielding, M. Nottingham and J. Reschke, *HTTP Semantics*, RFC 9110, Jun. 2022. DOI: 10.17487/RFC9110. [Online]. Available: <https://www.rfc-editor.org/info/rfc9110>.
- [43] C. M. Lonvick and T. Ylonen, *The Secure Shell (SSH) Protocol Architecture*, RFC 4251, Jan. 2006. DOI: 10.17487/RFC4251. [Online]. Available: <https://www.rfc-editor.org/info/rfc4251>.
- [44] lovdata. 'Forskrift om bruk av informasjons- og kommunikasjonsteknologi.' (), [Online]. Available: <https://lovdata.no/dokument/SF/forskrift/2003-05-21-630> (visited on 13/03/2023).
- [45] ehelse. 'Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.' (), [Online]. Available: <https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren>.

Appendix A

Project Agreement



Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett

Er den rett som den som skaper et åndsverk har til å fremstille eksemplarer av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater

Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater

Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn

Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring

Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt:
Veileder ved NTNU: Jia-Chun Lin e-post og tlf. Jia-chun.lin@ntnu.no 45849287
Ekstern virksomhet: Sopra Steira Ekstern virksomhet sin kontaktperson, e-post og tlf.: Tea Knudsen tea.knudsen@soprasteira.no +47 404 92 089
Student: Jonas Simonsen Fødselsdato: 14 August 1999
Student: Sondre Bakke Fødselsdato: 28 November 1994
Student Murad Dimen Fødselsdato: 21 Juli 1995

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	x
Prosjektoppgave	
Annen oppgave	

Startdato: 10.01.2023
Sluttdato: 22.05.2023

Opgavens arbeidstitel er: SopraSteria - Cybersikkerhetmodenhetsmåling

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:
--

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven¹. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

¹ Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven
---	--

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt
--	---

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

x	Oppgaven skal være offentlig
---	------------------------------

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Opgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss	Sett dato
<input type="checkbox"/>	ett år
<input type="checkbox"/>	to år
<input type="checkbox"/>	tre år

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt




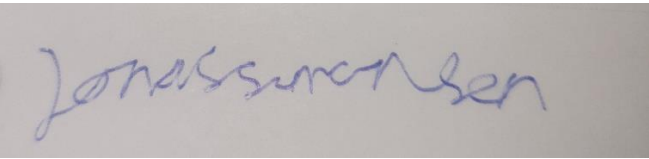

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU:  Dato: 31.01.2023
Ekstern virksomhet: Tea Knudsen  Dato: 02.02.2023
Student: Murad Dimen  Dato: 31.01.2023
Student: Jonas Simonsen  Dato: 31.01.2023
Student Sondre Bakke  Dato: 31.01.2023

Appendix B

Project Plan

Bachelor: Project Plan

Project plan for bachelor in cyber security

Sondre Bakke

Murad Dimen

Jonas Simonsen

Supervisor: Jia-Chun Lin

Faculty of Information Technology and Electrical
Engineering

Norwegian University of Science and Technology
Norway

2023 Spring

Contents

1	Background and goals	2
1.1	About us	2
1.2	Background	2
1.3	Project goals	3
2	Scope	4
2.1	Subject area	4
2.2	Task description	4
2.3	Limitations	5
3	Project organization	6
3.1	Roles	6
3.2	Role responsibility	6
3.2.1	Project leader	6
3.2.2	Minute Leader	6
3.2.3	Log Leader	6
3.3	Workflow	6
3.3.1	Communication	6
3.3.2	Meetings	7
3.3.3	Method	7
3.3.4	Collaborative tools	7
3.4	Sanctions	7
4	Planning and reporting	8
4.1	Main Project Section	8
4.1.1	Development model	8
4.1.2	Methods and Approach	8
4.2	Flowchart	9
4.3	Status Meetings and Decision Points	11
5	Quality control	12
5.1	Documentation, Standards and Source Code	12
5.1.1	Documentation	12
5.1.2	Standards	12
5.2	Configuration Management	12
5.3	Risk Analysis:	12
6	Project plan	14
6.1	Work breakdown structure	14
6.2	Gantt chart	14
6.2.1	Deliveries	15
7	Confirmation	16

1 Background and goals

1.1 About us

Our names are Murad Dimen, Jonas Simonsen and Sondre Bakke. All three students are currently studying our third year in Digital infrastructure and cybersecurity at NTNU in Gjøvik. We have a broad understanding about cybersecurity precautions companies should enable, and especially how they can secure sensitive data.

