A Solution to Selecting Cyber-Security Software Tools for an Organization Using Security Controls

ALEXANDRE MARCOS CONCA
A SOLUTION FOR SELECTING CYBER-SECURITY SOFTWARE TOOLS FOR AN ORGANIZATION USING SECURITY CONTROLS

Author: Alexandre Marcos Conca

Supervisor: Margus Välja

Examiner: Mathias Ekstedt

A thesis submitted in fulfilment of the requirements for the Master of Science Thesis in the Department of Electric Power and Energy Systems

March 2017
“Everyone faces challenges in life. It’s a matter of how you learn to overcome them and using them to your advantage.”

Celestine Chua
Abstract

School of Electrical Engineering
Electric Power and Energy Systems

Master of Science

A SOLUTION FOR SELECTING CYBER-SECURITY SOFTWARE TOOLS FOR AN ORGANIZATION USING SECURITY CONTROLS

In the last decade, cyber-threats have evolved dramatically, forcing organizations year after year to use increasingly sophisticated security measures, security software among others. This has led to a huge increase in the number of security tools available in the industry. The result of the increase is that that companies often do not know in which software to invest in order to meet their security needs. The purpose of this thesis is to address this problem by developing a solution that helps companies to choose the right security software based on their security needs and that allows to do the selection process in a systematic and reliable way.

The solution proposed in the thesis builds on interviews with experts in information security, data collection from the literature and Internet and on a case study. The solution consists of firstly an investigate method with which it is possible to categorize any security tool according to the list of cyber-security controls proposed by CIS Critical Security Controls (CSC), which were chosen after a comparative study with other publicly available controls because they are actionable, relevant and updated frequently. Secondly, the solution proposes a user-friendly web tool that has been developed to allow the users to visualize the collected information for comparison. The visualization tool will help the users to select the security tools in which the company could be interested to invest in. The visualization is done in a simple way and the CSCs that would be covered are shown together with the gaps and the overlaps of the selected tools. In order to verify the viability of the solution that was developed with real data, the project includes a case study with a representative set of security tools. The case study facilitates the comprehension of the process undertaken and shows how this method could be applied in a real case scenario.

Keywords: Information Security, Critical Security Controls, Investigative Method, Security Tools, Web Tool.
Sammanfattning

Skolan för Elektro och Systemteknik
Elkraftteknik

EN LÖSNING TILL VAL AV CYBER SÄKERHETSMJUKVARA VERKTYG FÖR EN ORGANISATION MED SÄKERHETSKONTROLLER

Under det senaste decenniet har cyberhot utvecklats dramatiskt. Hotet tvingar organisationer att år efter år använda allt mer sofistikerade säkerhetsåtgärder, bland annat säkerhetsmjukvara. Detta har lett till en enorm ökning av antalet av säkerhetsverktyg som finns i branschen. Resultatet av ökningen är att företag ofta inte vet i vilken programvara de borde investeras i för att möta sina säkerhetsbehov. Syftet med denna rapporten är att ta itu med detta problem genom att utveckla en lösning som hjälper företag att välja rätt säkerhetsprogramvara baserat på deras säkerhetsbehov och som gör urvalsprocessen på ett systematiskt och tillförlitligt sätt.

Den lösning som föreslås i rapporten bygger på intervjuer med experter inom informationsäkerhet, datainsamling från litteraturen och Internet och på en fallstudie. Läsningen består först av en utredningsmetod med vilken det är möjligt att kategorisera vilket säkerhetsverktyg som helst enligt listan över cybersäkerhetskontroller som publiceras av CIS Critical Security Controls (CSC). CSC valdes efter en jämförande studie som inkluderade andra allmänt tillgängliga förteckningar över kontrollerna, eftersom CSC kontroller är genomförbara, relevanta och uppdateras ofta. För det andra föreslår lösningen ett användarvänligt webbverktyg som har utvecklats för att göra det möjligt för användare att visualisera den insamlade informationen för jämförelse. Visualiseringsverktyget kommer att hjälpa användarna välja säkerhetsverktyg som företaget kan vara intresserade av att investera i. Visualiseringen sker på ett enkelt sätt och CSCs som omfattas visas tillsammans med de luckor och överlappningar som finns i den valda programvaran.

För att bekräfta genomförbarhet för den lösning som utvecklats med verkliga data, omfattar projektet en fallstudie med ett representativt urval av säkerhetsverktyg. Fallstudien underlättar förståelsen för klassificeringen och urvalsprocessen genom att visa hur denna metod skulle kunna tillämpas i ett verkligt fall.

Nyckelord: Informationssäkerhet, Kritiska Säkerhetskontroller, Undersökanste Metod, Säkerhetsverktyg, Webbverktyg.
Acknowledgements

This project consumed huge amount of work, research and dedication. Still, implementation would not have been possible if I did not have a support of many people. Therefore I would like to extend my sincere gratitude to all of them.

First, I would like to express my gratitude to my Master Thesis Supervisor, Margus Välja, for taking the time, effort and patience to provide me with his invaluable guidance, comments and encouragement to complete this project. His extensive discussions and knowledge around this work have been very helpful for this study.

I am also grateful to my friends and all the people I have met in this wonderful city called Stockholm. During this time I have had the opportunity to understand better than ever that a place is only as good as the people you know in it. I would like to make a special mention to my buddies Juan and Fer. Your humor and support in the last months has been essential for me. This has been just the beginning of a great friendship.

Of course, I would like to express my sincere thanks towards Blancalux for her great help both with the project and her incredible motivation in every single difficult moment in which I thought I could not continue. Without you, everything would have been much harder. Thank you for your simplicity and for being such as you are.

Last but not least, I express my deepest gratitude toward my parents and sister. Without you, I would not have lived this amazing experience as a student during 25 years. You were with me when my studies started and you continue with me now that they are over. This report symbolizes the end of my studies and is dedicated to you. Lo conseguimos.
Contents

Abstract ii

Sammanfattning iii

Acknowledgements iv

Contents v

List of Figures viii

List of Tables ix

Abbreviations x

1 Introduction 1
  1.1 Background ......................................................... 1
  1.2 Problem Definition ............................................... 3
  1.3 Purpose, Scope and Goals ........................................ 4

2 Methodology 6
  2.1 Introduction ....................................................... 6
  2.2 Procedure ........................................................ 6
  2.3 Data Collection ................................................... 11
  2.4 Interview .......................................................... 12
    2.4.1 Participants .................................................. 13

3 Literature Review 14
  3.1 Introduction ..................................................... 14
  3.2 Information Security in a Company ............................ 14
  3.3 Information security guides .................................... 17
    3.3.1 ISO 27001 and 27002 ....................................... 19
    3.3.2 NIST Special Publication 800-53 .......................... 20
    3.3.3 The CIS Critical Security Controls for Effective Cyber Defense ... 22
  3.4 Security Tools .................................................... 24
  3.5 Method theory .................................................... 25
    3.5.1 Qualitative investigation ................................ 25
    3.5.2 Quantitative investigation ................................ 25
Contents

G  Survey Template 2 Investigative Method, Open-ended questions 89
# List of Figures

1.1 Information security spending worldwide from 2011 to 2016. . . . . . . . . 2  
2.1 Diagram of the procedure . . . . . . . . . . . . . . . . . . . . . . . . . . 7  
5.1 Method diagram . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35  
5.2 Relations between the security tools analyzed by the method and the  
CSCs covered by them . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42  
5.3 Data model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43  
5.4 Matrix to relate security tools and Critical Security Controls . . . . . . 44  
5.5 Case of security situation through matrix . . . . . . . . . . . . . . . . . . 45  
5.6 Relation between the different entities . . . . . . . . . . . . . . . . . . . 46  
5.7 Selection of security tools in the developed tool . . . . . . . . . . . . . . . 46  
5.8 Warming in the developed tool . . . . . . . . . . . . . . . . . . . . . . . . 47  
5.9 Matrix showing the security situation of the selected company in the  
developed tool . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47  
5.10 Gaps and overlaps of the selected company in the developed tool . . . . 48  
5.11 Data stored on the basis of the data model. . . . . . . . . . . . . . . . . . 50  
5.12 Filtering based on a Critical Security Control. . . . . . . . . . . . . . . . 51  
5.13 Filtering based on a security tool. . . . . . . . . . . . . . . . . . . . . . . 51  
5.14 Example of providers with different products. . . . . . . . . . . . . . . . 52  
5.15 Parameters of a security tool. . . . . . . . . . . . . . . . . . . . . . . . . 52  
5.16 Security tools selected. . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53  
5.17 Matrix with the first security tools set. . . . . . . . . . . . . . . . . . . . 54  
5.18 Matrix with the second security tools set. . . . . . . . . . . . . . . . . . . 54  
5.19 Gaps and overlaps of the second security tools set. . . . . . . . . . . . . 55  
D.1 Flowchart of the method draft. . . . . . . . . . . . . . . . . . . . . . . . . 82
# List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Participants of the interviews</td>
<td>13</td>
</tr>
<tr>
<td>3.1</td>
<td>Percentage main security threats according Organizational Insiders and Information security professionals.</td>
<td>16</td>
</tr>
<tr>
<td>3.2</td>
<td>Percentage of threat vulnerability themes according Organizational Insiders and Information Security Professionals.</td>
<td>16</td>
</tr>
<tr>
<td>3.3</td>
<td>The most commonly used security guides and their classification.</td>
<td>18</td>
</tr>
<tr>
<td>3.4</td>
<td>Control Areas and their number of controls (ISO/IEC 27002:2013)</td>
<td>20</td>
</tr>
<tr>
<td>3.5</td>
<td>Families, their identifier and their number of controls (NIST SP 800-53 Rev.4)</td>
<td>21</td>
</tr>
<tr>
<td>3.6</td>
<td>Critical Security Controls and their effects on attack mitigation.</td>
<td>23</td>
</tr>
<tr>
<td>4.1</td>
<td>Number of security tools collected by each CSC</td>
<td>28</td>
</tr>
<tr>
<td>5.1</td>
<td>Advantages and disadvantages of the main frameworks and standards</td>
<td>33</td>
</tr>
<tr>
<td>5.2</td>
<td>Required parameters of each Security Tool</td>
<td>42</td>
</tr>
<tr>
<td>D.1</td>
<td>Questions about the Critical Security Controls 1/4</td>
<td>78</td>
</tr>
<tr>
<td>D.2</td>
<td>Questions about the Critical Security Controls 2/4</td>
<td>79</td>
</tr>
<tr>
<td>D.3</td>
<td>Questions about the Critical Security Controls 3/4</td>
<td>80</td>
</tr>
<tr>
<td>D.4</td>
<td>Questions about the Critical Security Controls 4/4</td>
<td>81</td>
</tr>
<tr>
<td>E.1</td>
<td>Representative set of security tools</td>
<td>85</td>
</tr>
<tr>
<td>F.1</td>
<td>Questions about the security tool 1/3</td>
<td>86</td>
</tr>
<tr>
<td>F.2</td>
<td>Questions about the security tool 2/3</td>
<td>87</td>
</tr>
<tr>
<td>F.3</td>
<td>Questions about the security tool 3/3</td>
<td>88</td>
</tr>
<tr>
<td>G.1</td>
<td>Question(s) about the hypothesis(es)</td>
<td>89</td>
</tr>
</tbody>
</table>
Abbreviations

DDoS    Distributed Denial-of-Service
IoT     Internet of Things
CaaS    Crime as a Service
APT     Advance Persistent Threat
CVE     Common Vulnerability and Exposures
ICS     Information and Communication and Systems
ISMS    Information Security Management Systems
ISO     International Organization for Standardization
IEC     International Electrotechnical Commission
BSI     British Standards Institution
NIST    National Institute of Standards and Technology
SP      Special Publication
FIPS    Federal Standard of Processing of Information
CSC     Critical Security Control
CIS     Center for Internet Security
CVE     Common Vulnerability and Exposures
CVE     Common Vulnerability and Exposures
ROI     Return On and Investment
SPA     Single-Page Application
Chapter 1

Introduction

1.1 Background

According to the ISO 27000:2016, information security is the preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [1]. Organizations invest in information primarily to protect information assets of the cyber risks that endanger the processing, storage and transport of these assets by information systems that are interconnected. This group of cyber-risks includes: traditional malwares (viruses, trojans, spyware, adware, etc.), standard phishing attacks, standard distributed denial of service (DDoS) attacks, manipulated hardware and firmware, the usage of stolen certifications, advanced persistent threats (APTs)³, etc.

Over the years, threats and cyber risks have evolved. The creation of new business models, moving within a few years from hacker who operated individually, or in small communities, to business model referred to as Crime-as-a-Service (CaaS) [3]. The CaaS model has allowed cyber-criminals to work more effectively, sharing the techniques of attack, tools and objectives, making easier the way such attacks are conducted and therefore improving their success rate[4].

This has led organizations to use methodologies, techniques, security tools, organizational structures, technology and other elements more and more sophisticated to reducing emerging risks to an acceptable level, mitigating the latent threats. This explains why according to recent estimates [5], the worldwide information security market grew from $3.5 to $77 billion between 2004 and 2015, and it is forecasted to reach $170 billion by 2020. Information security spending worldwide has not stopped to increase in the last years, as shown in Figure D.1.

However, most organizations do not view their information security investment decisions in the same way that they view other investment decision. This is due to:

---

¹Knowledge or data that have value for an organization, ISO 27001.
²They cover the applications, services, information technology assets or other components that allow the handling of it, ISO 27001.
³Advanced Persistent Threats (APTs) are a cyber-crime category directed at business and political targets. APTs require a high degree of stealth over a prolonged duration of operation in order to be successful[2].
Firstly, the investment in security information is something abstract, and it is not easy to make a financial analysis as it is not possible to calculate the amortization of the investment due to organizations do not know their future attacks. From the perspective of a business, "security is an investment to be measured in dollars saved as a result of reduced losses from security breaches, or in profits from new ventures that would be too risky to undertake without investments in security" (Schechter, 2004) [6].

Secondly, information security term is something abstract itself. In this field it is not possible to say that something is secure, since always new ways of attacking can come up. Security is a concept associated with certainty or lack of risk and it should be clarified that absolute certainty is not possible. Therefore, it can never be guaranteed that with a correct investment in information security an organization may be considered completely secure, but it may be more or less acceptably secure.

In short, information security is an uncertain and complex field. That is why there are information security guides (standards, frameworks, etc.), such as ISO 27001, NIST 800-53 or CIS 20 CSCs, whose target is to help organizations to protect their information assets. Although all the guides have the same final goal, they are different, since they are oriented of different way. Some are updated more frequently than others, some have a technical background and others are more specific to business managers, etc. In short, there is no one better than others, but they depend on the objectives of each organization.

Some of the guides propose a finite list of security controls, which indicates any type of control (preventive, detective or corrective) that a company may need to comply to avoid known threats. Obviously, this list is a reference for companies. Each company has a size and requirements. Some companies have to take measures to comply with all the proposed controls and others only need to take measures for part of the controls.
However, despite the existence of these guides, with even lists of well-defined security controls, sometimes, organizations do not know what remedies or measures to establish to comply with controls. This happens for example, and mainly, with the software, with the security tools. In these cases, the problem is not that organizations do not know which controls should be covered, but that they do not know exactly what security tools are adequate to comply with these controls. Either because the vendors of software tools do not indicate it clearly, or because of naming problems.

This often means that business managers do not know which security tools to invest and end up investing inadequately.

1.2 Problem Definition

As it has been introduced in the previous section, it is often difficult for companies to choose which security tools are appropriate for the company to become acceptably secure, even in the case that the company knows which are its security need requirements. This is due to the fact that many times, the organizations only have as source to know the features of the security tools, the information stated by the security tools vendors themselves. Unfortunately, these features stated by the vendors are often exaggerated, or partially defined, for marketing reasons. In addition, there is usually no standardized way of referring to the features of security tools. As a result, users who are not experts in information security may have doubts about which security controls are covered by a security tool, even though their characteristics are well specified.

This situation is not a problem for large companies, which have experts in information security that can do an efficient investigation of the possible security tools to determine which are the most suitable for the needs of the company. However, most companies do not have the resources (budget, time, etc.) needed to carry out this kind of investigation. Therefore, they only have the choice of trusting in the stated by software vendors or, as much, to trust in the security tools reviews done by other users that may be even less reliable.

On the other hand, as mentioned, information security is complex and abstract and is usually difficult be understood by business managers, who often ask themselves questions such as Why should I buy additional software or replace it? What did I get for my money and how does it serve to protect information assets? Why are there still security breaches?

This is another problem, even though security experts can know what software the company needs to become secure, the investment is made by business managers and they should be able to understand it too. Therefore, it is necessary that the software requirements of the company can be communicated to the business managers in a clear and simple way. It would even be advisable to communicate on to the rest of the company’s employees, since the greater the understanding of information security by employees, the greater the chance of avoiding security breaches.
1.3 Purpose, Scope and Goals

The purpose of this thesis is to propose a solution to the problem raised in the previous section. That is to say, to develop a solution that helps companies to choose, in the most rigorous possible way, the necessary software to cover the security controls that the company requires, in a clear and simple way. The goal of this is that companies can deploy the software necessary to become acceptably secure. In order to comply with this proposal, a series of concise and measurable goals have been established, on which the thesis is based:

(i) Analyze the different information security guides to choose a list of security controls that includes all the control requirements that an organization may need to cover. The list of security controls must meet these requirements:
   - Well defined and actionable - not ambiguous
   - Relevant to the industry
   - Updated Frequently

(ii) Develop a method which allows to categorize objectively any security tool based on the list of security controls mentioned in the previous goal.

