UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

DECISION SUPPORT FOR SELECTING INFORMATION SECURITY CONTROLS

Luís Miguel Sousa Trindade de Almeida

Mestrado em Informática

Dissertação orientada por:
Professora Doutora Ana Luísa Do Carmo Correia Respício

2018

Acknowledgements

First, I would like to thank Prof. Ana Respício for allowing me to have done my dissertation under her supervision. Her patience, guidance and availability along the entire project is something that I will never forget.

I would like to express a word of gratitude to all my colleagues from *Faculdade de Ciências da Universidade de Lisboa* for all the support they gave during the entire master's degree.

Ana, no words can express how you helped me through this journey. Thank you for always believing in me, even when I didn't.

To my Father and Mother, who are my pillar, I'm grateful for their unconditional love and support through my entire academic journey. I would not be the person I am today without both of you.

Lastly but not least, I would like to thank from the bottom of my heart to my grandfather António for all the support that he gave me in the beginning of my academic journey. Wherever you are, I hope that I made you proud.

This work is dedicated to My Father, My Mother and my girlfriend.

Resumo

A evolução da Humanidade permitiu várias mudanças quer a nível social, tecnológico e até mesmo organizacional. Com o aparecimento da Internet, as Tecnologias de Informação (TI) assumem um peso bastante significativo dentro de uma empresa porque se encontram inseridas em todos os departamentos da organização e detêm um papel muito importante quer em processos internos como externos. Para além disso, as Tecnologias de Informação têm vindo a criar novos processos de negócio e de partilha de informação que auxiliam a gestão de informação e a tomada de decisão.

Com estas evoluções tecnológicas, surgiu assim por parte das organizações a necessidade de se utilizarem computadores com uma maior capacidade de processamento, de armazenamento e de consulta de operações, por forma a que o seu desempenho e funcionamento possam ir ao encontro das mudanças tecnológicas. Na Era globalizada e competitiva em que vivemos, as empresas e organizações tendem cada vez mais a valorizar a informação crítica da empresa, assim como os seus ativos, tendo como principal objetivo a manutenção e aperfeiçoamento de forma contínua dos seus processos de negócios. Assim, existe a necessidade de manter uma estrutura informática forte e também uma equipa competente e atualizada que consiga ir ao encontro dos objetivos propostos pela organização e responder às necessidades que possam surgir na segurança de informação.

A valorização de informação, de ativos e de processos de negócio pode ser gerida com base em referências internacionais que permitam orientar diversos procedimentos na área de gestão de segurança de informação, tema esse que tem vindo a ganhar uma maior relevância quer junto de pequenas, como de grandes organizações. Devido a esse facto, estas referências internacionais têm aos poucos deixado de ser encaradas como simples Normas mas também como instrumentos diferenciadores e capazes de proporcionar confiabilidade no que diz respeito ao apoio à decisão para todos os *stakeholders* envolvidos no negócio.

As novas tecnologias têm dado espaço para se implementarem vários mecanismos que suportem a tomada de decisão e contribuam para um bom desempenho de uma empresa. A utilização de sistemas de suporte à decisão pode auxiliar as organizações na redução de custos para filtrar informação que possa representar uma vantagem

competitiva nos vários processos de negócio. Com isto, na presente dissertação é dado ênfase aos diversos sistemas que permitem auxiliar os gestores de uma organização na tomada de decisão. O trabalho desenvolvido relaciona-se com o *Model-Driven*, uma vez que é utilizado um modelo de otimização tendo em conta dois objetivos. Para além disso é ainda utilizado um conjunto de informações e parâmetros que serão definidos por parte do utilizador.

A decisão de uma empresa sobre quais os controlos que esta deve adotar, por forma a que os requisitos que se pretendam implementar na segurança de tecnologias de informação sejam aqueles que tragam melhores resultados e benefícios à empresa, é um problema bastante recorrente nos dias de hoje, pelo facto de ser um processo moroso e complicado, com um orçamento previamente estipulado que se pretende que não seja elevado.

Este trabalho propõe uma *framework* que permite auxiliar a tomada de decisão de uma organização na seleção de controlos para a mitigação de vulnerabilidades que possam comprometer o desempenho e o objetivo de diversos processos de negócio. A *framework* tem como base um conjunto de controlos de segurança, que se encontram sugeridos no presente portfólio e que podem ser de natureza variada, como por exemplo controlos de *hardware*, onde estão incluídos componentes como *Firewalls* ou controladores de acesso, e também por um conjunto de políticas, procedimentos e ações de formação.

A *framework* implementada rege-se pelas normas internacionais ISO / IEC 27001:2013 e ISO / IEC 27002:2013 por forma a garantir uma correta proteção de informação e de dados de uma organização.