1.2 Background

Sopra Steria is a company that supervises and gives advice to other businesses in their transition to digitalize their business. They are established in more than 30 countries, and headquartered in Paris. It was established in 1969, but changed name to Sopra Steria in 2015.

Today it is more important than ever that companies store sensitive data in a secure and efficient way. There are a lot of examples of not only small companies losing sensitive data, but also big and acknowledged companies. One example of this is Yahoo![1]. In 2016 they announced that a data breach had taken place in 2014, exposing information about more than 500 million users. Some of the leaked data includes passwords, phone numbers, e-mails and security questions. Even Google failed to properly handle user data and also failed to get consent regarding ad targeting. In 2019 they got a fine which was about 50 million euro, for breaching rules regarding GDPR (General Data Protection Regulation) [2]. If companies break the rules regarding GDPR (or other acknowledged frameworks), it can potentially lead to not only big economic consequences, but also a loss in reputation.

By creating a simple and efficient solution for companies to check how exposed they are to cyber threats or negligence of compliance to the frameworks, we can help them avoid these consequences.

Our contact is Tea Knudsen from Sopra Steria.

1.3 Project goals

It can be confusing for companies to know what sort of rules and frameworks they need to comply to. Companies that handle more sensitive data, needs to be even more careful and aware. SopraSteria want us to make a model so companies easily can measure how compliant they are to specific frameworks regarding cybersecurity and protection of personal data. This should be a three-way model. The first part should explain what information security laws the organization need to comply with in order to fulfill the framework requirements. Secondly, the model will rate the company in terms of how closely it follows the requirements. The last part will measure how mature the company is in this category.

The model will be customized based on what sector the company specializes in, as well as what kind of data the company handles. The model will also be based on high quality standards that have gained recognition both internationally and/or locally within Norway.

2 Scope

2.1 Subject area

Our thesis will encompass a wide range of subjects within the field of information security laws. Specifically, we will delve into various topics such as Standards and framework for maturity measurement.

- **Regulatory Compliance:**

- Our thesis will detail the laws and regulations that organizations must comply with based on their industry sector and the services provided.
- It will also provide an overview of compliance requirements to mitigate legal risks.

- **Compliance assessment:**

- Determining the extent to which the organization is meeting legal and regulatory requirements for information security.

- **Design and Implementation of Graphical User Interfaces:**

- Our goal is to design and implement a graphical user interface (GUI) using Power BI, which will aid organizations in identifying and assessing compliance with information security regulations and standards.

- The GUI will provide a user-friendly and intuitive interface for accessing and analyzing relevant data, enabling organizations to effectively evaluate their information security compliance.

2.2 Task description

Our objective is to develop a comprehensive, three-part model that will allow us to determine the laws and regulations that an organization should adhere to, based on the sector in which it operates and the services it provides. This model will then be utilized to assess and evaluate the level of compliance with these laws and regulations by the organization. Furthermore, this model will enable us to determine the level of information security maturity of the organization in various areas, providing a comprehensive and holistic view of the organization's compliance and security posture.

2.3 Limitations

The parameters of our project define the boundaries of our focus and the areas that will not be included in the project's scope. The project specifications have established a clear set of objectives for the final outcome and have also identified certain limitations that have been deemed necessary for optimizing the efficiency of the project. These limitations have been considered to ensure that the project is executed within the given time frame and resources, while still maintaining the desired level of quality and functionality.