(iii) To design a data model for organizing and storing the elements obtained in the previous method in a way that it is easy to access them.

(iv) From the above goals, develop a ubiquitous, user-friendly and simple visualization tool that helps companies choose, based on their needs, the adequate security tools in a clear way.

(v) Do a case study where a representative set of security tools is classified according to part of the method and to show some examples of how the information is stored and how the developed tool works.

Regarding the scope of this thesis, it is limited to the limitations described below, what the thesis covers and what not:

- As indicated above, a company can not be secure. Only some level of security is achievable. Therefore, this thesis is limited to helping companies to become acceptably secure from the software perspective, based on all the problems known so far.

- The information security guides propose solutions more holistic than the security controls, like the Information Security Management Systems (ISMS). However, the objective of this thesis is to establish a clear and concise list of controls that are actionable, therefore the research is limited to what is related to security controls.

- The information security guides propose security controls that, in turn, group sub-controls, making a total of hundreds of sub-controls. The goals of this thesis are focused on the controls, without going into the details of their sub-controls. The further research of the sub-controls is one of the proposals for future tasks.
• Companies are different, have different business processes and technical needs. Because of this variety, they have different needs for security controls. In this thesis is not specified a list of security controls for each kind of organization, but it is defined a general list of security controls that addresses all the known security issues. Each company will have to use the list according to its needs.

• One of the goals of the thesis is to create a rigorous method for categorizing any security tool. Subsequently, a case study is proposed, as other of the goals, where a set of security tools is classified according to this method. However, the method created requires an evaluation part which to carry it out would require surpass the scope of this project. Therefore, the evaluation part of the method has not been performed in the case study.
Chapter 2

Methodology

2.1 Introduction

This chapter explains what has been done throughout the whole project as well as the refinements that have been made as the project has progressed. It shows the relationship of all the chapters and the reasons of the decisions taken. In Section 2.2, Procedure, all the phases that have been carried out in the project are linked to the concrete goals introduced in Chapter 1, explaining what has been done, the variables that have been involved in the study and the deliverables of each phase. In Section 2.3, Data Collection, it is explained how the data has been researched, gathered and used. Finally, in Section 2.4, Interview, the interview carried out in this project is described as well as the participants to whom it has been conducted.

2.2 Procedure

The purpose of this thesis is to develop a solution that helps companies to choose, in the most objective way, the necessary software, i.e. the security tools, to cover the security controls that the company requires. In addition, the solution must be clear and simple, so that the solution can also be understood by users not experts in information security, such as business managers or any employee of an organization.

In order to carry out the purpose, a process has been followed which can be divided into 4 phases, corresponding to each of the first 4 goals established in Section 1.3. Below, the steps followed in each of the phases to obtain the deliverables are explained. The resulting deliverables are detailed in Chapter 5. It is important to note that each phase has been done after the previous one, so the order is important to understand the whole process, which has been summarized in Figure 2.1.
Phase 1: Security Controls Choice

This phase corresponds to the first goal:

*Analyze the different information security guides to choose a relevant, updated frequently and well-defined and actionable list of security controls that includes all the control requirements that an organization may need cover.*

**Figure 2.1:** Diagram of the procedure
As has been indicated, the final purpose of this thesis is to create a solution that allows the companies to choose the adequate software for they can become acceptably secure. It very important to note that this does not mean that with the choice of the right software the company will be either secure or acceptably secure. This means that the company will have the option of becoming acceptably secure as long as it also complies with other security measures that are not considered in this thesis.

For this, it has been firstly necessary to carry out a literature review on information security in companies, described in detail in Section 3.2. The reason has been to be able to define the current situation of security in organizations and to understand the reason why the information security guides help the companies to become acceptably secure. Once this has been defined, various information security guides (standards, frameworks, benchmarks, etc.) have been thoroughly investigated from the approach of security controls. Those best known and with security controls lists most suitable with the requirements of the thesis have been detailed in the literature review, Section 3.3. Based on all the information collected, the advantages and disadvantages of the lists of security controls have been compared and the most suitable has been chosen, the Critical Security Controls (CSCs). The list of security controls chosen, is the one that has been considered that companies should follow to become acceptably secure. Of course, not all organizations must comply with all controls since each organization has different business processes and technical needs. The comparative analysis of the guides and its deliverable are in the Analysis and Results Chapter, Section 5.2. With the objective of validating that the chosen list of security controls is indeed relevant for the companies, 4 interviews have been conducted to security experts of organizations. The data obtained in the interviews are reflected in Section 4.3.1. Finally, in the discussion and conclusion chapters, there is a discussion over how adequate the chosen security controls are to meet the proposed goal.

Phase 2: Development of the method

This phase corresponds to the second goal:

*Develop a rigorous method which allows to categorize any security tool based on the list of security controls mentioned in the previous goal.*

In the previous phase it has been produced a list of security controls that a company should cover partially or completely, according to their needs, to become acceptably secure. However, it is necessary to know when the company complies with the controls or not. This project is carried out from the perspective of helping the companies to choose the adequate security tools. Therefore, for this perspective, it is necessary to know when a security tool covers a security control or several security controls. However, the problem is that it is not known which security controls are covered by each security tool, at least it is not known in a reliable way. Therefore, it is necessary to create a rigorous method that allows to categorize any security tool according on the security controls it covers. The methodology followed to develop the investigative method has been:

(i) Literature review to find existing methods for software classification according to features.

(ii) Design the first draft method.

(iii) Conduct interviews to 4 cyber-security professionals to:
Methodology

Chapter 2.

(a) Find out the investigative process followed by their organizations to choose the security software based on their needs.

(b) Get feedback about the first draft method.

(iv) Design the final investigative method based on the information gathered and the experience gained conducting interviews.

(v) Use the method to classify 44 security tools to verify that it is usable.

The whole design of the investigative method is described in Section 5.3.

Phase 3: Storing of the data

This phase corresponds to the third goal:

To create a data model for organizing and storing the elements obtained in the previous method in a way that it is easy to access them.

In the previous phase it has been produced a method which allows to classify any security tool according to the security control(s) covered by it. It has been decided that the final result of the method, i.e. the mapping between the security tool and the security control(s) covered by it, is stored in MySQL. The reasons of using MySQL have been:

(i) Free to use

(ii) It has thorough documentation available

(iii) It is compatible with the visualization tool of the phase 4.

However, although the final result of applying the method is the relationship between the two mentioned variables, during the method relevant data are obtained, such as the features of the security tool, the software security provider, the references of the information obtained, etc. These data are very important and needed in the case that future investigators want to continue with the investigation or verify the stored result. That’s why, it has been developed a data model to organize the storage of all the data that can be obtained when applying the method. The data model is shown in Section 5.4.

Phase 4: Visualization tool development

This phase corresponds to the fourth goal:

From the above goals, develop a ubiquitous, user-friendly and simple visualization tool that helps companies pick up, based on their needs, the adequate security tools.

In the previous phase, a database instance has been created for storing mappings between security tools and CSCs. With this information, it is possible to develop a tool which allows the companies to choose the adequate software to comply with the security controls according to their needs. According to the requirements of the goal, the visualization tool has to be:

To develop the visualization tool the following steps have been followed based on the objective requirements:
(i) To meet the ubiquity requirement, a web tool has been developed using AngularJS since it allows that can be used from anywhere, without any requirement.

(ii) To meet the user-friendly requirement, the web tool has been designed to have only two sections. In one the user selects the security tools to analyze and in the other the final result appears.

(iii) To meet the simplicity requirement, the visualization tool has been designed so that the final result is represented by a simple matrix and a color legend.

The whole development of the web application is described in Section 5.5.

With the development of the 4 phases, the first 4 goals have been sought to be met and fulfill the purpose of the thesis. For this, in summary, firstly a set of security controls have been chosen. Secondly, a method has been created that allows to determine which of these controls are covered by any tool. Thirdly, a way to store the data has been chosen and a data model has been designed. And fourth, finally, a tool has been created which, with the use of all the previous steps, helps companies to choose the software they need to meet their security needs.

However, in order to be able to show the whole solution in a practical way, a case study has been carried out, which corresponds to a fifth phase, and to the fifth goal.

**Phase 5: Case study**

This phase corresponds to the fifth goal:

*Do a case study where a representative set of security tools is classified according to part of the method and show some practical examples of how the data are stored and how the developed tool works.*

In this phase, a set of security tools has been classified using the investigative method developed in phase 2. The method has been created to classify any security tool. Nevertheless, there are thousands of security tools and therefore, unfortunately, it is not possible to consider all of them in this collection. So, 44 security tools have been collected. Since the set of security tools has had to be quite small compared to the number of existing tools, it has been decided that the set at least is relevant, as the goal mentions. To achieve this, two guidelines have been followed:

- The set of security tools must be diverse, therefore, as many Critical Security Controls as possible must be covered. In this way, all cases that could occur in an company can be considered.
- The security tools from the set have to be widely used in the companies nowadays for avoiding use outdated tools or tools unknown by most companies. To get this the following has been done:
  - Conducting interviews with companies, asking questions about the security tools used in these companies and the security controls covered by them.
  - Searching information about the most used security tools in Gartner reports.
Once the security controls set has been chosen, which is shown in the Data chapter, Chapter 4, each cyber-security tool has been classified following the investigative method of phase 2. Unfortunately, the evaluation part of the method has not been carried out for the reasons explained in Discussion chapter.

The data that have been obtained when carrying out the investigative method have been stored in an orderly manner following the data model of phase 3. The data have been stored in the graph database Neo4j. Using this graph database is not a requirement of the thesis, but has been used for the author’s convenience. The final result of the method, the mapping between the 44 categorized tools and the security controls covered by them, has been stored in MySQL. This is a requirement of the thesis, since it is the only database compatible with the visualization tool developed.

Finally, some practical examples have been made using both Neo4j and the visualization tool developed to show them to the reader in Section 5.6.

2.3 Data Collection

This project has focused mainly on the development of a solution that allows to help any company to choose the adequate software to cover its needs to become acceptably secure. To this end, a thorough investigation and a great collection of data has been necessary. The research carried out has been of a qualitative type, since the goal of this research has been to obtain a deeper understanding possible of the topic to develop the project. The data collected have been of two types:

(i) Secondary data: This kind of data corresponds with the information reviewed and analyzed but that it has been written by other researchers. Although this data have not been obtained firsthand, all the information used has been referenced to demonstrate that reliable sources have always been used. This information has allowed:

- On the one hand, the review of the literature in Chapter 3. The reasons for collecting the information shown in the chapter of the literature review have been explained throughout Section 2.2. However, in order to clarify, the information collected in each of the sections is briefly explained again:
  - Firstly, information about the Information security in a company has been collected, which has allowed to determine what a company needs to be secure and how it can be achieved.
  - Secondly, the analysis of the various Security information guidance, has allowed to analyze in depth the most important information security guides and to obtain a list of adequate security controls for the requirements of this thesis.
  - Thirdly, information about Security tools has been searched, which has been necessary to identify them and to be able to determine what information should be extracted from them in order to categorize them.
  - Fourthly, a revision of the Method theory has been done, which has been fundamental to be able to create the method that allows to classify the security tools in function of the covered security controls.
Chapter 2. Methodology

- The compilation of a representative set of security tools, found in the Data Chapter, in Section 4.2. From reliable sources, mainly Gartner reports, the security tools widely used have been selected to cover as many security controls of the chosen list as possible. The target of this has been to use the collected security controls for their classification in the case study of Section 5.6.

(ii) Primary data: This kind of data corresponds with the information obtained firsthand through interviews with different users of companies. In these interviews it has been tried to obtain information about:

The questions asked in the interviews and the manner in which they were conducted are detailed in Subsection 2.4. The ideas obtained from the interviews are reflected in Section 4.3.1

2.4 Interview

As part of this project a series of interviews were conducted. Interviews were the main choice for obtaining primary data about the security situation of the companies. The interviews have been carried out to find out:

(i) If the Critical Security Controls are relevant for the companies. The target of this is to use this information to validate if the list of security control chosen, the Critical Security Controls, is relevant indeed.

(ii) Which are the security tools mostly used by companies to cover Critical Security Controls. The target of this is to use these data for the case study.

(iii) Which is the protocol, or the criteria, that the companies follow to choose the security tools according to their security needs. The target of this is to use this information for the developing of the method.

(iv) Which is their opinion of the first draft of the developed method. The target of this is to get a feedback from cyber-security professionals to improve the method.

It was tried to arrange interviews with around 20 companies, and it was ended interviewing only 4 companies, detailed in Subsection 2.4.1. The interview, attached in Appendix G, has been made in English and Spanish, depending on the nationality of the interviewee. It has always been done personally, either face to face or Skype.

In each one of the interviews, first, the 20 Critical Security Controls are explained or remembered. Then, there are 23 open-ended questions. In the first question is asked to the interviewee if he/she is familiar with the 20 CSCs. In the other 20 questions it is asked if the company covers each one of the CSCs, if they are relevant for their company and which security tools are used to cover each one, if they are used. It should be emphasized that it is not directly questioned by the CSC, but by its guidelines. That is, it is asked about what should be achieved with them. Should be added that the respondent is free to add any comments he/she deems relevant. After this, in question 22, it is asked which is the criteria followed by the company to choose the security tools according to the security needs of the organization. Finally, in the last question, it is
asked to analyze the first draft of the developed method, indicating what they would change and add.

2.4.1 Participants

In this section the respondents of the interview explained in the previous subsection are detailed. For reasons of privacy, and since it has no relevance, the name of the participants is not indicated, referring to them by means of an identifier. They are listed in Table 2.1, indicating the company to which they belong or have belonged, its corporate function and the pertinent observations, if any.

The interview was made to those people who meet the following criteria:

(i) Belong to a company with a size greater than 100 employees. Interviews have also been conducted for those who no longer belong to companies with these conditions, but have recently belonged to them.

(ii) Have a corporate function related to information security or know how the information security of their company is structured.

It should be added that interviews have been also conducted with people who do not know exactly how the information security of their company is structured, but they can give relevant information of other companies since they are auditors or consultants.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Company</th>
<th>Corporate function</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respondent A</td>
<td>MBA incorporado S.L.</td>
<td>Information System Director</td>
<td>The respondent is working with information security management and has CISSP certification</td>
</tr>
<tr>
<td>Respondent B</td>
<td>SKV Bygg &amp; VVS AB</td>
<td>Information Security specialist</td>
<td></td>
</tr>
<tr>
<td>Respondent C</td>
<td>Ernst &amp; Young AB</td>
<td>CISO</td>
<td>Was chosen as a candidate for their broad knowledge and background in information security</td>
</tr>
<tr>
<td>Respondent D</td>
<td>Business560, UAE</td>
<td>Consultant — Auditor</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3

Literature Review

3.1 Introduction

To carry out the development of this project an information seeking through the available literature of different useful and reliable sources has been done, such as articles, reports and books. This information has been analyzed based on the established objectives and the main ideas have been reflected in this chapter.

The chapter is divided in 4 sections. In the first section, Information Security in a Company, it is analyzed why the information security in companies is essential and how the information security guides help the companies to determine their security needs to become acceptably secure. In the next section, Information Security Guides, some lists of security controls of the most known standards and frameworks are analyzed. The goal is to obtain a security controls list suitable with the requirements of the goal established in Chapter 1, to help the companies to choose the adequate security tools to comply the controls as far as possible. That is why, given the importance of the software, in the third section, Security Tools, the possible properties of security tools have been analyzed as well as the types. Finally, another goal established in Chapter 1 is to develop a method that allows to classify any security tool in function of the security controls covered by it. Therefore, in the fourth section, Method Theory, all the information that has been needed to develop the method is reflected.

3.2 Information Security in a Company

Information Security is formally defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [7]. It encompasses people, processes, and technologies and it concentrates on how to protect:

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes, being a process a set of interrelated or interacting activities which transforms inputs into outputs [8].
**Integrity:** Property of accuracy and completeness, without unauthorized modification [8].

**Availability:** Property of being accessible and usable upon demand by an authorized entity [8].

No matter how large or small the company is, all the companies need a plan to ensure the security of their information assets. All businesses use information such as employee information, tax information, proprietary information, or customer information. Therefore, the value of an organization lies within its information. Its security is critical for business operations, as well as retaining credibility and earning the trust of clients. If that information is compromised in some way, the business may not be able to function. Then, the key asset and the value of any business is its data, its information [9]. Unfortunately, all information held and processed by an organization is subject to the risks of threat, error and natural disaster, and other vulnerabilities inherent to its use. The terms threat and vulnerability are defined below:

- According to the National Institute of Standards and Technology (NIST), a **threat** is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [10]. A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm.