A adoção da norma ISO/IEC 27001:2013 tem como principal objetivo garantir que os princípios que ela suporta são cumpridos, oferecendo assim aos vários *Stakeholders* de um negócio conforto no que diz respeito à Segurança de Informação. Dito isto, esta norma foi utilizada em vários domínios para estabelecer, manter e melhorar de forma contínua um Sistema de Gestão de Informação de uma organização. Por outro lado, a norma ISO/IEC 27002:2013 apresenta um conjunto de recomendações e práticas que devem ser adotadas na gestão da Segurança de Informação, conjunto esse que suporta a *framework* criada na escolha de controlos que devem ser implementados.

A revisão bibliográfica realizada sobre as duas normas acima mencionadas, focou-se essencialmente nas cláusulas nove, doze e treze, que são respetivamente denominadas de Controlo de Acessos, Segurança de Operações e Segurança de Comunicações. Após ser estabelecida uma relação entre as duas normas e respetivas cláusulas, foi possível discriminar um conjunto de possíveis vulnerabilidades que possam ocorrer dentro de uma organização, assim como a definição de um conjunto de produtos de segurança informática que conseguem mitigar essas mesmas vulnerabilidades. Para isso, foram consideradas algumas empresas que comercializam produtos informáticos.

Como base no que foi descrito anteriormente, foi desenvolvido um modelo que permite suportar a decisão para a escolha de controlos que mitiguem vulnerabilidades identificadas, tendo como base duas premissas: A otimização (minimização) de custos de investimento e a minimização da perda esperada (*expected loss*) caso haja um ataque bem-sucedido.

A otimização de custos permite que seja efetuada automaticamente a escolha de produtos que tenham um custo de mercado mais baixo, mas que consigam realizar a mitigação de vulnerabilidades identificadas. Já a minimização do *expected loss* permite que a organização consiga definir e prever qual o impacto que determinada vulnerabilidade pode vir a ter sobre os ativos da empresa, após a implementação de um controlo de segurança. O modelo foi implementado numa ferramenta que permite a um utilizador a definição de diversos parâmetros e informações relevantes, por forma a que a solução vá de encontro às necessidades e objetivos de uma organização.

A existência destas duas premissas permite que a ferramenta desenvolvida seja capaz de produzir um *output*, que se traduz num portfólio que consegue incluir a minimização de custo em relação aos produtos que são escolhidos na solução, ao mesmo tempo que minimiza o *expected loss* da organização. Este processo permite que o portfólio produzido seja personalizado dependendo das necessidades de cada empresa, e que leve a uma tomada de decisão conscienciosa por parte dos decisores de uma organização, com o objetivo de se garantir uma escolha correta de controlos de segurança de informação.

Numa fase final, foram elaborados alguns *case-scenarios* com a utilização de diferentes valores nos parâmetros que dizem respeito à otimização de custos e à minimização do *expected loss*, onde foram utilizadas as mesmas vulnerabilidades em todos os cenários propostos. Concluindo, com isto, é possível comparar os resultados

obtidos nos diferentes cenários e verificar possíveis oscilações nos resultados que ocorreram, quando é apresentada a solução juntamente com o portfólio de produtos de segurança informática escolhidos.

Palavras-Chave: Sistema de Gestão em Segurança de Informação, Risco, Vulnerabilidades, Segurança, Apoio à decisão, ISO/IEC 27001:2013, ISO/IEC 27002:2013.

Abstract

The evolution of mankind has allowed several technological changes, which result in computers with greater capacity to process, store and consult operations that correspond to the normal functioning of the organization. Thus, in the globalized and competitive world in which we live, organizations tend to value the critical information of the company as well as its assets in order to maintain and improve its business processes. Therefore, there is a need to maintain a structure with a competent team to respond to the needs that may exist as regards information security.

This valuation of information and its assets can be managed using international references for the management of information security, a topic that has been gaining greater relevance to organizations over time, leaving these to be seen as a simple standard, but also as a support to the differentiating decision making.

The correct use of an Information Security Management System (ISMS) is an instrument that can demonstrate to the customers and suppliers of an organization that the components of Information Security are verified and in order within the organization: Integrity, confidentiality and availability in data and systems. Choosing controls to meet IT security requirements, given a limited budget, is a time-consuming and complicated process that most organizations face today.

The present work proposes the development of a framework that supports an organization's decision making regarding the mitigation of various vulnerabilities that could compromise the performance and objective of several business processes, based on two objectives: Investment optimization and minimization of the expected loss. The security controls that are suggested in this portfolio may be of a mixed nature, such as hardware controls, which include components such as Firewalls or access controllers, and a set of policies, procedures, and training actions. This framework was implemented with the support of the standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013. ISO/IEC 27001: 2013 is used in various domains to establish, implement, maintain and improve an organization's information security management system. The main purpose of ISO/IEC 27002: 2013 is to allow the choice of controls that will mitigate the vulnerabilities that were identified and could be present into an organization environment.