Some of the limitations that have been identified include:

- **Frameworks and Standards for Information Security Compliance:**
We will utilize the IOS 27001 standard as our primary framework and reference for information security regulations and requirements.
- **Project sector coverage:**
The project will focus on a limited scope of sectors, specifically two to three sectors, out of the numerous sectors in which companies operate. The following sectors were chosen as primary sectors:
 - **The Healthcare sector**
 - **The Information security sector**Also, if we have enough time, we can use the following sector (secondary sector):
 - **The financial services sector**
- **GUI Design and Implementation:**
-During the course of development and implementation of the graphical user interface (GUI), our primary focus will be on utilizing Power BI. Additionally, for the purpose of database management, we will utilize either SQL or Excel as the underlying table structure.

3 Project organization

3.1 Roles

- **Project leader:** Sondre Bakke
- **Minute Leader:** Jonas Simonsen
- **Log Leader:** Murad Dimen

3.2 Role responsibility

3.2.1 Project leader

Project leader is the leader of the group. If a group member fails to fulfill the agreement, the project leader will be in contact with the student supervisor for eventual sanctions, as well as decision maker if the group members get in an argument and can't find common ground.

3.2.2 Minute Leader

Minute Leader is responsible for taking notes with the student supervisor as well as potential meetings with the customer/client. Those notes should be available each Monday so the student supervisor can read the progress made each week. Will also be responsible for maintaining the hour log if necessary in the project.

3.2.3 Log Leader

Log Leader is responsible for controlling the backup either for the software/GUI that is to be made, the report or other related documents. He is also responsible to periodically make local saved backups alongside what is stored either in Teams, Overleaf or Git.

3.3 Workflow

3.3.1 Communication

For communication within the group we have created a Discord server that all group members have joined. We also have a Microsoft teams channel for communication with the student supervisor. We also communicate with Sopra Steria through mail, but also Teams when it is necessary to have meetings.

3.3.2 Meetings

- Monday 10:00-12:00 Progress meeting
- Tuesday 14:00-1430 With student supervisor
- Tuesday before and/or after meeting with student supervisor to plan work ahead.
- Thursday 10:00-12:00 Progress meeting

If meetings outside of the mandatory ones are needed they will be planned through the official Teams communication channel.

3.3.3 Method

The method will generally it will be in a individual manner, but if a person is stuck or needs collaboration with other group members, they will work together either in a team meeting or schedule when they can collaborate.

3.3.4 Collaborative tools

- Discord/Teams for communication
- Latex through Overleaf for documents that will be delivered
- Git through GitHub for version control and collaboration with the coding of the software.

3.4 Sanctions

If a group member either doesn't do enough to satisfy the contract, fails to do substantial work or does not meet during mandatory team meetings sanctions might occur.

We will work with a warning system where after 5 warnings, the student supervisor will get involved to find a solution. Potential solution might be to kick the team member out of the group.

4 Planning and reporting

4.1 Main Project Section

4.1.1 Development model

There are several different development models that can be used in order to complete the thesis in a successful manner. First we thought about using the waterfall model, but after some consideration we realized we will most likely have to complete different tasks at the same time, which makes the waterfall model a bit too strict. We would like to have some more flexibility to our development model.

Kanban is another popular model. It is known for being simple, but also efficient. We did however find it a bit too unstructured for developing our thesis. One of the reason is because structured time frames are not common in Kanban.

Scrum is also a well-known development model which we considered, but we do not have much experience with this model. We found it too risky to start using this model for our thesis, because it requires some experience to use properly and we are a smaller team where transparency is easy to achieve naturally.

In the end we decided to go for an incremental development model. This model makes it easy for us to organize the different tasks and sub-tasks within different modules. We will then split the sub-tasks of the modules, and work with them in iterations. We also found it advantageous to be able to work with our model and thesis in a parallel development, instead of having to fully complete our model before we can write the thesis.

4.1.2 Methods and Approach

To develop our model and technically complete all requirements we have decided to use a combination of Node.JS and Power BI. Power BI enables us to manage and display data in our model in a structured and efficient way. It also makes it easier to scale and manage our model, and make it usable within different sectors and companies. It also enables us to update the model in real time so companies easily can monitor differences before and after they have applied security measures. Another advantage with Power BI is that it does not require a lot of programming knowledge, so it can be easier for companies to manage, modify and use the program.

4.2 Flowchart

This is our flowchart of how the Three-Way Model will operate:

1- Initial phase: The model will present the relevant laws and regulations that apply to companies operating in various sectors. The user will then answer a set of general questions pertaining to their company's security setup.