- According also to the National Institute of Standards and Technology (NIST), a **vulnerability** is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat [10]. A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions [11]. The known threats are enumerated in Mitre Corporation’s Common Vulnerability and Exposures (CVE), a dictionary of publicly known information security vulnerabilities and exposures.

In the last years there has been a development of Information and Communication Systems (ICS) as well as a great proliferation of the use of broadband on the Internet. This, coupled with increased mobility and dispersion of users and employees, has led companies to adopt new business practices, increasing the communication intern (employees, offices, delegations, etc.) and external (clients, suppliers, media, public administration, etc.) by electronic means. All these factors mean the existence of a new reality for companies, which have to face new risks and threats, which did not exist a few years ago. Threats and risks such as computer fraud, espionage, sabotage, vandalism, fires, physical catastrophes, etc [12].

In addition to external risks, nowadays, one of the biggest cause of leaks of information is the ordinary organizational insiders\(^1\). Insiders, make daily decisions that have a direct impact on their organization’s security[14]. Regardless of the technological security

---

\(^1\)Insiders are part-time employees, full-time employees, temporary workers, and consultants who have access to an organization’s information and/or information systems[13]
measures in place, the success or failure of an organization’s security efforts relies on these insiders’ diligence and knowledge. So, it is important to note these insiders pose considerable intentional[15] and accidental security risks to firms[16], both of which are extremely costly[17]. In fact, according to a study[18], in which 33 interviews were conducted, both organizational insiders and information security professionals, considered that the employees, in an intentional or unintentional way, are the main threat in security of the organizations, with a percentage of 36% and 57% respectively. This is shown in Table 3.1.

Table 3.1: Percentage main security threats according Organizational Insiders and Information security professionals.

<table>
<thead>
<tr>
<th>Organizational Insiders</th>
<th>Information Security Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hackers-39%</td>
<td>1. Employees-unintentional-35%</td>
</tr>
<tr>
<td>2. Internet threats-22%</td>
<td>2. Internet threats-26%</td>
</tr>
<tr>
<td>3. Employees-unintentional-19%</td>
<td>3. Employees-intentional-22%</td>
</tr>
<tr>
<td>4. Employees-intentional-17%</td>
<td>4. Social Engineering-13%</td>
</tr>
<tr>
<td>5. Intrusion by competitors-3%</td>
<td>5. Hackers-4%</td>
</tr>
</tbody>
</table>

Source of Data: [18]

In the mentioned study, it was also verified that according to information security professionals, the main threat vulnerability in an organization it’s the uneducated/inexperienced of the employees in the company. In fact, as can be seen in Table 3.2, 40% and 48% of the themes elicited from insiders and security professionals, respectively, related directly to insider’s involvement. Both groups noted that employees could be the “weak link” in the security chain through their careless actions, unwillingness to follow protocol and a general lack of participation or interest in security education, training, and awareness programs.

Table 3.2: Percentage of threat vulnerability themes according Organizational Insiders and Information Security Professionals.

<table>
<thead>
<tr>
<th>Organizational Insiders</th>
<th>Information Security Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inadequate system configuration-20%</td>
<td>1. Uneducated/inexperienced employees-35%</td>
</tr>
<tr>
<td>2. Careless/lazy employees-20%</td>
<td>2. Inadequate system configuration-31%</td>
</tr>
<tr>
<td>3. Organizational structure-15%</td>
<td>3. Disgruntled employees-8%</td>
</tr>
<tr>
<td>4. Uneducated/inexperienced employees-10%</td>
<td>3. Inadequate policies-8%</td>
</tr>
<tr>
<td>4. Disgruntled employees-10%</td>
<td>4. Careless/lazy employees-4%</td>
</tr>
<tr>
<td>5. Telecommuters-5%</td>
<td>4. Organizational structure/culture-4%</td>
</tr>
<tr>
<td>5. Physical security-5%</td>
<td>5. Amount of information in organization-4%</td>
</tr>
<tr>
<td>6. Personal information collected by organization-5%</td>
<td>4. High employee workloads-4%</td>
</tr>
<tr>
<td>5. Crowded areas-5%</td>
<td>4. Equipment failure-4%</td>
</tr>
<tr>
<td>6. Amount of information in organization-5%</td>
<td></td>
</tr>
</tbody>
</table>

Source of Data: [18]
From this study is understood, firstly that it’s fundamental to transfer the security situation of a company from the experts to the workers. Secondly, from this study can also be drawn that even with the best security tools, a company will remain highly vulnerable to attacks if insiders are not properly trained and no security measures are followed. Thus, the activities and the behavior carried out by employees must be include in the list of measures and controls of any company.

Threats from companies are constantly increasing and cyber-risk exposures are embedded in the operations of organizations across all sectors and countries. No company is fully secure, no matter how sophisticated its cyber-defense mechanisms are. As technology and digital connectivity evolve, companies face new threats every day. It is a vicious cycle. As technology advances, the risk for new sophisticated attacks increases. Therefore, a company may not be considered completely secure, since security is a concept associated with certainty or lack of risk and absolute certainty in this field is not possible. In a company the element of risk is always present, regardless the measures or controls used, being able to become only acceptably secure.

Although no protection is infallible and no company can be completely secure, vulnerabilities can be greatly reduced through information security, covering each of the security needs of the organization. This is important, since security is not an issue that can be left to lower levels of the organization or to the highest levels, but must be considered in every single level. However, information security is an uncertain and complex field, and it is difficult for companies to determine what levels or controls they should cover in function of their business processes and technical needs. That is why, companies often use guides to determine how to protect their information assets.

### 3.3 Information security guides

The recently revised ISO/IEC 27000:2016 gives a comprehensive view of Information Security Management Systems (ISMS). An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. Its aim is to effectively manage the accessibility of information, seeking to ensure the confidentiality, integrity and availability of information assets, while minimizing information security risks. Although the term is mainly used by the series ISO 27000, in this project the term may be used independently of these series.

The majority of security guides that specify the requirements for establishing, implementing, maintaining, monitoring, reviewing and/or continually improving the ISMS within the context of any organization can be placed into one of these categories:

**Benchmark:** Recommended technical control rules for specific environments (hardening operating systems, middleware and software applications, network devices, etc) [20].

**Standard:** Techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization [21].

**Framework:** A series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. [22].
Regulation: Typically an enforced guideline with prescribed repercussions (penalties).

The purpose of cyber-security regulation is to force companies and organizations to protect their systems and information from cyber-attacks [23].

The most used are shown in the Table 3.3. Most address specific security issues and provide advice based on experience, collaborative information and activities (best practices) that have been proved to be effective. Each provides detailed guidelines on how to apply security, how to build an effective security program and how to measure security investments [24].

Table 3.3: The most commonly used security guides and their classification.

<table>
<thead>
<tr>
<th>Benchmarks</th>
<th>Standards</th>
<th>Frameworks</th>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Benchmarks</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISA Checklists</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>ISO 15408</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>ISO 27001/27002</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>NIST 800-53</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>NIST CSF</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>TOP 20 CSC</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>COBIT v.5</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>HIPAA</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>NERC CIP</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>SOX</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>GLBA</td>
<td></td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>

Source of Data: [24]

Any of these security guides helps organizations to undertake the following steps in establishing, monitoring, maintaining and improving its ISMS [1]:

(a) Identify information assets and their associated information security requirements
(b) Assess information security risks and treat information security risks
(c) Select and implement relevant controls to manage unacceptable risks
(d) Monitor, maintain and improve the effectiveness of controls associated with the organization’s information assets

The points a, b and d are specific steps that each company must follow according their specific assets. However, the third point, selection of the relevant controls to manage unacceptable risks, corresponds with the list of security controls that a company must meet to be considered safe. This list of security controls may come from existing sets of security controls, generally included in some of the information security guides enumerated in the Table 3.3 (ISO 27002, TOP 20 CSC, etc.), or be the result of a combination of the mentioned set and the added modifications according to the requirements of a specific organization. This project requires to have a list of security controls that is as generic as possible in order to be able to help any company and not a specific one. Therefore, the most used and significant security guides are detailed in the next subsections, showing the security controls list of each one and its benefits and problems. In
Chapter 3. Literature Review

this way, in Chapter 5 it will be possible to decide which is the most suitable security control list.

3.3.1 ISO 27001 and 27002

ISO/IEC 27001 is a standard for information security (Information technology - Security techniques - Requirements) approved and published as an international standard in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [25]. It specifies the requirements to establish, implement, maintain and improve an information security management system (ISMS) according to what is known as the ”Deming Cycle”: PDCA - an acronym for Plan, Do, Check, Act. It is consistent with the best controls described in ISO/IEC 27002, developed by the British Standards Institution (BSI). Thus, ISO 27001 and 27002 are two standards for information security systems and processes that complement each other. 27001 focuses on management while 27002 focuses on detailing the security controls necessary to make 27001 possible. Both certifications are aimed at performing risk assessments and then making appropriate changes in policies, processes (ISO 27001) and controls (ISO 27002) [26]. As ISO standards are reviewed every 4 or 5 years, the latest updates are from 2013 (ISO 27001:2013 and 27002:2013) and therefore many of the security controls of ISO 27002 are outdated. The objectives of this study fall on security controls, hence this section focuses on ISO 27002:2013.

ISO 27002 is one of the most known data security frameworks, especially in Europe, and controls can be easily interpreted by both internal and external stakeholders such as auditors, customers, government, etc [27]. It provides recommendations of the best practices in the management of the information security to all those interested and responsible in initiating, implementing or maintaining ISMS [28]. Within ISO/IEC 27002:2013, the information of ISO/IEC 27001:2013 annexes is expanded, describing the control domains and the control mechanisms which can be implemented within an organization, according to ISO 27001 guidelines. In this version of the norm is the controls that seek to mitigate the impact or possibility of occurrence of the different risks of any organization [29]. ISO 27002 is used as a reference document but, unlike ISO 27001, is not a formal specification and is not certifiable [30]. Despite it is not going to be taken into account in this thesis, it is important to note that there are specific versions of ISO/IEC 27002, focused on different types of specific companies: manufacturing, health sector, financial sector, among others. Although the ISO nomenclature is different, they are standards that take as reference the aforementioned ISO 27002 and therefore are alienated for the correct management of information security.

The current version, ISO 27002:2013, contains 114 controls presented in fourteen control areas, as opposed to the 133 controls presented in eleven control areas documented within the previous version. Within each section, the objectives of the different controls for information security are specified. For each of the controls a guide for their implementation is also indicated [31]. The sections as well as their number of controls are shown in the Table 3.4. In the Appendix the 35 controls objectives (one per security control category) are enumerated according to the ISO/IEC 27002:2013.

In conclusion, ISO 27002 serves as an information point for the series 27000. It evaluates its implementation through the application of control objectives. These objectives have
Table 3.4: Control Areas and their number of controls (ISO/IEC 27002:2013)

<table>
<thead>
<tr>
<th>Families</th>
<th>Number of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security policies</td>
<td>2</td>
</tr>
<tr>
<td>Organization of information security</td>
<td>7</td>
</tr>
<tr>
<td>Human resource security</td>
<td>6</td>
</tr>
<tr>
<td>Asset management</td>
<td>10</td>
</tr>
<tr>
<td>Access control</td>
<td>14</td>
</tr>
<tr>
<td>Cryptography</td>
<td>2</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>15</td>
</tr>
<tr>
<td>Operations security</td>
<td>14</td>
</tr>
<tr>
<td>Communications security</td>
<td>7</td>
</tr>
<tr>
<td>System acquisition, development and mainten-</td>
<td>13</td>
</tr>
<tr>
<td>ance</td>
<td></td>
</tr>
<tr>
<td>Supplier relationships</td>
<td>5</td>
</tr>
<tr>
<td>Information security incident management</td>
<td>7</td>
</tr>
<tr>
<td>Information security aspects of business</td>
<td>4</td>
</tr>
<tr>
<td>continuity management</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>8</td>
</tr>
</tbody>
</table>

Source of Data: [31]

to be fulfilled to guarantee the correct implementation of the rules, as well as the correct operation of the company in terms of information security.

3.3.2 NIST Special Publication 800-53

The purpose of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 is to recommend the necessary guidelines for selecting and specifying appropriate security controls for organizations and information systems [32]. Although NIST SP 800-53 controls have been designed for US government agencies, they provide information security standards that can be applied to a wide range of environments and organizations [33].

Specifically, the NIST Special Publication 800-53 aims at the Risk Management Framework that is in charge of selecting the security controls for federal information systems according with the requirements in the Federal Standard of Processing Of Information (FIPS) 200. Recognizing the importance of maintaining the relevance and currency of Special Publication (SP) 800-53, NIST is updating Revision 4 to Revision 5. In fact, on April 2016 closed the period for public comments on the draft. Currently, the version in force is the Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, which represents the most comprehensive update to the security controls catalog since its inception in 2005 [34]. It provides a more holistic approach to information security and risk management. It focuses on strengthening information systems, providing security controls with the breadth and depth needed to deal with new cyber-attacks and new threats [35].

The Security Control Catalog is on Appendix F of the standard SP 800-53 and it is a set of controls that are the safeguards (or countermeasures) of management, operations and techniques prescribed to ensure the confidentiality, integrity and availability to the
information of the organizations. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices [32].

In this catalog, the controls are categorized into 18 families and each one encompasses security controls related to the general security topic of the specific family. In order to be able to identify each family of control, it is assigned a identifier of 2 characters to each one of the 18 families. Also, for the controls, a number is added to the above-mentioned identifier to indicate the control number within the family. The families, the associated family identifier as well as the number of security controls into each family are listed in Table 3.5. In Appendix the Families and their general objectives are enumerated according to the NIST SP 800-53, Revision 4.

<table>
<thead>
<tr>
<th>ID</th>
<th>Families</th>
<th>Number of Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>25</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
<td>16</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
<td>5</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>11</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
<td>13</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
<td>11</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td>10</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>6</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
<td>8</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
<td>8</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
<td>20</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
<td>9</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
<td>16</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
<td>6</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorization</td>
<td>9</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communications Protection</td>
<td>44</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
<td>17</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisition</td>
<td>22</td>
</tr>
</tbody>
</table>

Source of Data: [32]

As already mentioned, this thesis is trying to define a list of controls as general as possible and precisely NIST SP 800-53 meets this requirement. The standard has not the aim of providing guides on the application of security controls to specific technologies or environments of operation. In fact, according textual words of the standard the security controls in the catalog with few exceptions, have been designed to be policy and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission.

The first control of each family (known as the the dash-1 control) addresses the policies and procedures necessary to implement the remaining controls of the family. These policies and procedures are not repeated in the rest of controls. Therefore, this standard has some controls that are more priority than others. This priority comes determined by
one of the sections of the security control structure, the *priority and baseline allocation section*, which provides:

(i) The recommended priority codes used for sequencing decisions during security control implementation

(ii) The initial allocation of security controls and control enhancements to the baselines

The priority codes are designed by a $P$ and a number from 1 to 3 ($[P1],[P2],[P3]$), from more priority to less. If the priority code is $[P0]$, it indicates the security control is not selected in any baseline. This prioritization helps to ensure that the basic security controls, on which other controls depend, are implemented first. This allows organizations to deploy controls more efficiently and prioritize the use of available resources. It is important to emphasize that the implementation of part of the controls following the prioritization codes does not mean the achievement of any defined level of risk mitigation until the other necessary security controls have been implemented. The priority codes are only intended to indicate the order of implementation of the controls, not to decide which controls to select for the organization and which not [32].

Therefore, to implement the needed controls, organizations must first determine the security category of their information systems and to select a set of basic security controls based on FIPS 199 worst case scenarios, adapting and complementing to fit more closely with their organizational goals or environments. The information system security categorization (low, moderate or high) determines the collection of reference controls that must be implemented and monitored. Companies must adjust these controls and adapt them to fit more closely with requirements.

### 3.3.3 The CIS Critical Security Controls for Effective Cyber Defense

Since 2008, the SANS Institute has released 20 Critical Security Controls (CSC) for Effective Cyber Defense (often referred to as the SANS Top 20) that provides a recommended set of actions for cyber-defense. The publication was initially developed by the SANS Institute and from 2014 it began to be published by the Center for Internet Security (CIS) in order to ensure information on the network. Currently it is governed by CIS, an international, independent, expert, not-for-profit organization with a global scope and public goals [36] [37].

The main objective of the CIS document is to gather those controls that allow reducing the probability of gaps in cybersecurity. The controls are effective because they are created by actual attacks and effective defenses and reflect the combined knowledge of experts volunteers, who know how attacks work, from every part of the ecosystem with every role and within many sectors. This allows the controls to be the most effective set of technical measures available to detect, prevent, respond to and mitigate the most common damage [38].

Basically, CSC offers a relatively short list of controls which establish a framework that reduces risk and increases safety. Thus, spending is oriented towards the protection of information in a way that actively promotes Return On investment (ROI). This makes
the 20 CSCs more suitable for business managers than a conventional audit guide, although the objectives are very similar: to help to provide information security to the companies [39].

The key is that controls are constantly re-evaluated and updated based on new attacks that are identified and analyzed by groups as Verizon or Symantec so that controls can stop or mitigate those attacks. Therefore, the publication of the CSC for Effective Cyber Defense is updated quite regularly. In fact, since 2014, new versions have been drawing each year approximately. The latest version is the version 6.1, which was released on August 31, 2016 [40].