Based on what was described previously, a tool was developed to support the selection of a set of security products, through a portfolio. This portfolio corresponds to the optimized selection of security controls to be implemented in a certain scenario.

Keywords: Information Security Management System, Risk, Vulnerabilities, Security, Decision Support, ISO/IEC 27001:2013, ISO/IEC 27002:2013.

Contents

List of figures

List of Tables

1 Introduction

In a globalized and competitive world in which we live, organizations increasingly rely on information to manage, maintain and grow their business. With this, it is of the utmost importance to create and maintain a continuous review of computer security policies and controls to ensure the services availability to customers. These security policies and controls must be effectively implemented in order to value the importance of integrity, confidentiality and availability of information in relations with all the stakeholders involved in the company business. From what has been said, it is clear that there is a need in the development of decision support tools to select security controls, in order to assist information security investments management, to create and maintain high security standards.

1.1 Motivation

Due to the technological expansion that many organizations face, there is a greater diversity of critical information circulating within the company's assets. Such expansion allows for a greater susceptibility to exploitation of vulnerabilities by attackers. It is extremely important to design controls and policies that contribute to the integrity, confidentiality and availability of the information hold within an organization.

To convey the concern of this need to senior managers, it is important to devise an analytical approach to the vulnerabilities inherent in the natural technological expansion of the organization, as well to controls that mitigate those vulnerabilities.

With this, the main motivation of the present work is to support the needs of an organization to implement or prioritize Information Security controls through a decision support framework.

1.2 Objectives

According to the above, the objective of this work is to develop a tool capable of doing the optimization of security controls portfolio, using a bi-objective model. The result will be a portfolio that provides the optimal selection of security controls for the

vulnerabilities that were identified using international Standards such as the ISO/IEC 27001:2013 (ISO/IEC, 2013a) and ISO/IEC 27002:2013 (ISO/IEC, 2013b).

It is intended that the use of this framework aims to assist the user, by making an evaluation to the company needs, with the ultimate goal of understanding how ready his organization is to be certified to ISO/IEC 27001:2013 standard.

1.3 Contributions

In this dissertation it is mentioned the importance of offering to an organization a decision support for the selection of information security controls. For this, it was necessary to survey possible vulnerabilities using the international standard ISO/IEC 27001:2013, establishing the relationship with generic controls using the ISO/IEC 27002:2013 standard. An optimization model was developed and implemented, which allows the support of the choice of security products on the market that can mitigate a set of vulnerabilities. When a user intends to use the developed tool, it is possible to evaluate if the controls that are suggested by the Solver application correspond or not to the company's needs, based on two objectives: investment optimization and the minimization of the Expected loss.

As long as this is a proof of concept, it is possible for the user to change the proposed vulnerabilities, as well as allowing the use of security products other than those that are suggested by the tool.

From the knowledge of the author, there is no open-source solution that optimizes the selection in a portfolio for computer products on the market that mitigate some of the vulnerabilities that we identified from ISO / IEC 27001:2013 and ISO / IEC 27002:2013.

According to what was previously described, the contribution of the developed tool can be summarized as follows:

- Allow top managers to assess and prioritize the implementation of controls based on identified vulnerabilities;
- Continuously improve controls and information security rules;
- Allow to identify the existence of vulnerabilities based on ISO/IEC 27001:2013
- Provide an optimization model for the choice of computer products in the market, based on its price and expected loss.

In addition, the work that was developed during this dissertation lead to the writing of an article to be presented and published in the proceedings of "The 19th Open Conference of the IFIP WG 8.3 on Decision Support Systems (IFIP DSS 2018), 13-15 June 2018 in Ljubljana, Slovenia".

1.4 Work planning

In this section it will be presented the work plan, since the beginning to the conclusion of the present work.