2- Sector selection: The model will present a list of sectors for the user to choose from. The user will select the sector that best represents their company.

3- Results calculation and presentation: Based on the answers provided in the first and second phases, the model will calculate the security maturity of the company and present the results.

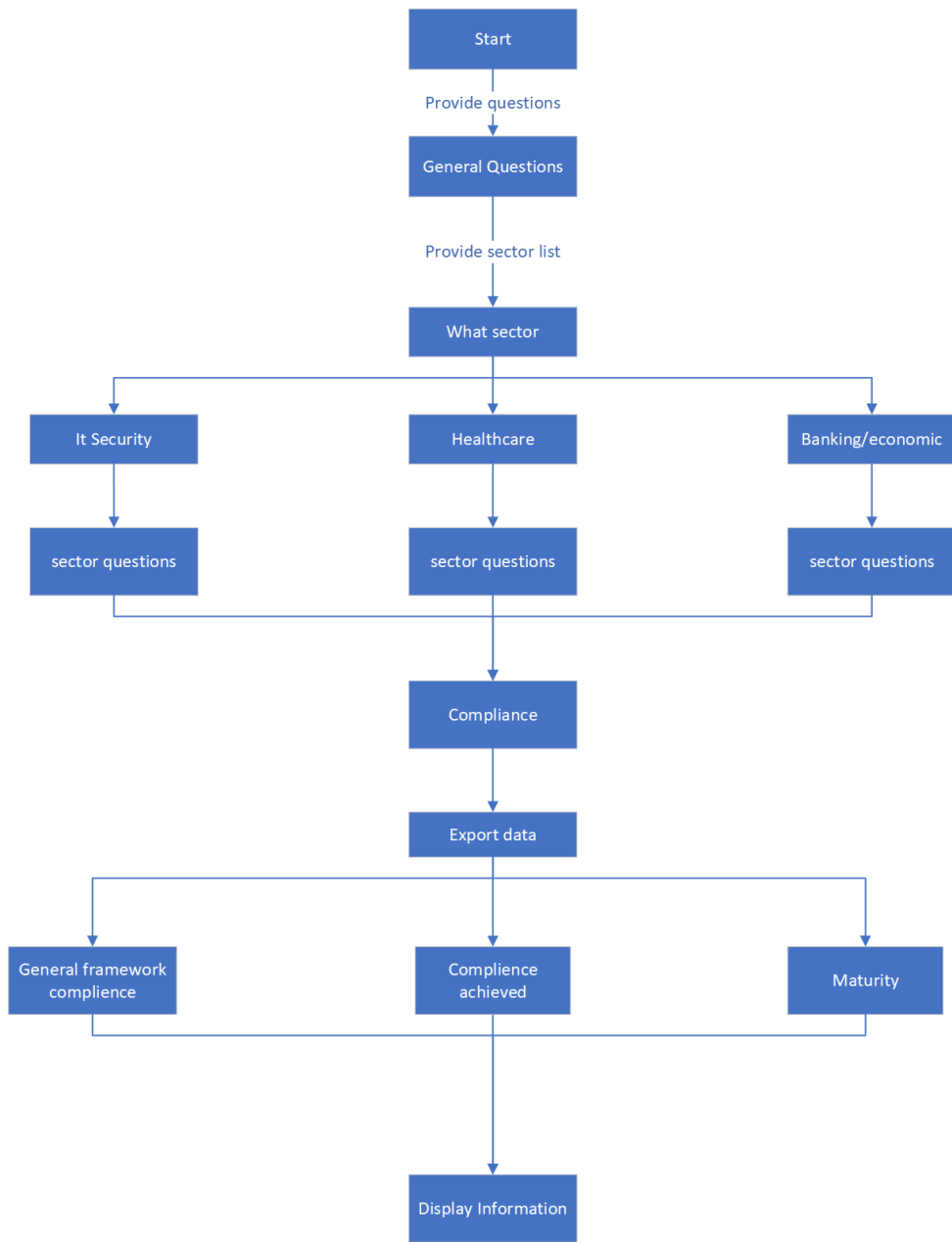


Figure 1: flowchart

4.3 Status Meetings and Decision Points

Each Tuesday at 14:00 or 2:PM we have a meeting scheduled with our student supervisor, where updates regarding the progress we have made on the project will be submitted. We will also have regular meetings within the group at least three times a week, but we are flexible to change this if we see that we have to meet more frequently or have longer meetings than usual. Our meetings will be on Mondays, Tuesdays and Thursdays.