It is important to note that some controls provide more protection than others, that is, some have more priority than others. For example, the controls from CSC 1 to CSC 5, according to the last version of the publication of the CSCs, are known as "Fundamental Cyber Hygiene" since they are the basic things that must be done to create a solid foundation for the defense of any organization. The list of the 20 Critical Security Controls of the version 6.1 is listed in the Table 3.6 as well as the effect on attack mitigating of each one. Appendix C shows how the structure of the CSCs is and each one of them is briefly described.

<table>
<thead>
<tr>
<th>Critical Security Control</th>
<th>Effect on Attack Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 1: Inventory of Authorized and Unauthorized Devices</td>
<td>Very High</td>
</tr>
<tr>
<td>CSC 2: Inventory of Authorized and Unauthorized Software</td>
<td>Very High</td>
</tr>
<tr>
<td>CSC 3: Secure Configurations</td>
<td>Very High</td>
</tr>
<tr>
<td>CSC 4: Continuous Vulnerability Assessment and Remediation</td>
<td>Very High</td>
</tr>
<tr>
<td>CSC 5: Controlled Use of Administrative Privileges</td>
<td>High</td>
</tr>
<tr>
<td>CSC 6: Maintenance Monitoring and Analysis of Audit Logs</td>
<td>High</td>
</tr>
<tr>
<td>CSC 7: Email and Web, Protections</td>
<td>Very High</td>
</tr>
<tr>
<td>CSC 8: Malware Defenses</td>
<td>High</td>
</tr>
<tr>
<td>CSC 9: Limitation and Control of Network Ports</td>
<td>Moderately High</td>
</tr>
<tr>
<td>CSC 10: Data Recovery Capability</td>
<td>Moderately High</td>
</tr>
<tr>
<td>CSC 11: Secure Configurations for Network Devices</td>
<td>Moderately High</td>
</tr>
<tr>
<td>CSC 12: Boundary Defense</td>
<td>Moderately High</td>
</tr>
<tr>
<td>CSC 13: Data Protection</td>
<td>Moderate</td>
</tr>
<tr>
<td>CSC 14: Controlled Access Based on the Need to Know</td>
<td>Moderate</td>
</tr>
<tr>
<td>CSC 15: Wireless Access Control</td>
<td>Moderate</td>
</tr>
<tr>
<td>CSC 16: Account Monitoring and Control</td>
<td>Moderate</td>
</tr>
<tr>
<td>CSC 17: Security Skills Assessment and Training</td>
<td>Moderately Low</td>
</tr>
<tr>
<td>CSC 18: Application Software Security</td>
<td>Moderately Low</td>
</tr>
<tr>
<td>CSC 19: Incident Response and Management</td>
<td>Low</td>
</tr>
<tr>
<td>CSC 20: Penetration Tests and Red Team Exercises</td>
<td>Low</td>
</tr>
</tbody>
</table>

Source of Data: [41]
On the other hand, the CSCs can be categorized based on three possible families [41]:

- System
- Network
- Application

3.4 Security Tools

It is important to note that, as already was indicated in Section 3.2, for a company to become acceptably secure, to carry out several different measures is necessary such as to use adequate security software, to train the employees, to meet the policies, etc. Although different measures and perspectives are necessary to be able to cover the security controls of the lists mentioned above, the purpose of this project is to help companies to comply, as far as possible, with the security controls through the suitable choice of the software. Therefore, this section shows the entire theoretical part related to software security tools.

Security tools is a general term used to describe any software that helps to protect a company against malicious threats, such as malicious attacks. The target is to minimize the likelihood that something or someone is able to manipulate applications to access, steal, modify, or delete information assets of the companies. In this way the company could continue to function properly under such potential risks [42].

There are many types of security tools such as anti-virus software, encryption software, firewall software, SIEM software, spy-ware removal software, etc. Security tools can be classified based on their function. The possible functions are [43]:

- **Preventive**: They act before an event occurs and its function is to stop unwanted agents.
- **Detective**: They detect if there are attempts to breach the security of the system and reveal the presence of unwanted agents in any component of the system. They are characterized by sending a notice and recording the incident.
- **Corrective**: They are applied when a system security violation has been detected to recover its normal operation.

Nevertheless, in spite of its functions the final objective of the security tools is to provide integrity, confidentiality and availability to the assets, that is, the resources that are part of the system. Generally, the 3 main elements to protect in any organization are [44]:

- **Hardware**: Set of all physical elements of a computer system such as CPU, terminals, cabling, secondary storage media (booths, disks, tapes, DVDs, ...), etc.
- **Software**: Logical elements or programs that run on the hardware, whether it is the operating system itself or the applications.
- **Data**: It comprises the logical information that the software processes using the hardware. In general they are structured in databases or information packets that travel through the network.
Chapter 3. Literature Review

3.5 Method theory

One of the goals of this project is to create an investigative method which allows to determine which security controls are covered by any security tool. Hence, this section shows the theoretical part related to the method that has been investigated to take part of the decisions.

The term method refers to the set of strategies and tools that are used to reach a specific goal. It is a rigorous procedure, formulated in a logical way, that must be followed step by step. If a method is well formulated and its steps are repeated it should give the same or similar results. The following subsections list and explain some of the strategies that are used to create a method. It is important to understand this theoretical part, in order to understand the decisions that are made in the next chapter.

There are two general approaches to gathering and reporting information: qualitative and quantitative approaches. This thesis only uses the first one, but it has been considered that it can be better understood if the two are explained in the 2 first subsections, 3.5.1 and 3.5.2. Then, in Subsections 3.5.3 and 3.5.4, the collection of documentary information and interviews are explained respectively.

3.5.1 Qualitative investigation

Qualitative investigation seeks to acquire in-depth information in order to obtain a complete and detailed description of the investigation topic. Usually, it has an exploratory perspective. Qualitative investigation is ideal for the initial phases of a investigation project. It is, therefore, designed to gather accurate information that explains concepts or events that are not well understood. The collection of accurate information is a critical part of the investigation and the main instrument in this type of investigation is the investigator. Various information collection strategies are used, depending on the orientation or approach of the investigation, including revision of existing bibliography, surveys, interviews, tests, observations and samples. This type of investigation has a fundamentally subjective approach since it is the investigator who makes the decision based on the information he/she has collected and at their criterion [45].

3.5.2 Quantitative investigation

Qualitative investigation is based on numbers to investigate, analyze and verify information and data. It provides the investigator with a clearer vision than qualitative investigation. It is highly recommended for the last part of the project. Quantitative investigation makes use of tools such as questionnaires, interviews, measurements and other equipment to collect numerical or measurable information. In this investigation, contrary to the qualitative, the investigator tends to remain objectively separated from the topic. This is because quantitative investigation has an objective approach in the sense that it only looks for the most precise measures possible and an analysis of the hypothesis without the investigator making use of his criterion [46].

The techniques of qualitative and quantitative investigation are not opposed but complementary. In many cases to use both techniques is advisable, starting usually with the qualitative ones that allow to explore meanings, followed by quantitative ones [46].
3.5.3 Documents compilation

Documentary compilation is a fairly common form of investigation, which occurs when an investigator examines and extracts information from documents that contain information about the topic to be analyzed. There are different kinds of documents: written, numerical or statistical, software codes, image and sound, etc. The information can be obtained by conducting a selective search in both libraries and on the Internet, trying to gather critical information from any type of source such as books, scientific papers, websites, whitepapers, etc. However, the sources will be valid only when they can be admitted as valuable and reliable and that can be cited by their source [47].

3.5.4 Interviews

The purpose of interviews is to obtain data by consulting or interrogating a set of people chosen for investigation, usually randomly selected. Interviews can be administered in person, by Skype, mail, telephone or electronically. They can also be given to an individual or a group. The conditions must be established in such a way that the observable facts are carried out in the most natural possible way and without influence of the investigator or other factors. When to use this method is decided, the careful preparation of the observers is essential, ensuring the reliability of the data that is recorded and collected [47].

Previously, in subsections 3.5.1 and 3.5.2 have been indicated that both qualitative and quantitative investigation collect information through interviews. However, there is a difference between the type of interview depending on the questions being asked. There are mainly three types of questions and are classified according to the answer that the respondent admits [48]:

(i) **Close-ended questions**: Also called precoded or fixed response, are those in which the respondent, to reflect their opinion, should choose only a response between two or more options: YES / NO, TRUE / FALSE, A / B / C / D, etc. They have as advantage that they are easy response and coding. However, the information they offer is limited. They are characteristics of quantitative investigation.

(ii) **Multiple-answer questions**: They are those that the respondent, to reflect their opinion, can choose a response or several between two or more options. With these estimation questions to obtain a score for each of the respondent of the investigation is not intended, but simply a distribution of frequencies of the responses issued.

(iii) **Open-ended questions**: Open questions are considered when the respondent is given the freedom to respond in their own words. This type of question is used in qualitative studies. They have as advantage that they provide much information and maximum freedom to the respondent. However, the coding of the answers may involve certain difficulties and demands a greater effort for the respondent to answer.
Chapter 4

Data

4.1 Introduction

This chapter shows all the data and all information collected that has not been covered in the literature review. The chapter has been divided into two sections. In the first, Secondary Data, a set of security tools are described that have been collected for their classification in the case study of Section 5.6. In the second section, Primary Data, data obtained from the interviews is shown.

4.2 Secondary Data

In this section the collected security tools are shown in order to meet the last goal explained in Chapter 1:

Do a case study where a representative set of security tools is classified according to part of the method and with the results show how they are stored and how the developed tool works.

In every single Critical Security Controls, except in CSC 17, one (or several) security tool(s) widely used by the companies of nowaday have been collecteds, the result is shown in Appendix E. CSC 17 is a security control related to the knowledge, skills and abilities needed for employees, to support defense of the enterprise. Therefore, there are no security tools that cover this control, at least not in a relevant way. Anyway, in Table 4.1 is detailed the number of security tools collected for each CSC.

As discussed in the Methodology chapter, Gartner reports have been reviewed to determine the widely use of security tools collected. The references of each security tool are stored in the Neo4j database, in References parameter.

The fact that the security tools have been categorized according to the CSC that they cover mainly does not mean that they do not cover more than one of the controls. In the case study, all the collected security tools have been classified following the method of Section 5.3, in order to determine which CSC(s) is(are) covered by each one.
4.3 Primary Data

4.3.1 Interview Data

This section reflects the ideas obtained from each of the interviews conducted. The interviews have been carried out to obtain relevant information that helps to achieve the objectives established in Section 2.4. Despite the few interviews conducted, almost all the required information has been obtained. Even though some respondents did not answer some questions, in the overall all answers have been answered. However, to obtain the information from one of the established sources has not been possible:

*To find out which are the security tools most used by companies to cover Critical Security Controls*

To meet this objective, it was necessary that the respondents indicate which are the security tools used in their company to cover the different CSCs. However, for reasons of confidentiality and privacy of the companies, none of the respondents has given any information about it. According to the exact words of one of the respondents, *information security in companies is a very delicate and confidential topic, and in particular security tools is even more “black box”. That is to say that nothing can be said about it and in many cases even employees do not know the tools that are used to prevent leaks.*

Therefore, next the main ideas of the information obtained for each of the other objectives are reflected, according to the respondents:

**Respondent A:**

*Are the CSCs relevant?*

The respondent did not know the CSCs. He/she belongs to a small company, approximately 200 employees, of commercialization of medical surgical technology products. The company does not cover the most of the controls since, according to their own

---

**Table 4.1:** Number of security tools collected by each CSC

<table>
<thead>
<tr>
<th>CSC 1</th>
<th>CSC 2</th>
<th>CSC 3</th>
<th>CSC 4</th>
<th>CSC 5</th>
<th>CSC 6</th>
<th>CSC 7</th>
<th>CSC 8</th>
<th>CSC 9</th>
<th>CSC 10</th>
<th>CSC 11</th>
<th>CSC 12</th>
<th>CSC 13</th>
<th>CSC 14</th>
<th>CSC 15</th>
<th>CSC 16</th>
<th>CSC 17</th>
<th>CSC 18</th>
<th>CSC 19</th>
<th>CSC 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

---

Chapter 4. *Data* 28
words, there is not sensitive or valuable information in the company that requires a big investment in information security. He/she also said that obviously the company covers its security needs, which he/she preferred not to indicate, but taking into account the size of the company and the kind of business. We do not require the same investment in information security than a bank, for example. He/She pointed out that although he/she did not know the CSCs before, they seemed well structured and well defined and could be relevant to establish the company’s security needs.

Criteria followed to choose the security tools

They do not follow any rigorous process to pick the tools. They simply chose the tools that covered the necessary following the recommendations of the vendors and these are updated periodically.

Opinion about the draft method

The respondent did not mention any modification but he/she said that the steps seemed logical. He/she also said that it would be very useful to have an extensive database which contains objective information about the different security tools, obtained from such a rigorous method like the one that was presented to their. In this way, small companies like their, which do not have the necessary resources, could have reliable information.

Respondent B:

Are the CSCs relevant?

The respondent did not know the CSCs. In his/her company information security is tracked through system security plans that come from ISO standard. They cover completely 12 CSCs, partly 4 CSC and the other 4 are not cover. However, the respondent considers that all the CSCs are relevant for his/her company, except the last one.

Criteria followed to choose the security tools

The respondent explained that each tool is procured as part of a project. The first step is to identify functional requirements for the tool, such as the protocols supported. The second step is to talk to partners from the same field and see what tools they are using. The third is to contact the tool vendor itself. He/she added that quite often when a software is acquired, the software vendor also recommends other security tools that they are familiar with the recently acquired.

Opinion about the draft method

The respondent did not add any comment about it.

Respondent C:

Are the CSCs relevant?

The respondent is a CISO that was working on EY with the ISO standard, so he/she was asked about ISO controls as well as about the CSCs. The respondent thinks that the control objectives of the ISO standard are very general and that the true utility of the standard is to establish a framework of control or government from which to "control" the security of an Entity. However, of course there are exceptions, it can be a very powerful tool if the company gives it value and do not just writes superfluous policies and procedures. To do this, the organization, or the audit, must carry out a detailed
implementation and should be concerned that the controls within the control objective are real, measurable and that lead to remediation actions when necessary. The respondent concluded by adding that, in short, ISO controls are more government-oriented, while CSCs are more management-oriented controls, being the last ones more actionable and less ambiguous.

**Criteria followed to choose the security tools**

The participant responded in a general way, and did not indicate the specific criteria followed in their company for privacy reasons. He/she said that normally, each entity establishes its own protocol and is not a procedure that transcends to avoid leaks. In the big companies there are committees of new initiatives through which all the requests pass. Both by request of the departments by needs (whether or not security) or by products that are presented to companies through commercial or pre-sales (which are a mix between technical and commercial). According to this, different techniques are applied to choose or not the software: opinions in specialized forums (almost all security professionals share information among them to see market trends, products, etc.), Vendor Risk Management projects (to evaluate suppliers with analysis of Risks, etc.) and contracting consulting services to evaluate the product, either externally (Gartner) or internal (using experts to evaluate a pilot or demo).

**Opinion about the draft method**

Unfortunately, it was not possible to ask to the respondent this question.

**Respondent D:**

**Are the CSCs relevant?**

The participant responded based on their broad experience in information security and not based on a specific company. The interviewee knew the CSCs and considers that they are very relevant, since any large company tries and needs to cover each and every one of the controls. In fact, he/she added that on many occasions, large companies use several security tools to cover a single CSCs. He/she concluded by saying that for small and medium-sized enterprises, it may be enough to check whether CSCs are covered or not, but that in larger companies it would be necessary to go one step further. That is, analyze whether or not each of the sub-controls is covered, since the small details of information security make the difference in this type of companies. However, the respondent pointed out that such a detailed analysis is much more costly.

**Criteria followed to choose the security tools**

The interviewee responded based on the draft of the proposed method.

**Opinion about the draft method**

The respondent indicated that he/she considered that the method lacked objectivity. The steps to follow are correct: carry out an research of the chosen tool, analyze the data collected, construct a decision and finally evaluate it. However, the whole process is done based on the criteria of a single researcher, which makes it very subjective. The researcher who has carried out the investigation can not carry out the evaluation, since this will possibly give a biased result. The use of the trial version of the chosen security tool can be used as a support, but not as a single evaluation method. Large companies have committees and experts who come to a consensus to make these kinds of decisions. It is
right that in the method proposed, interviews are conducted to collect information from
the security tool, but, in my opinion, interviews should also be conducted to evaluate the
decision. I believe that it would be appropriate for the decision to be evaluated through
surveys conducted to several security experts who have used the security tool. This would
allow to achieve much more objective and realistic results.
Chapter 5

Results and Analysis

5.1 Introduction

This chapter presents the results of the thesis according to the goals established in Chapter 1. Each section of this chapter corresponds to one of the goals. In section Security Controls, the different information security guides identified in the literature review are analyzed and the most suitable list of security controls is chosen. In the section called Investigative Method a rigorous method is developed using the data collected from the literature review and interviews conducted to information security experts. The purpose of this method is to categorize any security tool according to the chosen security controls list. In section Data model, a data model is designed which allows to organize the data obtained from the method. In section Visualization tool, a tool is developed which, with the information of the previous sections, helps the companies to choose, based on their needs, the adequate security tools. Finally, in section Case Study, the implemented case study is described based on the work described in the previous sections.

5.2 Security controls

This section shows the chosen list of security controls from all the guides that have been investigated. For this, the advantages and disadvantages of ISO 27002: 2013, NIST SP 800-53 and CIS Critical Security Controls have been summarized in Table 5.1, based on the literature review of Section 3.3.

CIS CSCs was chosen as the list of security controls that is most suitable for this study. However, it is important to note that this does not mean that the guide is better than the others, but it is better from the perspective of the requirements established in Chapter 1, which say that the list of security controls should be:

- Well defined and actionable - not ambiguous
- Relevant to the industry
- Updated Frequently
### Table 5.1: Advantages and disadvantages of the main frameworks and standards

<table>
<thead>
<tr>
<th>Frameworks/Standards</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| ISO 27002:2013       | - Adequate framework for complying with information security legal, regulatory and contractual requirements.  
- It is an internationally recognized and accepted standard. The controls can be easily interpreted by both internal and external stakeholders.  
- Companies can become certified with it (ISO 27001) | - ISO standards are reviewed every 4 or 5 years. Many of the controls of ISO 27002:2013 are obsolete  
- Does not distinguish between controls that are applicable to a specific organization and those that are not |
| NIST SP 800-53, Rev 4. | - The security controls have been designed to be policy and technology-neutral  
- Security controls are created by actual attacks and effective defenses | - SP 800-53 has a biennial update.  
- Families of controls are ambiguous and the list of specific controls exceeds 250 security controls. |
| The CIS Critical Security Controls | They emphasise on “What Works”.  
- Small number of actions with high pay-off results.  
- Security controls are constantly re-evaluated and updated based on new attacks. The publication is updated every year approximately.  
- Well-defined and simple list of security controls  
- Suitable for business managers | - It is less known than the others. |
As can be seen in Table 5.1, the CSCs have several advantages but the most important are those that correspond to the established requirements.

Firstly, it is important to note how well-defined they are. The CSCs are 20 while other lists are longer. The CSC list also contains all the topics covered by the other lists in a concise way. In addition, the list of controls is simple and clear, so it can be understood without having a deep knowledge in information security. Thereby, the information security experts could explain the security need requirements of the company to the business managers and them to the rest of the company, without complications.

Secondly, they are relevant to the industry since according to the authors the list has been created combining knowledge and information from security experts working in the industry. They are created by actual attacks and effective defenses, emphasizing on “What Works”.

Thirdly, they are constantly reevaluated and updated based on the new attacks, which is an aid to companies to be able to also update their security needs. Up until now the CSC list has been updated annually.

The list of security controls, and therefore the deliverable of the first goal, is the Critical Security Control list which is shown in Table 3.6 of the literature review chapter.

5.3 Investigative method

This section defines a set of steps which must be followed successively to categorize any chosen security tool, according to the security controls covered by it. Many of the security tool vendors exaggerate the features of their products. That is why, to establish this mapping between security controls and security tools in a completely objective way is difficults. Thus, the guidelines and decisions taken in each of the steps of the method developed have followed an evolutionary process, a process of improvement, detailed in Section 2.2 of the methodology chapter, with the aim of making a method as reliable as possible. The method is generalized and repeatable, so it can be solved in the same way in similar future problems and to obtain the same reliable results.

The method has been divided in four parts. Each of the parts is explained in the subsections of this section. To understand better the whole method, the four parts are summarized in Figure 5.1.

Before starting with the method, it must be indicated that as was mentioned in Appendix C each CSC has different sub-controls. This means that sometimes the CSCs could not be fully covered by only one security tool, but that they are just partially covered in function of the sub-controls covered by that security tool. However, in this project the sub-controls are not considered, due to the scope, as was indicated in the introduction chapter. Only the 20 Critical Security Controls of Table 3.6 are taken into account. Therefore, the controls may be either completely covered or not covered. The case where controls are partially covered is not considered.
5.3.1 Identification and data compilation

The method input variable is any security control software tool. Therefore, before analyzing any tool should check whether it meets the requirements to be analyzed with the method. According to the literature review of the Section 3.4, a security control software tool is any software that helps to protect a company against malicious threats providing integrity, confidentiality and/or availability. Their possible functions are preventive, detective and/or corrective. Thus, a tool is included in this method, only when can be used to prevent, detect, or correct a threat to information confidentiality, integrity and availability.

The respondents of Section 4.3 agree that the first step in choosing a tool is to identify it, what the tool is capable of, which are its features, who is its provider, etc. For this, it has been decided that firstly a qualitative investigation should be carried out. According to the literature review of Section 3.5, in this investigation it has been decided that the investigator should acquire in-depth information in order to identify completely the security tool and to be able to decide which is/are the Critical Security Control/s covered by the chosen security tool through a documents compilation.

In order to be able to understand in depth the features of the analyzed security tool, the investigator must examine and extract valuable information from documents related with the topic. As was mentioned in the Subsection 3.5.3, the gathering of the information can be done from any type of source but it has to be admitted as valuable and reliable.
Therefore, the information must be extracted from sources of quality and reliability. The quality of sources ensures, through the control of validity and authenticity, that the criticism and interpretation of the information obtained can be carried out with the certainty of an analytical basis without errors. Below, there are some sources, ordered from the most reliable to the least reliable, that have been chosen for this method based on the answers of the respondents of Section 4.3:

(i) *Gartner* reports

(ii) Scientific papers

(iii) Demo tool

(iv) Websites (Security tools vendors)

(v) Websites (Reviews, blog/forum)*

*Note: Information from this source should be extracted cautiously. It has been proven from experience that the information presented in this source is usually unreliable, so it should be taken only as a support of the other sources, to clarify concepts.*

It is necessary to decide what data one wants to obtain from said sources. For this the following parameters have been defined that the investigator must complete in the most objective possible way. These help with the identification of the analyzed tool and its subsequent categorization. The parameters are explained below, as well as the reasons why these have been chosen:

- **Tool:** This parameter includes the complete name of the security tool. It is important to note that the name of the product must be written and no the name of the company which has created the product. Usually software providers develop several products and each has different objectives. Therefore, each product should be considered and analyzed differently. This parameter is required/mandatory as it is used as an identifier for a particular tool. Therefore, the full name should be noted to avoid confusion with other products with a similar name.

- **Overview:** This parameter should introduce by means of a brief summary what the security tool does from a general perspective. This helps to to make a first categorization and that future investigators can identify the product without going into detail.

- **Description:** This parameter includes a deeper description of the security tool from the perspective of the control(s) covered by it. Therefore, it is a specific description in function of the target(s) and the feature(s) of the security tool. This parameter is fundamental since with all the features of the security tool listed, subsequently to decide which control(s) is (are) covered by the tool will be possible.

- **Provider:** This parameter includes the name of the company or organization who provides the tool. This is another parameter to identify the tool. It should be noted that some products have been created by a provider and subsequently another company has purchased the product rights and now it belongs to it. Therefore, it must be indicated the current provider and not the designer.
References: This parameter includes the references of the artifacts that have been used to obtain the above information. In this way, any user will be able to corroborate the reliability of the sources and as was said in the Subsection 3.5.3, a reference helps to determine the trustworthiness of an information, by being able to determine the trustworthiness of the source.

Date: Includes the date (mm/yy) in which the data is entered into the database. The information of the database will be used by other investigators in the future and since software probably will get old in 3-5 years, the information could be obsolete.

On the other hand, according to the respondents of Section 4.3, the companies usually contact partners or software providers to obtain external information about the security tool. That is why it has been decided that interviews could be another option to collect more data. However, based on the experience gained throughout the project, it has been found out that it is difficult to arrange such interviews, since it is difficult to find people who have the knowledge needed. In addition, even if these people are found, after wasting a lot of time, they do not usually want to reveal cyber-security information in detail. This is often considered confidential. Therefore, it is recommended that the use of interviews to collect more data be performed only if necessary. That is, only if the investigator has not been able to collect from the other sources the information needed to make a decision on the CSCs covered by the tool.

Although this is an optional step, which only is taken if it is necessary, the guidelines that should be followed are described below. According to the literature review of Section 3.5, being a qualitative investigation, the interviews are done with open-ended questions, providing in this way much information about the topic and maximum freedom to the respondent. Interviews to be conducted should not be more than two, to prevent the method from becoming too lengthy. The only criterion that has to be met by the interviewees, besides to have a role related with information security, is that they have used (configured/run) the tool. For these interviews, the people to be interviewed do not need to be familiar with the CSCs. This is because it is not intended to determine which CSC(s) is(are) covered by the tool in the interviews, since this is done in the next part of the method. The purpose of the interviews is to get as much information about the security tool as possible. Potential candidates for interviews could be:

(i) Employees of companies with information security roles*

(ii) Users with information security knowledge

*Note: If the investigation is carried out by a company, it may be interesting to look for candidates in companies with similar business interests. However, must be warned that they will probably not provide information on the software used by them.

According to the literature review, the interviews conducted face to face are better since it is possible to see the body language and engage the respondent’s attention better. However, when conducting interviews it has been ascertained that on many occasions to interview people from other cities and countries is required. On these occasions, it is better to do the interview through Skype or telephone, since the time and money
spent on traveling is not worth it. In addition, to being open-ended questions suppose a greater effort for the respondent to answer and thereby to get accessible respondents from the same place is more complicated.

The interview template is attached in Appendix E. The questions are simple, since based on the experience gained in this thesis, if the respondent does not understand the question, no answers will be obtained. However, the job of the investigator is to help the respondent with examples, if it was needed, and to write down all the information that the interviewee indicates. Although the interviewee does not need to know the 20 CSCs, the interview consists of 20 questions related with them. In each of the questions is wondered if the security tool covers the guidelines of each CSC. The respondent has to answer with Yes or No and explain the reason of their answer.

### 5.3.2 Analysis and decision

As indicated in the previous step, the data come from different sources. All this information must be ordered according to the source and the type, transcribing the important things and obviating the repeated or unnecessary information. All useful data obtained after the ordering must be analyzed in order to identify which CSCs are related to the features of the security tool analyzed. For this, it is very important that the investigator knows the 20 CSCs in detail in order to identify the relationships. Anyway, the investigator should also use the CIS Critical Security Controls guide as support.

In the case that interviews have been carried out in the previous step, the investigator can use the concise answers of the respondents as an aid in taking the decision. Nevertheless, it is important that the investigator keeps a critical mindset when evaluating all the gathered evidence.

Given the available information it up to the investigator to decide if the software control tool is good enough to meet the requirements set by each of CSCs. Although the decision is something subjective based on the criterion of the investigator, it is needed to try to reach the highest degree of objectivity possible with respect to the information.

The investigator will write a decision or several depending on the number of CSCs covered. It is important that each decision is evaluated independently, and not all as a set. That is, in the case that it is decided that a security tool covers three CSCs, if after of the evaluation it is corroborated that it only covers two of the three security tools, two decisions will be accepted and one rejected.

To maintain order, the decision has to be written as follows:

\[
\text{The Security Tool A covers the Critical Security Control X.}
\]

where:

A - the full name of the security tool analyzed

X - the number of the tool correspondent [1-20]

In the case that there were more CSCs covered by the same tool the other decisions would be written as follows:
5.3.3 Decision evaluation

In this part the decision is evaluated. One of the respondents of Section 4.3 indicated that, in order to achieve much more objective and realistic results, it would be appropriate for the decision to be evaluated through interviews conducted to several security experts who have used the security tool.

Since it is only necessary to evaluate if a decision is correct or not, to carry out surveys with close-ended questions, dichotomous, could be logical. However, based on the experience gained conducting interviews, the problem of conducting surveys is that it is not possible to speak directly to respondents. Therefore, the investigator can not be sure that the respondents understand correctly the question(s). To evaluate their knowledge in the area is not possible. In addition, for the results to be representative, to have at least 20 respondents and choose them randomly would be necessary. Given the low response rate, to get 20 respondents would be necessary to send the survey to at least 100 people. That is why, doing surveys would take a lot of time and would not be profitable. Therefore, it has been decided to find a few right people and then using the most effective cost approach to interview them to evaluate the decision taken in the previous step.

The number of interviews to be performed must be greater than or equal to 6, so that the evaluation is sufficiently objective. For the same reasons as explained in step 1, Identification and data compilation, the interview can be conducted face-to-face, by Skype or by phone. The only criterion that has to be met by the interviewees, besides to have a role related with information security, is that they have used (configured/run) the tool. It would be advisable that the interviewee knows the 20 CSCs. However, adding this requirement would greatly limit potential candidates and lengthen the method. Therefore, in case the interviewee does not know the 20 CSCs, it will be the investigator’s obligation to explain objectively the requirements set by each CSCs evaluated. Potential candidates for interviews could be:

(i) Employees of companies with information security roles*

(ii) Users with information security knowledge

*Note: If the investigation is carried out by a company, it may be interesting to look for candidates in companies with similar business interests. However, must be warned that they will probably not provide information on the software used by them.

The interview is basically a question in which it is asked to the respondent if he/she agrees with the decision, that is, it is asked if the analyzed security tool covers the CSC decided in the previous step. In the case that there were more than one decision they would be asked in the same way. The answer is dichotomous, Yes or No. However, the respondent should explain his or her response(s) so that the investigator can verify if the question(s) has been correctly understood.

As indicated in the introduction to the method, sometimes the security software tools
only cover partially the Critical Security Controls since they could cover some of their sub-controls and not all. In these cases, respondents must respond Yes, since intermediate responses have not been considered. All these guidelines are established in the template of the interview, which can be found attached in Appendix F.

5.3.4 Final Decision

In this last step of the method it is decided if the decision is accepted or rejected. In the case that there are more than a decision, they have to be accepted or rejected independently. Thus, it is necessary to calculate the percentage of people agree with the decision(s), that is, the percentage of people whose answer is Yes. According to this percentage, the acceptance intervals shown below are set:

(i) (Acceptance ≤ 50%) : This case occurs when a percentage among 0% and 50% of the respondents have answered Yes. In this case the decision is rejected. If half or more than half of the experts interviewed consider that the decision is incorrect, it can not be ensured that the analyzed security tool covers the particular CSC. At this point, the investigator must do the method again from the beginning since some premise that was taken as certain is not. It will be possible to use the data obtained from this first round of the method but with caution, it should not be forgotten that the decision has been formulated incorrectly.

(ii) (50% > Acceptance < 100%) : This case occurs when a percentage among 50% and 100% (not included) of the respondents have answered Yes. This situation is complicated, since half or more than half of the experts have considered that the decision is correct. However, a significant percentage of the respondents has considered the opposite. That means there is something that leads people to think that the tool analyzed does not actually cover the CSC. In this case, the investigator must analyze the reasons of the respondents who answered No. Then, as one of the respondents of Section 4.3 proposed, he/she could use a demo version of the analyzed security software and try to find out why these respondents do not agree with the decision. Based on their judgment and keeping a critical mind, he/she will decide whether the decision is accepted or not. If it is accepted, the investigator must store in a database which Critical Security Control is covered by the security tool. If it is rejected, the investigation should re-analyze all the information obtained in the first step of the method, Identification and data compilation), and write a decision that will be re-evaluated.

(iii) (Acceptance = 100%) : This case occurs when all the respondents have answered Yes. In this case the decision is accepted. At this point, the investigator must store in a database which Critical Security Control is covered by the security tool.

It is important to note that the amount of respondents is of a minimum size of 6 respondents. However, the larger the size, the more reliable the decision taken.

Below, all the steps of the investigative method are shown again but in a more schematic and clearer way. The reason of this is to show better the final result of this phase, the deliverable.
1. Identification and data compilation

1.1 Inclusion
   a) Does it address impacts to information integrity, confidentiality and availability?
   b) Are any of its functions preventive, detective and / or corrective?

1.2 Qualitative investigation
   1.2.1 Document investigation
      a) Gartner reports
      b) Scientific papers
      c) Demo tool
      d) Websites (Security tools vendors)
      e) Website (Reviews, blog/forum)*
      *Note: Information from this source should be extracted cautiously

   1.2.2 Open-ended questions surveys*
      (a) Employees of companies with information security roles
      (b) Users with information security knowledge
      *Note: Optional, only if it is necessary.

2. Analysis and decision

2.1 Data Analysis
2.2 Construction of the decision

3. Decision evaluation

3.1 Open-ended questions surveys
   (a) Employees of companies with information security roles
   (b) Users with information security knowledge

4. Final Decision

4.1 Decision based on the acceptance intervals of the decision
   a) (Acceptance ≤ 50%) : The decision is rejected. The method must be done again.
   b) (50% > Acceptance <100%) : The investigator uses a demo tool of the software analyzed and based on their criteria and all the answers gathered decides if the final decision is:
      (i) Accepted. The result is stored in a database.
      (ii) Rejected. The method must be done again from the part of Analysis and decision.

Analysis and decision.