5 Quality control

5.1 Documentation, Standards and Source Code

5.1.1 Documentation

All theoretical information that is being used in the project report requires proper citation of sources so both team members and readers can verify the information and make sure the project isn't plagiarised.

5.1.2 Standards

- Report-Latex
- Code - JavaScript/Node.js
- Data visualisation- Potentially PowerBI as used by the company

5.2 Configuration Management

5.3 Risk Analysis:

Some risks that can be found with description describing the severity of events.

Type: Administrative

Risk: Group member becomes ill

Consequence: Low/Medium

Probability:High

Description:Group member becomes ill and is unable to attend weekly meetings. Depending on severity of illness consequence of it may increase

Mitigation strategy: Depending on length and severity of the illness, group members might need to rearrange the work planned for the period the team member is ill. With an extended period of a person becoming ill, contact with supervisor will be established to figure out a solution.

Type: Administrative

Risk: Student supervisor becomes ill

Consequence: Low

Probability:Low

Description: Student supervisor becomes ill and can't participate in a weekly meeting with the group.

Mitigation strategy: Potentially reschedule meetings.

Type: Data

Risk: Data loss

Consequence: High

Probability: Low

Description: All stored data will disappear due to complete server shut down.

Mitigation strategy: Should be prevented by regularly taking backups and keeping the report and software stored in one or multiple clouds.

Type: Project

Risk: Delivery not ready by deadline

Consequence: Severe

Probability: Low

Description: Project isn't ready to be delivered by either deadline.

Mitigation strategy: Good communication within the group with regular meetings to make sure group is on track towards the goal.

Type: Program

Risk: Functionality doesn't match specification given to the team by the business

Consequence: High

Probability: Low

Description: The GUI the team develops doesn't match the standards set up by the business and becomes unusable

Mitigation strategy: Regular progress meetings with the business as well as quality control within the group to maintain high quality of the program