4.1 (c) (Acceptance = 100%): The decision is accepted. The result is stored in a database.
5.4 Data model

During and after of carrying out the method described in the previous section, relevant data are obtained from each analyzed security tool. In order to be able to store all this data in an orderly way, a data model has been designed in this section. These data are classified according to the parameters listed in Table 5.2.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Overview</th>
<th>Description</th>
<th>Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td>CSC(s)</td>
<td>Family</td>
<td>Date</td>
</tr>
</tbody>
</table>

As can be seen from the table, the first 6 parameters have already been named and explained in Subsection 5.3.1. However, there are two parameters that have not been correctly detailed yet:

- **CSC(s):** This parameter includes which is (are) the security control(s) covered by the security tool. The possible options are the 20 Critical Security Controls that are enumerated in Table 3.6. This is the most important parameter, since it allows the mapping between the security tool and the security controls.

- **Family:** This parameter includes the family where the control belongs. The possible families are listed in Subsection 3.3.3.

The most important parameter is the one obtained as a result of the method, i.e., the parameter **CSC(s)**. The information of this parameter is the one that helps the companies to choose the appropriate security tools, through the visualization tool developed in this thesis, explained in the next section, Section 5.5. This information is simply a relation between the security tool and the CSC or the CSCs covered by it, as it is shown in Figure 5.2. It must be stored in the MySQL database, since the visualization tool has been developed in such a way that it is only compatible with it.

![Figure 5.2: Relations between the security tools analyzed by the method and the CSCs covered by them](image)
Although the parameter CSC(s) contains the data required by the goals established in the thesis, the rest of parameters, which are obtained when the method is carried out, are very relevant as well. The data of these parameters are the ones that have allowed to reach the final result. Therefore, they are decisive during the development of the method, and are also very important in the case that another investigator wants to verify the results or to carry out future investigations.

All parameters are related to each other. In order to store the data based on the relations between the attributes, a data model has been designed that is shown in Figure 5.3.

![Data model diagram](image)

**Figure 5.3: Data model**

As can be seen in the figure, there are 3 main relationships between the parameters, which are explained below:

(i) **GROUPS:** This relationship indicates in which of the 3 possible families (*System, Network and Application*) are grouped each of the possible Critical Security Controls ([CSC1, CSC20]). In the *Family* block, the corresponding family name is stored. In the *CSC* block the name of the corresponding Critical Security Control is stored as well as a brief description of it.

(ii) **COVERS:** This relationship indicates which security tools (of all those analyzed through the method) cover each of the possible Critical Security Controls ([CSC1, CSC20]). In the *Security Tool* block, the parameters *Tool, Overview, Description* and *References*, explained in Subsection 5.3.1, are stored.

(iii) **PROVIDES:** This relationship indicates which is the provider of each of the possible security tools (of all those analyzed through the method). In the *Provider* block the name of the corresponding provider is stored.

This data model and all gathered data are used by the investigator carrying out the method. Therefore, unlike the final result that is used in the visualization tool, there is
no restriction on which way the rest of the data should be stored. It is the investigator’s role to decide which database to use. For the case study shown in Section 5.6, Neo4j has been used because it has been considered that being a graph database, it can be more user-friendly and easier to visualize the relationship between the data. However, it is only a support tool in the investigation process and therefore to use it is not a requirement.

5.5 Visualization tool

The visualisation tool that will be explained in this section is based on the previously introduced work. In the previous steps an investigative method has been developed that allows to categorize any security software based on the CSCs it covers. This method can be carried out by the companies themselves or by other investigators who want to expand the database with more security tools objectively categorized. However, it is the visualization tool exposed in this section which will be used by the companies as support to choose the appropriate security software based on their security needs. Thanks to this tool, users or companies can visualize the mapping between Critical Security Controls and the security tools analyzed using the method.

In Section 1.3, a series of requirements have been established that the visualization tool must meet, are remembered below:

(i) The mapping has to be shown in a graphic and simple way.

(ii) Ubiquity of the tool so that any user can access it from anywhere.

(iii) User-friendly interface.

In order to meet the first requirement, it has been decided that the mapping is shown through a simple matrix. In this way, at a glance the CSCs covered by the security tools can be seen. This matrix contains the 20 Critical Security Controls, listed in the columns, and secondly, the security tools selected by the user, listed in the rows. The appearance would be similar to the matrix shown in Figure 5.4

<table>
<thead>
<tr>
<th>Security Tool 1</th>
<th>CSC 1</th>
<th>CSC 2</th>
<th>CSC 3</th>
<th>CSC 4</th>
<th>...</th>
<th>CSC 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Tool 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Tool 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Tool 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Tool n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5.4:** Matrix to relate security tools and Critical Security Controls

It has been decided to assign the green to those cells that are the intersection between the security tools and the CSCs covered by them, showing in that way the mapping between the tools and the controls. The Critical Security Controls covered depends on
the security tools selected by the user. Therefore, depending on the mapping, three possibilities can be given:

- The CSC is covered only by one of the security tools selected by the user. In this case, the intersection cell would be green, as indicated.

- The CSC is covered by more than one of the security tools selected by the user, there being an overlap. In this case, the intersection cells between said security tools and the CSC are assigned the blue.

- The CSC is not covered by any of the security tools selected by the user, there being a gap. In this case, all the cells in the CSC column are assigned the red.

In Figure 5.5, a possible case is shown. In it, CSCs 1, 3 and 20 are covered by security tools 3, 2 and 4 respectively. In the CSC 2 there is an overlap, being covered by the security tools 1 and 3 at the same time. However, the CSC 4 is not covered by any of the security tools, therefore there is a gap. In this way, the security situation of the company can be seen quickly and easily.

![Figure 5.5: Case of security situation through matrix](image)

In order to meet the second requirement, the tool has been developed as a web application. In this way, it is possible for any user to use the tool wherever and whenever. To develop the tool as a web application has been used:

- **AngularJS**: It is an open source JavaScript framework maintained by Google. It is used to create and maintain web applications of a single-page application (SPA), for the purpose of giving users a smoother experience, in a very clean way. It is used for the design.

- **Node.js**: It is a run-time environment to build server-side applications. It is used to run the server and connect the application to the database.

- **MySQL**: It is a common database in web applications. It stores the mapping between the 20 Critical Security Controls and all the tools introduced after being categorized by the method.

Figure 5.6 shows the relation between the different entities. The browser shows the web application to the user using **AngularJS**. Once the user selects the tools, **AngularJS** sends an HTTP request to the server. The server uses **Node.js** and once it receives the
request it queries *MySQL* database in order to see which CSCs are covered, then it send
an HTTP response to the client with this information (in *JSON* format). The web
application is uploaded to the website http://alexmarcos.myftp.org:8080 and has been
turned on only for demonstration purposes since it uses the author’s personal computer
as a server. However, the web application could be uploaded to an official server and
have full availability.

In order to meet the **third requirement**, the last one, it has decided to make a designed
very user-friendly. based on only two parts, one for the user and other one which shows
the security situation of the company.

In the first part, the interface is formed by a dropdown in which all the security tools of
the database are listed. In this way, the user can choose the tools which correspond to
those in which he/she is interested clicking the button *ADD TOOL*, as shown in Figure
5.7.

---

**Figure 5.6:** Relation between the different entities

**Figure 5.7:** Selection of security tools in the developed tool
If the user selects a tool that was already introduced, a warning appears indicating it, as shown in Figure 5.8.

![Warning](image)

**Figure 5.8:** Warming in the developed tool

Once the user has introduced all the security tools that wants to analyze, the CSCs covered can be shown by clicking on the *Analyze* button. After the tool checks the mappings between the selected security tools and the CSCs, the tool performs a few simple calculations and finally displays the matrix explained above in a visual way, as shown in Figure 5.9

![Matrix](image)

**Figure 5.9:** Matrix showing the security situation of the selected company in the developed tool

Finally, if the user would like to know the gaps and overlaps using the selected security tools in a specific way, without having to examine the matrix, he/she could do it by clicking on the *Show/Hide Results* button. The result would be like the one shown in Figure 5.19.
5.6 Case study

Up to this point, a solution has been developed that allows through the use of a visualization tool to visualize the collected data in a meaningful way. In this way, companies can choose the right software to have the opportunity to become acceptably secure. For this, firstly a set of security controls which meets with the requirements of the thesis has been chosen, the Critical Security Controls. Secondly, a method has been developed that allows to determine which of these controls are covered by any security tool. Thirdly, a data model to store the information of the method has been designed. And finally, a visualization tool has been developed which with the use of all the previous steps allows the users to know which CSCs are covered by the set of security tools that the user or company chooses.

This section has been done in order to show a practical implementation of the developed solution through a case study.

Firstly, a representative set of security tools has been chosen, a set of 44 security tools that allows to simulate all possible possibilities. It was decided that for the set to be representative, it should meet the following two conditions:

(i) Made up of widely used security tools.
(ii) Covers all possible CSCs.

The set is listed in the Data chapter, Section 4.2, and the explanation of how the conditions have been met in the Methodology chapter, Section 2.2.

From the set of security tools, the practical use of: the developed method, the data model and the data storage and the developed visualization tool are shown in the next subsections.

5.6.1 Use of the developed method

Once the security controls set has been gathered, part of the method in Section 5.3 has been used to determine which CSC(s) is(are) covered by each of the security tools. To classify the set by following step by step the developed method would have been the ideal. However, the steps of the method that involve conducting interviews, have not been able to be carried out for the reasons explained in the Discussion chapter. Therefore, the method used has been:
1. Identification and data compilation

1.1 Inclusion

a) Does it address impacts to information integrity, confidentiality and availability?

b) Are any of its functions preventive, detective and/or corrective?

1.2 Qualitative investigation

1.2.1 Document investigation

a) Gartner reports

b) Scientific papers

c) Demo tool

d) Websites (Security tools vendors)

e) Website (Reviews, blog/forum)*

*Note: Information from this source should be extracted cautiously

1.2.2 Open-ended questions surveys*

(a) Employees of companies with information security roles

(b) Users with information security knowledge

*Note: Optional, only if it is necessary.

2. Analysis and decision

2.1 Data Analysis

2.2 Construction of the decision

3. Decision evaluation

4. Final Decision

It is important to emphasize that the tools classification using this simplification of the method causes that the results are not objective, since they have not been evaluated. Therefore, the mappings shown in the next subsections are not accurate. They should be taken as an approximation to reality, to illustrate the case study.
5.6.2 Use of the data model

In carrying out classification of each of the security tools through the method, data have been obtained and have been stored following the data model of Section 5.4. The database that has been used as support of the investigation process is Neo4j. In Figure 5.11, a screen shot of Neo4j can be seen, in which all the data collected are stored based on the data model mentioned.

In the last figure it is difficult to appreciate the data model because the data of the 44 security tools are mixed. However, the information can be filtered based on any parameter or relation. For example, in Figure 5.12 a filtering has been performed based on the Critical Security Control 15 and the data model can better understood. In the figure it can be seen the relationship of the filtered Critical Security Control (blue graph) with the Family that groups it (red graph) and with the Security Tools that cover it (yellow graphs). In turn, the security tools are related to their Providers (green graphs).

If, instead of a CSC filter, a filter is performed based on a security tool, the result is something similar to Figure 5.13, filtered based on the security tool Tripwire Configuration Compliance Manager. In this case, it is shown which CSCs are covered by the
filtered Security Tool and which is its Provider. In the same way, CSCs are grouped on the basis of the Family.

![Diagram](image-url)

**Figure 5.12:** Filtering based on a Critical Security Control.

In the previous case, it can be verified that only one of the products of the Tripwire provider has been stored. However, it is very likely that the same provider has several products, as in the examples shown in Figure 5.14.

![Diagram](image-url)

**Figure 5.13:** Filtering based on a security tool.

In case the investigator wants to know the data of the parameters established in Section 5.4 of a security tool, he/she can also do it quickly using the Neo4j tool. It is simply
needed to select the security tool. As an example of the above case, the parameters of the *StoredIQ* Security Tool of the *IBM* provider are shown in Figure 5.15.

![Diagram showing providers with different products.](image)

Figure 5.14: Example of providers with different products.

As it has been seen, the *Neo4j* database is a very useful and highly visual support tool for the investigation process. That is why, all the data obtained in this case study have been
stored in it. However, the tool has been chosen for convenience, it is not a requirement to store the data in this database. It is simply used to facilitate investigation, so each investigator can use the database most suitable for him/her.

However, it should be noted that it is a requirement that the final result of the method, i.e. the CSCs covered by the security tools analyzed, must be stored in the MySQL database. This is because it is the only database compatible with the developed visualization tool.

5.6.3 Use of the visualization tool developed

In this last part of the case study, the visualization tool developed is used with the representative mentioned set of security tools, which has been analyzed by the method of Subsection 5.6.1. This tool has been designed to help companies choose the right security tools, according to their security needs, concretely according to the CSCs. In this way, they can have the necessary software tools to cover all the CIS CSC security controls.

As an example, it is assumed the case of a company that wants to analyze what CSCs would cover with investing a set of security tools. First, it would introduce the tool set into the visualization tool, as shown in Figure 5.16.

![Tools selected]

**Tools selected**
- Nessus, Tenable Network Security
- Aruba ClearPass, Hewlett Packard Enterprise
- Splunk Enterprise
- Websense Web Filter & Security, Forcepoint
- Commvault Back up and Recovery
- Datadvantage, Varonis
- Zscaler Web security
- Centrify Identity Service
- Symantec Endpoint Protection

**Figure 5.16**: Security tools selected.

Afterwards, the organization would ask the tool to perform an analysis of the CSCs covered with the selected security tools. The visualization tool would quickly return the matrix shown in Figure 5.17. Thanks to the tool, the company could know that with the selected security tools, the CSCs 3, 11, 13, 17, 18 and 19 would not be covered and there would be an overlap in the CSCs 7, 14 and 15.
Figure 5.17: Matrix with the first security tools set.

The company could continue using the tool to check which security tool set is the most suitable for their security needs. Removing selected tools and adding unselected ones. For example, it could remove the security tools *Nessus, Datadvantage, and Zscaler Web Security* and add *Tripwire CCM, Defendpoint, and HPE Security Fortify SSC*. In this way, the situation would become that shown in Figure 5.18.

Figure 5.18: Matrix with the second security tools set.
In case the company would like to see the results in a summarized way, without using
the matrix, the gaps and the overlaps of the selected security tools set, it could do so
by clicking on the Show/Hide Results button, resulting in Figure 5.19.

Thus, in a quick and easy way, any user could know which CSCs are covered by the set
of security tools he or she chooses.

Figure 5.19: Gaps and overlaps of the second security tools set.
Chapter 6

Discussion

6.1 Introduction

This chapter discusses the work and findings from the previous chapters. It also explains the problems and limitations that have been encountered in performing the results. The chapter has been divided into three main sections along which the whole project is discussed. In the first section, Security Controls, the success or failure of having chosen the security controls of the CIS Critical Security Control guide is discussed. In the second section, Investigative Method, the viability of the developed method and its possible improvements are discussed. And in the third section, Visualization tool, the developed tool is evaluated and its benefits and limitations are discussed.

6.2 Security controls

As explained in 3.3 section, many information security guides exist today. However, in this project a guide has been sought that provides a list of security controls that complies with the requirements established at the beginning of the thesis. Several guides have been investigated, but most have not been included in literature review because they do not include a defined list of security controls. For instance, this is the case of COBIT 5, developed by ISACA, one of the most important frameworks. This framework does not have a properly detailed security controls list since it can be applied in concordance with other standards such as ISO 27001 or NIST. Proof of this is Annex H of COBIT 5 for Information Security, where the processes are mapped with the clerks and the controls of the standards mentioned [49]. So, this framework has not been considered, even if it is one of the most known. Another similar case is NIST Cyber Security Framework [50]. NIST CSF is not a set of control areas or control families. The categories and subcategories of this framework are limited to consolidating and describing security concepts as expectations to be achieved. In fact, the framework is often distinguished by not being a technician standard or a standard which provides a set of defined security controls, but rather a more holistic risk management tool. Since the goal was to get a well defined and actionable security controls list, this framework has not been analyzed either.
The three information security guides that were the most suitable to the established requirements were investigated further in depth and reflected in the Literature Review chapter. After analyzing the three guides based on the author’s criteria, it was clear from the outset that the Critical Security Controls list was the most appropriate and that the other lists of controls did not meet the criteria that the solution needs. In order to validate the decision taken, interviews were conducted to validate that the selected controls were indeed relevant for the companies.

From the interviews carried out, it was verified that 50% knew the CSCs before the interview and the other 50% did not. However, all have confirmed that they could be relevant and actionable for companies. In fact, one of the experts who has worked for years with the ISO standard confirmed that CSCs are more management-oriented controls and more actionable and less ambiguous than the controls of the ISO standard.

After collecting various information about CIS CSCs, it became clear that CIS has started updating the list frequently - at least once a year. This could be one of the reasons why the list of controls is becoming better known and more relevant. Even, some of the software vendors have begun to advertise their products based on CSCs. In other words, it does not only specify the security tools features, it is said which CSCs would be covered with the promoted security tools. This could have a growing tendency, given that this is an actionable, clear and simple list for cyber-security management, not an ambiguous list as other standards propose. If the list of CSCs was adopted little by little by all, it would have great advantages for organizations. For example doing the case study was seen that vendors often use different nomenclatures to refer to the same things. In many cases it is not known exactly what the software is covering and what not. If the CSCs list was widely adopted, the management of information security could be simpler, especially for users who are not information security experts, like most business executives.

The list of CSCs has been created by the industry for the industry, it is a non-profit community model. Based on the opinions of the interviewees and the author, the list of CSCs has the necessary elements to be relevant and to be taken as a reference. Therefore, it can be said that the choice of CSCs meets all the requirements established at the beginning of the thesis and that they have been a good choice as a result.

6.3 Investigative Method

The list of Critical Security Controls is increasingly used, which is good, as it could be useful for organizations. However, as said in the previous section, some software vendors are starting to promote their products using the CSC list, and this can be a problem since the vendors might not be truthful and exaggerate. To date, there are software vendors who claim that some of their products cover most CSCs without any objective studies to support this. The investigative method developed in this thesis can help fill this gap. The method has been designed to analyze tools objectively and with a critical mindset. That is why, the evaluation part of the method is very important. Interviews and methods to increase objectivity have been sought and used.

The method developed has been sought to be rigorous, however another requirement that has been sought is to be viable. That is, to serve as a guide for any organization and that can be carried out without many complications and without a long process. In
Section 5.3, the method has been designed to categorize a security tool. However, ideally several security tools should be categorized at the same time, so that the interviews are much more efficient and much more information can be drawn.

Unfortunately, even though a viable method has been created, in the case of study it was not possible to carry out the whole method. This has been due to the fact that, in order to have a representative set of security tools that would cover all the possibilities in the case study, it has been necessary to categorize 44 security tools. The evaluation of the 44 decisions taken, through conducting interviews and using in many cases the demo version of the tools, would have exceeded the time of the project to the point of exceeding the scope of the thesis.

Therefore, it would be interesting to carry out the whole method as a future work, to objectively categorize several security tools and store the results in a database. In this way, the database could become increasingly large and could help the companies more.

It is important to discuss the input to the investigative method. It has been decided that the input is a security control software tool, because the objective is to classify the tools in function of the CSCs that they cover, so that later this information can be reflected in the visualization tool. However, it could be thought that for a company, having a CSC as input could be more important because the enterprise would use the method to find an appropriate tool according to its security needs. But, it should be noted that this is not the purpose of the method, but rather the purpose of the developed visualization tool. In fact, the tool as input could also be important for a company. If the company already has some security tools installed and want to know how much of the CSCs are covered with them and what other tools the organization would want to buy.

Another aspect that should be discussed in this section corresponds to the fact that the method has been designed so that the security tools are classified according to whether they cover the CSC or do not cover it. The possibility of a CSC being partially covered by a tool has not been taken into account. However, according to the responses of the respondents and the research carried out in the case study, it has been found that in many cases, a single product can not fully implement the the CSC in its entirety. This is because a single CSC control can be divided into several sub-controls. Therefore, considering partiality would imply analyzing each sub-control of CSCs, exceeding the scope of the thesis.

In order to facilitate future work, the method has been designed in such a way the analysis of the CSC sub-controls supposes only a step further and it is not necessary to design another method from the outset. That is the reason why the method has been designed with the condition that in the case that a security tool partially covers a CSC, the security tool is categorized as that it cover the CSC and not as that it does not cover it.

In this way, once the security tools have been categorized according to the method, in future investigations it will be possible to analyze which sub-controls of the covered CSCs (information obtained according to the current method) are covered and which are not covered.

Based on the research carried out in this thesis and the responses of the respondents, it can be affirmed no similar methods were found.
6.4 Visualization tool

In the previous section the method was developed for it to be used by any company. However, some companies, mainly small companies, might find that carrying out the method can be demanding. This is because their needs are smaller and therefore, they might believe that the results are not worth the time and resources spent using the investigative method. This is the case for one of the companies interviewed whose representative commented that given its business needs and its size, it was not reasonable to follow any rigorous method to choose their software. However, the respondent indicated that it would be very useful to have an extensive database which contains objective information from such a rigorous method. Thus, although some companies cannot use the method themselves, they could take advantage of the information obtained using it by other companies. Therefore, the developed visualization tool is very useful both for those companies who have not carried out the method and want to know which CSCs are covered by different security tools and for those who have carried out the method and want to see the results organized in a visual way. An additional perspective would be to use the visualization tool, for the companies that already have some tools installed to identify gaps in the CSCs usage.

However, it is very important to note that because of complexity of software use and security, it can be only a supportive tool to choose the right software. It is not possible to learn anything about the actual security situation of the company. The security information in a company depends on many variables and many measures are necessary besides the software. This tool can be used only as a support to know which controls are covered by the security tools. Even if the tool indicates that with a set of security tools all CSCs are covered, it does not mean that the company can be secure, but has the necessary software to be able to become secure.

In the case of Figure 5.18, one can make the mistake of thinking that after investing into 9 tools the company would be secure and this need not be so. For example, in case of a very large company, it would take several security tools to fully cover each of the CSCs. Or, another example, in case of a small company in which its value lies on its website. This company would need many more security tools to fully implement the CSC 7. Therefore, the visualization tool is only an aid to know in a more objective and clear way what the security software does. Each company must use the tool responsibly and take into consideration other factors such as its business needs.

For future work, it would be good to add the sub-controls to the visualization tool to be able to see what tools to implement with greater precision.
Chapter 7

Conclusions and Future Work

7.1 Conclusions

It is generally difficult for companies to decide on which software to invest in, since in many cases the information of the specifications of security tools is not clearly provided by the software providers or it is exaggerated to improve the promotion of the product. Therefore, it was decided to develop a solution that would help companies to choose the right software based on their security needs, in order to they could have the opportunity to become acceptably secure. It is important to emphasize that, as has been indicated throughout the thesis, with the last sentence it is not being said that using the right software companies will be acceptably secure, but they will have the opportunity to become acceptably secure. In addition to software, companies must consider many other security measures that have not been addressed in this thesis.

In order to fulfill the purpose of the thesis, a set of 4 concise and measurable goals were established as well as a fifth objective, which was proposed to carry out a case study to show practically everything that was developed in the other 4 controls. Throughout the thesis, to meet these goals has been tried structuring them in 5 phases, one per goal.

In the first phase, an investigation was conducted to choose a list of security controls that would include all possible security requirements of any organization. From this investigation, it was concluded that the list of security controls proposed by the CIS Critical Security Controls guide was the most appropriate one, since it met the requirements of first established goal of being frequently updated, relevant to the industry and well defined and actionable. In addition, thanks to the case study of the fifth phase and the interviews conducted to security experts, it was possible to validate that the controls chosen were indeed relevant for the companies. In fact, it could be verified that many current software vendors have begun to promote their products indicating which CSCs they cover.

The problem with the last assertion is that software vendors may exaggerate their products, promoting that they cover more CSCs than they cover. Therefore, in order to develop guidelines to help classify any safety tool according to CSCs objectively, it was essential to carry out the second phase. In this phase, based on an investigation carried out, interviews conducted to security experts and the experience gained in the development of the thesis, a investigative method was developed, which establishes the mentioned guidelines in a precise way. It has had an improvement process based on the
opinion of the respondents and the case the study, in which the method was used to categorize 44 security tools. The method has been designed in such a way to be viable, that it can be carried out by any company because is realistic. But also it has been designed to be rigorous, to obtain objective results.

The rigor of the method is very important, since the objective is that the data obtained be used by the company that has carried out the method, but that can also be used by other companies or users in the future. Therefore, the third phase was necessary. In it, a data model was designed so that all information obtained through the method can be stored in a database in a clear and orderly manner. This will allow future researchers to check the data of other researchers and add new data. In this way, the database can become larger and more users can benefit from objective results.

The previous phase allows to store in a database the mapping data between the security tools analyzed with the method and the CSCs covered by them. However, in order to facilitate to companies the process of choosing software based on their security needs, the fourth phase was carried out. In this phase a tool was developed that visually shows the mapping through a matrix. In this way the result is shown in a simple way, thus meeting the requirement of simplicity established in the fourth goal. On the other hand, the tool was developed as a simple web tool, allowing to meet the other two requirements established, ubiquity and user-friendly interface.

This section of conclusions verifies that all the goals and requirements established to carry out the purpose have been fulfilled, within the established limitations. However, in order to show with practical examples everything done in the thesis, the fifth and final phase was carried out. In this, a case study was performed, as has been indicated above. This has allowed to achieve two things. First, give the reader a clearer vision of everything developed during the project. And secondly, validate with real data that the project developed is viable and , from an experimental perspective, that the goals have been met.

### 7.2 Future Work

In the previous section, it has been concluded that the goals and requirements have been met, within the established limitations. However, as discussed in Chapter 6, if it was not for the limitations of the scope of the thesis, in some lines would have deepened more. Since this has not been possible, they are proposed in this section as future works.

(i) The first proposal as future work is to carry out the method developed in a rigorous way, step by step, to categorize as many security tools as possible. In the case study, several tools have been categorized, but due to the limitations mentioned in the discussion chapter, it has not been possible to evaluate them and therefore lack the necessary rigor. The aim is the database has as much data as possible, so that a wide variety of security tools can be selected in the visualization tool developed. To do this, it should be classified with the method the more tools the better.

(ii) The second proposal is to improve the method developed, including the sub-controls of the CSCs in the categorization. That is, to design the method in that way that once a security tool has been categorized based on the CSCs it
covers, to be possible determine which sub-controls of the covered CSCs would be complied by the security tool and which not.

(iii) The third and final proposal as future work corresponds to improving the visualization tool including also the sub-controls of the CSCs. Once the second proposal has been made, the database will have the necessary information. In this way, it will be possible to add the sub-controls to the visualization tool to be able to see what tools to implement with greater precision. The result should be the same as now, a simple web tool, ubiquitous and with a user-friendly interface, but with greater precision.
Bibliography


Bibliography

[34] NIST. NIST SPECIAL PUBLICATIONS (SP), 2017. URL http://csrc.nist.gov/publications/PubsSPs.html.


Appendix A

ISO/IEC 27002:2013

Following there are the 14 sections, or control areas, of the ISO / IEC 27002: 2013 standard as well as their 35 main security controls category. In each security control category is stated the control objective that is to be achieved according to the standard [28]. In the standard there are 18 sections but the control areas start in the section 5 and they end in the section 18.

A.1 Sections and main security controls

5. Security Policy Management

5.1 Provide management direction and support
Objective: To provide management direction and support for information security activities.

6. Corporate Security Management

6.1 Establish an internal information security organization
Objective: To establish a framework to manage information security within your organization.

6.2 Protect your organization’s mobile devices and telework
Objective: To ensure the security of mobile devices and telework (work done away from the office at home or elsewhere).

7. Personnel Security Management

7.1 Emphasize security prior to employment
Objective: To ensure that prospective employees and contractors are suitable for their future roles.

7.2 Emphasize security during employment
Objective: To ensure that employees and contractors meet their information security responsibilities.
7.3 Emphasize security at termination of employment
Objective: To protect your organization’s interests whenever personnel terminations occur or responsibilities change.

8. Organizational Asset Management

8.1 Establish responsibility for corporate assets
Objective: To protect assets associated with information and information processing facilities.

8.2 Develop an information classification scheme
Objective: To provide an appropriate level of protection for your organization’s information.

8.3 Control how physical media are handled
Objective: To protect information by preventing unauthorized disclosure, modification, removal, or destruction of storage media.

9. Information Access Management

9.1 Respect business requirements
Objective: To control access to your organization’s information and information processing facilities.

9.2 Manage all user access rights
Objective: To ensure that only authorized users gain access to your organization’s systems and services.

9.3 Protect user authentication
Objective: To make your users accountable for safeguarding their own secret authentication information.

9.4 Control access to systems
Objective: To prevent unauthorized access to your organization’s information, systems, and applications.

10. Cryptography Policy Management

10.1 Control the use of cryptographic controls and keys
Objective: To use cryptography to protect the confidentiality, authenticity, and integrity of information.

11. Physical Security Management

11.1 Establish secure areas to protect assets
Objective: To prevent unauthorized physical access to information and information processing facilities.

11.2 Protect your organization’s equipment
Objective: To prevent the loss, theft, damage, or compromise of equipment and the operational interruptions that can occur.

12. Operational Security Management
12.1 Establish procedures and responsibilities
Objective: To ensure that information processing facilities are operated correctly and securely.

12.2 Protect your organization from malware
Objective: To protect information and information processing facilities against malware.

12.3 Make backup copies on a regular basis
Objective: To prevent the loss of data, information, software, and systems.

12.4 Use logs to record security events
Objective: To record information security events and collect suitable evidence.

12.5 Control your operational software
Objective: To protect the integrity of your organization’s operational systems.

12.6 Address your technical vulnerabilities
Objective: To prevent the exploitation of technical vulnerabilities.

12.7 Minimize the impact of audit activities
Objective: To minimize the impact that audit activities could have on systems and processes.


13.1 Protect networks and facilities
Objective: To protect information in networks and to safeguard the information processing facilities that support them.

13.2 Protect information transfers
Objective: To protect information while it’s being transferred both within and between the organization and external entities.


14.1 Make security an inherent part of information systems
Objective: To ensure that security is an integral part of information systems and is maintained throughout the entire lifecycle.

14.2 Protect and control system development activities
Objective: To ensure that security is designed into information systems and implemented throughout the development lifecycle.

14.3 Safeguard data used for system testing purposes
Objective: To protect and control the selection and use of data and information when it is used for system testing purposes.

15. Supplier Relationship Management

15.1 Establish security agreements with suppliers
Objective: To protect corporate information and assets that are accessible by suppliers.

15.2 Manage supplier security and service delivery
Objective: To ensure that suppliers provide the agreed upon level of service and security.

16. Security Incident Management
16.1 Identify and respond to information security incidents

*Objective:* To ensure that information security incidents are managed effectively and consistently.

17. Security Continuity Management

17.1 Establish information security continuity controls

*Objective:* To make information security continuity an integral part of business continuity management.

17.2 Build redundancies into information processing facilities

*Objective:* To ensure that information processing facilities will be available during a disaster or crisis.

18. Security Compliance Management

18.1 Comply with legal security requirements

*Objective:* To comply with legal, statutory, regulatory, and contractual information security obligations and requirements.

18.2 Carry out security compliance reviews

*Objective:* To ensure that information security is implemented and operated in accordance with policies and procedures.
Appendix B

NIST Special Publication (SP) 800-53, Revision 4

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, the Security controls of the mentioned standard are organized into eighteen families. The security control structure consists of the following components:

(i) Control section: prescribes specific security-related activities or actions to be carried out by organizations or by information systems.

(ii) Supplemental guidance section: provides non-prescriptive, additional information for a specific security control.

(iii) Control enhancements section: provides statements of security capability to:
   (a) Add functionality/specificity to a control.
   (b) And/or increase the strength of a control.

(iv) References section: includes a list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines (e.g., OMB Circulars/Memoranda, Homeland Security Presidential Directives, FIPS Publications, and NIST Special Publications) that are relevant to a particular security control.

(v) Priority and baseline allocation section: provides:
   (a) The recommended priority codes used for sequencing decisions during security control implementation
   (b) And the initial allocation of security controls and control enhancements to the baselines.

Due to the extension, not all the controls will be listed. Only families will be listed and briefly described below [51].
B.1 Families

AC - Access Control
The Access Control family is a series of controls that determine the setting used for limiting access to systems and information stored on the systems. Some of the controls provide guidance on account management and privilege assignments. The guidance provided helps to address the assignment of roles and define business functions. Other settings covered include login time, screen saver requirements, and similar activity-based controls. The guidance for users that require access to system level resources or administrative rights is discussed in the controls. Developers and program managers can use these controls to understand session timeout settings and recommendations of least privilege.

AU - Audit and Accountability
The Audit and Accountability family provides the mechanism to record policy violations and related activities. The control provides guidance on log retention policies and configurations. The family also provides information on what data should be retained in each log. Time synchronization is important when performing incident response. Data collected using audit and accountability methods should use a common NTP server, and other guidelines related to timestamps are covered in this family.

AT - Awareness and Training
The Awareness and Training control assists with measuring the control and effectiveness of security controls. The metrics provide visibility into how well security controls protect systems and how well users understand the controls in use.

CM - Configuration Management
The Configuration Management family focuses on baseline establishment and identifying the minimal software installations. Many of the important details concerning change control and configuration management are described in this family.

CP - Contingency Planning
The Contingency Planning family contains many of the auditable settings for backup and recovery of systems. The settings include detecting the backup of sensitive data, scheduling backups, and other related settings.

AI - Identification and Authentication
The Identification and Authentication family primarily focuses on the configuration settings concerned with authentication systems. The controls provide detailed guidance on tracking users employed by the organization, as well as for guests, contractors, shared accounts, and service accounts. Some settings will also validate the configuration of RADIUS, TACACS, and two-factor authentication.

IR - Incident Response
The Incident Response family identifies auditable settings to support incident response efforts. The controls most often related to this family pertain to log retention settings. Windows computers are known for overwriting event logs, and therefore setting a maximum log size could be beneficial for incident response.