6 Project plan

6.1 Work breakdown structure

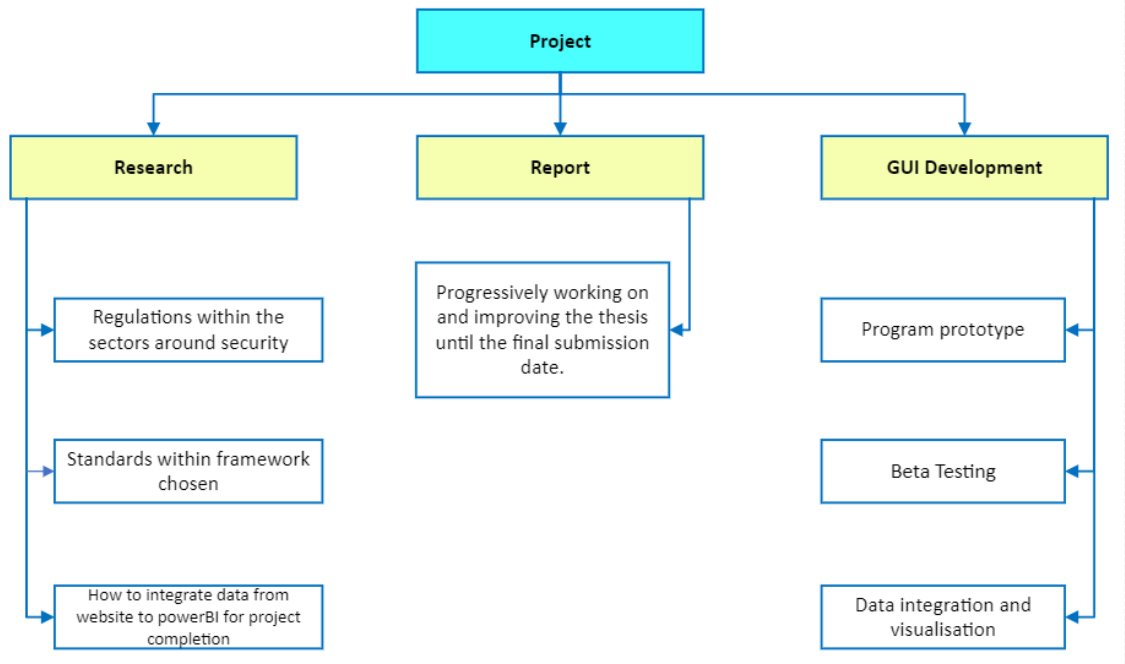


Figure 2: Work Breakdown Structure

6.2 Gantt chart

The accompanying illustration depicts a Gantt chart outlining the projected schedule for the project:

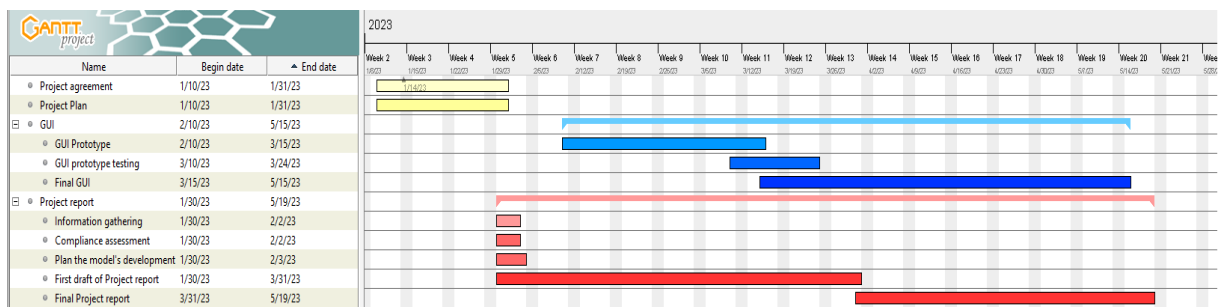


Figure 3: Gantt Chart

6.2.1 Deliveries

The following list presents the scheduled dates of delivery for various project documents:

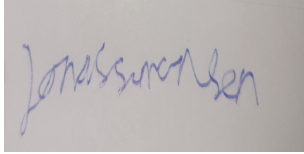
- Project agreement January 31.
- Project Plan January 31.
- First draft of Project report March 31.
- Project report May 22.

7 Confirmation

I have read the project plan and agree with its content.

Jonas Simonsen

Date and Signature: 23. 1. 2023



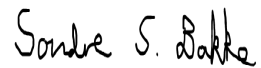
Murad Dimen

Date and Signature: 23. 1. 2023



Sondre Bakke

Date and Signature: 23. 1. 2023



References

- [1] Trautman, L. J., Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *Am. UL Rev.*, 66, 1231. (link: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/aulr66div=38id=p>)
- [2] Tambou, O. (2019). Lessons from the First Post-GDPR Fines of the CNIL against Google LLC. *Eur. Data Prot. L. Rev.*, 5, 80.

Appendix C

Project Task

Forslag til bacheloroppgave NTNU

System for oversikt over relevante informasjonssikkerhetslover i ulike sektorer og tjenesteleveranser og måling av modenhet på cybersikkerhet

Den stadig økende digitaliseringen gjør at IT-systemer blir en stadig viktigere del av organisasjoners leveringsevne og i mange tilfeller regnes IT-systemer som forretningskritisk. For å gjennomføre organisasjonens oppdrag er det derfor viktigere enn noen gang at IT-systemene er tilstrekkelig sikret mot angrep og uplanlagte utfall.

I Norge tilhører organisasjoner en eller flere sektorer, som ofte krever at organisasjonen må etterleve lover og regler for å kunne levere tjenester. Eksempelvis må helseorganisasjoner etterleve Normen for informasjonssikkerhet, organisasjoner som behandler personopplysninger må etterleve personopplysningsloven, og så videre.