MA - Maintenance
The Maintenance family provides guidance on how to perform, document, and audit records of maintenance and repairs on information systems. The organization should
track the maintenance activities of support personnel regardless of the location of equipment and personnel. Guidance that tracks impacted security controls is also discussed in this family.

**MP - Media Protection**
The Media Protection family provides information on how to maintain the security of digital media. By offering guidance on how to configure media controls, classification markings, storage policies, and usage, this family can assist an organization in using digital media more securely.

**PS - Personnel Security**
The Personnel Security family provides guidance on handling personnel-related issues such as termination, promotion, transfer, and other related tasks. The audit checks look for common settings that can assist with these tasks.

**PE - Physical and Environmental Protection**
The Physical and Environmental Protection family provides guidance on physical security requirements. Using logs from digital locks and other physical controls connected to network, the Log Correlation Engine (LCE) can correlate the events, which analysts can monitor for anomalies. Information leakage is also addressed in this family, providing guidance on how to address signal leakage and other electronic communication controls.

**PL - Planning**
The Planning family provides guidance on information security architecture and describes the overall philosophy, requirements, and approach organizations take with regard to protecting the confidentiality, integrity, and availability of information. The focus of this family is to illustrate how the security controls and control enhancements meet security requirements, but do not provide detailed technical descriptions of the specific design or implementation of the controls/enhancements. By setting interfaces to a security context with the appropriate controls, the organization can illustrate planning for the required security levels.

**PM - Program Management**
The Program Management family provides guidance on facilitating compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Additionally, the audits in this family provide a vehicle for the organization to document all of the security controls in a central repository.

**RA - Risk Assessment**
The Risk Assessment family provides guidance on the requirements to perform risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the nation based on the operation and use of information systems.

**CA - Security Assessment and Authorization**
The Security Assessment and Authorization family provides guidance for the effective implementation of security controls and enhancements. Guidance for corrective actions and related milestones are reported in this family. Other information with respect to penetration testing and other internal systems audits are described in this family.

**SC - System and Communications Protection**
The System and Communications Protection family provides guidance on how to implement protected communications for a system. One aspect is the separation of duties,
such as making sure the administrative interface is not part of the regular user interface. Other controls are limiting direct hardware access, memory address space controls, intrusion detection, and other methods of monitoring system resources.

**SI - System and Information Integrity**
The System and Information Integrity family provides guidance on monitoring information systems affected by announced software vulnerabilities, email vulnerabilities (spam), error handling, memory protection, output filtering, and many other areas of security. Many of these audit checks will need to be customized and should be reviewed by the organization.

**SA - System and Services Acquisition**
The System and Services Acquisition family provides guidance on using service-based software such as Telnet, HTTP, and other services. Tenable audit files look for some services that are known to be unauthorized, such as Telnet. However, the organization should review content to ensure authorized services are detected. These settings should be reviewed and customized to meet the local policies for the organization.
Appendix C

The CIS Critical Security Controls for Effective Cyber Defense

The 20 Critical Security Controls are presented in the official publication [41] using the same structure, which includes the following elements:

- A description of the importance of the Control, which is attached below.
- The sub-controls that organizations have to take to implement the specific control.
- Procedures and Tools that allow implementation and automation.
- Sample Entity Relationship Diagrams that show components of implementation.

C.1 Critical Security Controls

- **CSC #1. INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES:** Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

- **CSC #2. INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE:** Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

- **CSC #3. SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE:** Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
• **CSC #4. CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION:** Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

• **CSC #5. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES:** The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

• **CSC #6. MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS:** Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

• **CSC #7. EMAIL AND WEB BROWSER PROTECTIONS:** Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

• **CSC #8. MALWARE DEFENSES:** Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

• **CSC #9. LIMITATION AND CONTROL OF NETWORK PORTS:** Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

• **CSC #10. DATA RECOVERY CAPABILITY:** The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

• **CSC #11. SECURE CONFIGURATIONS FOR NETWORK DEVICES:** Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

• **CSC #12. BOUNDARY DEFENSE:** Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

• **CSC #13. DATA PROTECTION:** The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

• **CSC #14. CONTROLLED ACCESS BASED ON THE NEED TO KNOW:** The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

• **CSC #15. WIRELESS ACCESS CONTROL:** The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.
• **CSC #16. ACCOUNT MONITORING AND CONTROL:** Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

• **CSC #17. SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS:** For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

• **CSC #18. APPLICATION SOFTWARE SECURITY:** Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

• **CSC #19. INCIDENT RESPONSES AND MANAGEMENT:** Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.

• **CSC #20. PENETRATION TESTS AND RED TEAM EXERCISES:** Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.
Appendix D

Interview Template

Company:
Corporate function:

The Critical Security Controls are supported by SANS with training, certifications and research. They are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today’s most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

CSC 1. INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES
CSC 2. INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE
CSC 3. SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE
CSC 4. CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION
CSC 5. CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES
CSC 6. MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS
CSC 7. EMAIL AND WEB BROWSER PROTECTIONS
CSC 8. MALWARE DEFENSES
CSC 9. LIMITATION AND CONTROL OF NETWORK PORTS
CSC 10. DATA RECOVERY CAPABILITY
CSC 11. SECURE CONFIGURATIONS FOR NETWORK DEVICES
CSC 12. BOUNDARY DEFENSE
CSC 13. DATA PROTECTION
CSC 14. CONTROLLED ACCESS BASED ON THE NEED TO KNOW
CSC 15. WIRELESS ACCESS CONTROL
CSC 16. ACCOUNT MONITORING AND CONTROL
CSC 17. SECURITY SKILLS ASSESSMENT AND APPROPRIATE TRAINING TO FILL GAPS
CSC 18. APPLICATION SOFTWARE SECURITY
CSC 19. INCIDENT RESPONSES AND MANAGEMENT
CSC 20. PENETRATION TESTS AND RED TEAM EXERCISES
• Are you familiar with the 20 Critical Security Controls?

• Answer the following questions related with the 20 CSCs. In case of using security tools to cover the corresponding CSC, please indicate them. Indicate in the comment section if you think the control is relevant to your company and feel free to add any other relevant comment.

**Table D.1: Questions about the Critical Security Controls 1/4**

<table>
<thead>
<tr>
<th>Questions</th>
<th>Select one of the two options:</th>
<th>if security tools are used indicate them:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does your company control authorized and unauthorized hardware devices on the networks of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Does your company control authorized and unauthorized software on the networks of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Does your company establish a rigorous security configuration of the laptops, servers and workstations of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Does your company assess and take action on new information in order to identify, vulnerabilities, remediate and minimize the window of opportunity for attackers?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Does your company control the use, assignment and configuration of administrative privileges on the computers, networks and applications of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Does your company collect, manage and analyze audit logs of events that could help detect, understand, or recover from an attack?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table D.2: Questions about the Critical Security Controls 2/4

<table>
<thead>
<tr>
<th>Questions</th>
<th>Select one of the two options:</th>
<th>if security tools are used indicate them:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Does your company use any kind of protection for the web browsers and email clients of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Does your company control the installation, spread and execution of malicious code at multiple points of your organization, like end-user devices, email attachments, web pages, cloud services, user actions or removable media?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Does your company manage the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Has your organization a way to properly back up critical information with a proven methodology for timely recovery of it? * In case that, for example, attackers make significant changes to configurations and software of your organization.</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Does your company establish a rigorous security configuration of network infrastructure devices of your organization?</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Does your company detect/prevent/correct the flow of information that is transferred by networks of different trust levels? (with a focus on security-damaging data)</td>
<td>□Yes □No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table D.3: Questions about the Critical Security Controls 3/4

<table>
<thead>
<tr>
<th>Questions</th>
<th>Select one of the two options:</th>
<th>if security tools are used indicate them:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Has your company a way to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information of your organization?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Has your company a way to control secure access to critical assets according to the formal determination of which persons, computers and applications have a need and right to access these critical assets?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Has your company a way to control the security use of wireless local area networks (LANS), access points, and wireless client systems of your organization?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Does your company manage the life cycle of system and application accounts (their creation, use, dormancy, deletion...), in order to minimize opportunities for attackers to leverage them?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Does your company assess the specific knowledge and skills needed of the employees of your organization to reduce the security gaps, through developing policies, organizational plannings, trainings and awareness programs?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Questions</th>
<th>Select one of the two options:</th>
<th>if security tools are used indicate them:</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>18. Does your company manage the security life cycle of all in-house developed and acquired software to prevent, detect and correct security weaknesses?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Has your company an incident response infrastructure (e.g., plans, defined roles, management oversight...) for quickly discovering an attack and then eradicating the attacker’s presence and restoring the integrity of the network of your organization?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Does your organization test the overall strength defenses (the technology, the processes and the people) by simulating the objectives and actions of an attacker?</td>
<td>□ Yes □ No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Which protocol, or criteria, does your company follow to choose the security tools according to its security needs?

- Analyze the method draft proposed to categorize any security on function of the CSC(s) covered by it.

1. To collected reliable information from the chosen tool through:

   1.1 Research from different reliable sources:
      a) Websites (vendors)
      b) Whitepapers
      c) Scientific papers
1.2 Interviews asking about the CSCs covered by the chosen tool, conducted to cyber-security professionals:
   a) Companies
   b) Governments
   c) Individuals

2. To analyze all the information collected and take a decision of which CSC(s) is (are) covered by the chosen tool.

3. Evaluate the decision using the trial version of the chosen tool.

4. Take a final decision based on the evaluation done in the previous step. The possible options are:

   4.1 The security tool covers the CSC(s) indicated in the decision. Results are stored.

   4.2 The security tool does not cover the CSC(s) indicated in the decision. The method is done again, taking advantage of what has been learned.

---

**Figure D.1:** Flowchart of the method draft.
• What would you change from the method draft? What would you add?
Appendix E

Security Tools Collected
### Table E.1: Representative set of security tools

<table>
<thead>
<tr>
<th>CSC</th>
<th>Security Tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 1</td>
<td>Identity Services Engine, Cisco / Aruba ClearPass, Hewlett Packard Enterprise / CounterACT, ForeScout Technologies</td>
</tr>
<tr>
<td>CSC 2</td>
<td>Powerbroker Privileged Access Management, BeyondTrust / Defendpoint, Aveco / Nessus, Tenable Network Security</td>
</tr>
<tr>
<td>CSC 3</td>
<td>Tripwire Configuration Compliance Manager, Tripwire</td>
</tr>
<tr>
<td>CSC 4</td>
<td>Nexpose, Rapid7 / Qualys Vulnerability Management, Qualys / Metasploit, Rapid7</td>
</tr>
<tr>
<td>CSC 5</td>
<td>CA ControlMinder, CA Technologies</td>
</tr>
<tr>
<td>CSC 6</td>
<td>LOGStorm, BlackStratus / LogRhythm Security Intelligence, LogRhythm / ManageEngine EventLog Analyzer, Zoho Corporation / QRadar Security Intelligence, IBM / Splunk Enterprise, Splunk / SIEMStorm, BlackStratus</td>
</tr>
<tr>
<td>CSC 7</td>
<td>Websense® Web Filter &amp; Security, Forcepoint / (Blue Coat) Advanced Secure Gateway, Symantec / Zscaler Web security, Zscaler</td>
</tr>
<tr>
<td>CSC 8</td>
<td>Trend Micro OfficeScan, Trend Micro / CrowdStrike Falcon, CrowdStrike / Symantec Endpoint Protection, Symantec</td>
</tr>
<tr>
<td>CSC 9</td>
<td>Nmap, Nmap</td>
</tr>
<tr>
<td>CSC 10</td>
<td>Commvault Back up and Recovery, Commvault / Data Protection Suite, EMC / IBM Spectrum Protect, IBM</td>
</tr>
<tr>
<td>CSC 11</td>
<td>Manageengine Network Configuration Manager, Zoho Corporation</td>
</tr>
<tr>
<td>CSC 12</td>
<td>Fortinet Security Fabric, Fortinet / Snort, Sourcefire (Cisco)</td>
</tr>
<tr>
<td>CSC 13</td>
<td>Triton AP-Data, Forcepoint / Symantec Endpoint Encryption, Symantec</td>
</tr>
<tr>
<td>CSC 14</td>
<td>Datadvantage, Varonis / HPE ControlPoint, Hewlett Packard Enterprise / StoredIQ, IBM</td>
</tr>
<tr>
<td>CSC 15</td>
<td>Extreme Access Control, Extreme Networks</td>
</tr>
<tr>
<td>CSC 16</td>
<td>Okta Adaptive Multi-Factor Authentication, Okta / Centrify Identity Service, Centrify</td>
</tr>
<tr>
<td>CSC 17</td>
<td></td>
</tr>
<tr>
<td>CSC 18</td>
<td>Veracode Static Analysis (SAST), Veracode / Veracode Dinamyc Analysis ( DAST), Veracode</td>
</tr>
<tr>
<td>CSC 19</td>
<td>The Resilient Incident Response Platform (IRP), IBM</td>
</tr>
<tr>
<td>CSC 20</td>
<td>Kali Linux, Kali Linux / HPE Security Fortify Software Security Center (SSC), Hewlett Packard Enterprise /CORE Impact, Core Security</td>
</tr>
</tbody>
</table>
Appendix F

Survey Template Investigative Method, Open-ended questions

Company: 
Department: 
Name interviewee: 
Corporate function: 
Security tool analyzed:

Table F.1: Questions about the security tool 1/3

<table>
<thead>
<tr>
<th>Question</th>
<th>Select one of the two options:</th>
<th>Could you explain the reason(s) of your answer?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the security tool control authorized and unauthorized hardware devices on the networks?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>2. Does the security tool control authorized and unauthorized software on the networks?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>3. Does the security tool establish a rigorous security configuration of the laptops, servers and workstations?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>4. Does the security tool assess and take action on new information in order to identify, vulnerabilities, remediate and minimize the window of opportunity for attackers?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>5. Does the security tool control the use, assignment and configuration of administrative privileges on the computers, networks and applications?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
</tbody>
</table>
### Table F.2: Questions about the security tool 2/3

<table>
<thead>
<tr>
<th>Question</th>
<th>Select one of the two options:</th>
<th>Could you explain the reason(s) of your answer?</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Does the security tool collect, manage and analyze audit logs of events that could help detect, understand, or recover from an attack?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>7. Does the security tool use any kind of protection for the web browsers and email clients?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>8. Does the security tool control the installation, spread and execution of malicious code at multiple points, like end-user devices, email attachments, web pages, cloud services, user actions or removable media?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>9. Does the security tool manage the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>10. Does the security tool have a way to properly back up critical information with a proven methodology for timely recovery of it? <em>In case that, for example, attackers make significant changes to configurations and software.</em></td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>11. Does the security tool establish a rigorous security configuration of network infrastructure devices?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>12. Does the security tool detect/prevent/correct the flow of information that is transferred by networks of different trust levels? (with a focus on security-damaging data)</td>
<td>□Yes  □No</td>
<td></td>
</tr>
<tr>
<td>13. Does the security tool have a way to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information?</td>
<td>□Yes  □No</td>
<td></td>
</tr>
</tbody>
</table>
### Table F.3: Questions about the security tool 3/3

<table>
<thead>
<tr>
<th>Question</th>
<th>Select one of the two options:</th>
<th>Could you explain the reason(s) of your answer?</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. Does the security tool have a way to control secure access to critical assets according to the formal determination of which persons, computers and applications have a need and right to access these critical assets?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>15. Does the security tool have a way to control the security use of wireless local area networks (LANS), access points, and wireless client systems?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>16. Does the security tool manage the life cycle of system and application accounts (their creation, use, dormancy, deletion...), in order to minimize opportunities for attackers to leverage them?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>17. Does the security tool assess the specific knowledge and skills needed of the employees to reduce the security gaps, through developing policies, organizational plannings, trainings and awareness programs?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>18. Does the security tool manage the security life cycle of all in-house developed and acquired software to prevent, detect and correct security weaknesses?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>19. Does the security tool have an incident response infrastructure (e.g., plans, defined roles, management oversight...) for quickly discovering an attack and then eradicating the attacker’s presence and restoring the integrity of the network?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
<tr>
<td>20. Does the security tool test the overall strength defenses (the technology, the processes and the people) by simulating the objectives and actions of an attacker?</td>
<td>□ Yes □ No</td>
<td></td>
</tr>
</tbody>
</table>
Appendix G

Survey Template 2 Investigative Method, Open-ended questions

Company: 
Department: 
Name interviewee: 
Corporate function: 
Security tool analyzed: 

- Answer the question(s) of the Table G.1. Keep in mind that if you consider that the control is partially covered by the tool, the response should be Yes. Remember that you are free to add any relevant comments.

Table G.1: Question(s) about the hypothesis(es)

<table>
<thead>
<tr>
<th>Question:</th>
<th>Select an option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do you think the Security Tool A covers the Critical Security Control X ?</td>
<td>□Yes □No</td>
</tr>
<tr>
<td>2. Do you think the Security Tool A covers the Critical Security Control Y ?</td>
<td>□Yes □No</td>
</tr>
<tr>
<td>3. Do you think the Security Tool A covers the Critical Security Control Z ?</td>
<td>□Yes □No</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>