Oppgaven går ut på å lage en tredelt modell. Den første delen skal besvare hvilke informasjonssikkerhetslover og -regler en organisasjon må etterleve basert på hvilken sektor de tilhører, og hvilke tjenester de leverer. Deretter skal modellen kunne måle organisasjonens grad av etterlevelse av disse lovene og reglene. Til slutt skal modellen kunne brukes til å måle organisasjonens modenhet når det kommer til ulike områder innenfor informasjonssikkerhet. Studenten står fritt til å velge standard/rammeverk for modenhetsmåling, men bør ta utgangspunkt i kjente standarder som ISO27001, NIST Cybersecurity Framework, NSM sine grunnprinsipper for IKT-sikkerhet v 2.0, eller lignende.

Modellen bør være funksjonell og kunne testes. Det er ingen krav til teknologibruk, utover at det er fordelaktig å bruke teknologi som anses som lett tilgjengelig. I tillegg bør modellen etterstrebe å ha et GUI som gjør det enkelt for brukere å benytte seg av modellen. Modellen bør også inneholde forklarende tekst der det er hensiktsmessig.

Kontaktpersoner:

Tea Knudsen – tea.knudsen@soprasteria.com

Erik Øyan – erik.oyan@soprasteria.com

Appendix D

Log

Log

In keywords

Week 3

- Gantt chart- may need to go in more detail
- Questions to the business about requirements, functionality, and so on. Should it be web based? Non-core based functionality like usability and user friendliness.
- Evaluation based on fulfilled requirements from the company.
- Presentation of bachelor to be public?

Week 4

- Functional requirements more in depth
- More in detail on how we will implement.
- More contact with Sopra Steira.
- How do users get questions, dynamic or static?
- Flowchart about how the model will work.
- Authentication? Azura or Private/own Database

Week5:

- Start designing application
- Starting the implementing the interface
- How will store the user answers?! JSON/Database

Week6:

- Start implementing the functionality, Use JavaScript
- Find the right tool to demonstrate the results

Week 7:

- Improve the style and make the font bigger!
- Improve the description text in the webpages.

Week8:

- Resize the chats to be more readable

Week 9

- Short meeting
- Skyhigh contact to establish cloud resources.

Week 12

- Add question number before each question
- Number of questions before the test
- Survey results might need to be clearer- be clearer with who you can compare with
- Clearer on what files are compared.
- More explanation for the interface overall.
- Form to be able to contact people within relevant fields

Week 13

- Openstack account verified
- Still clearer interface
- More communication with Sopra Steria
- Fix so it can run from dedicated database server

Week 14

- Easter break- week off

Week 15:

- Fix backend, establish what tools to use and why
- Gained public ip address for external testers
- Correct the draft feedback from supervisor.
- on the healthcare questions, we do not mention anything about which laws apply to which questions, thus we do not answer what the task asks about by saying which laws they must follow. On the finance section, it must not say "policies for Health" first, it can say "The statements are from the regulations on the use of information and communication technology by the Norwegian Ministry of Finance. Check the ticker which is appropriate for your company". It can also read ICT = Information and communications technology
- in addition, there should be the sign § in front of the numbers on all the questions, not just some
- In addition, all the links to the various laws should be under the description of healthcare

Week 17:

- Make overview of compliances
- Explain ISO better
- Add percentage degree on the charts
- Change to display results for legal questionnaire to "display compliance to legal regulations"
- Change questionnaire to "General questions from ISO27001"
- (perhaps write a little more in the text about exactly what ISO27001 is)
- Display your questionnaire results --> Display results from the general questions

- (Write that this is to get a maturity rating so that it is clear in relation to the assignment we have from sopra steria)
- Compare your questionnaire results---> Compare results
- (If you could get a line or something between legal regulations and questionnaire, it would become more clear that were different parts, that would also have been nice)
- also change about to CyberTest4You

Week 18:

- Create user forms
- User testing
- Improve the style and the text in the pages

Week 19

- Continue writing, some parts lack information

Week 20

- Finishing the report
- Fix formatting, some figures and paragraphs are out of sync



 **NTNU**

Norwegian University of
Science and Technology