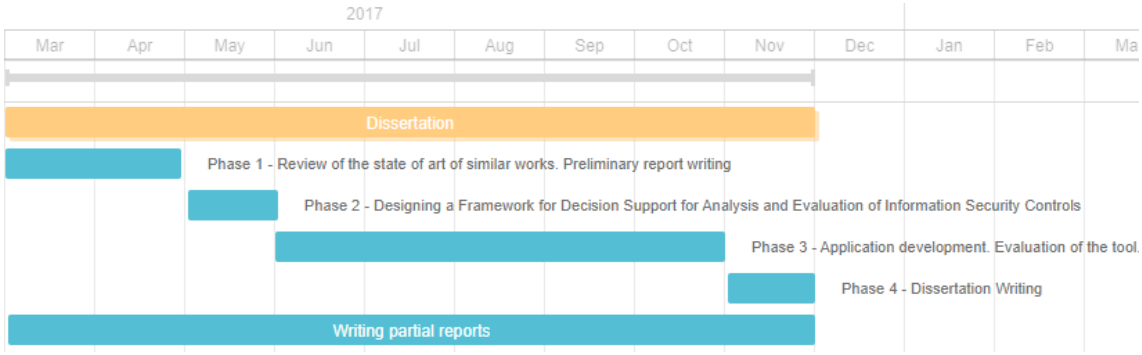

Figure 1 – Initial planning and phases of the work

Figure 1 allows the visualization of the work plan that was initially planned for the conclusion of the work. As we can see from the figure, the first phase was used to the review of several scientific works in the related field of this work. During a second phase, which took around four weeks to be done, a design and abstract planning of the current framework was produced, with the help of the project supervisor. A third phase was used to the research of the controls that could be used in the portfolio, as well as the implementation of the framework. In a fourth and final phase, which should take place in November, the writing and re-writing of several partial reports were done to finish the dissertation.

In general, most of the deadlines that were outlined at the beginning were fulfilled. Although, in the fourth phase – Dissertation Writing – there was a delay of two months from what was initially expected, which lead to the conclusion of the work to the end of January, instead of the beginning of December.

1.5 Structure of the document

The present dissertation is organized in five chapters. Next, we will briefly describe each one of them.

In Chapter 2 the state of the art is presented with regard to work related to ISO / IEC 27001:2013 and ISO / IEC 27002:2013 standards, decision support models, portfolios of Computer Security products and Information Security Management Systems.

Chapter 3 refers to the methodology used in the work. We begin giving an insight about the methodology that was used in the framework development. Next, an explanation about the identification groups of both ISO / IEC Standards and the establishment of their relations are given and, finally, the description of the optimization model takes place.

Chapter 4 begins by describing the model that will be used in the tool and how it can be adapted. Next, a general description of the tool takes place, as well as the description of the spreadsheets and parameters.

Chapter 5 presents the discussion of the framework. Here, three case scenarios are described in order to highlight the importance of the different weights for the two objectives in the optimization function.

Chapter 6 is reserved to discuss the conclusions of all the work that had been developed, as well as the future work that could be done from what has already been done.

2 Related work

This chapter reviews the state-of-the-art on work that is already done in similar scientific fields, such as Decision Support Systems (DSS), Security Product Portfolios, Information Security Management and ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013.

2.1 Decision support systems

The work of Veronica (2007) indicates that there are several methodologies for the elaboration of a Decision Support System, for example the ROMC[1] analysis (The analyst characterizes the different representations available for use as methods of communication between the user and the application), evolutionary development (advisable when the intention is the elaboration of a small DSS), Prototyping (Advised when the specifications aren't well defined at the beginning and the managers could include specifications) and end-user oriented development (advisable when it is intended to give users and managers freedom to build their own DSS).

Each type of decision support system has a unique set of methodologies for use. However, Veronica (2007) gives a set of methodologies that are used in all the decision support systems, except in the system-driven. This methodology is exposed and explained in Table 1.

Next, it will be presented the different types and characteristics of Decision Support Systems that exists, taking into account scientific articles and papers. Furthermore, it will be highlighted the benefits and constraints of each system whenever they are implemented in a organisation.

[1] ROMC – Process-oriented methodology, based on four entities: (R) Representations; (O) Operations; (M) Memory aids; (C) Control.

Requirements definition	- Specify the objective of the DSS; - Identify the processes that are going to be used in the system; - Define functional and non-functional requirements; - Studies about the viability of the DSS;
Analysis	- Elaboration and documentation of the requirements of the system, by using multidisciplinary teams; - Elaboration of a logical model;
Design	- Architecture design; - Graphic representation of system design; - Selection of the internal and external data that is going to be present in the developed system.
Prototype design and test	- Transforming a logical model into a physical model, by elaborating a system using programming languages; - System validation; - Integration of data into the DSS;
Implementation	- Distribution of the DSS to the users; - Functionality tests; - Elaboration of documentation; - Providing training to the users;
Maintenance and evolution	- Maintenance and updates; - Modular integrations;

Table 1 – Main steps for the development of a DSS

2.1.1 Document-driven DSS

Power (2001) states that Document-driven DSS has as its main function the storage and management of several documents in various formats to enable their retrieval and analysis. Furthermore, it helps to categorize development knowledge based on surveys, and also in the research and communication. The documents that can be accessed from this type of system vary from hypertext, images, sounds and videos, policies and procedures, products, meeting data and correspondence that is important for the organization (Power, 2008).

2.1.2 Knowledge-driven DSS

The Knowledge-driven DSS aims to find and recommend actions to the managers, by supporting the visualization of information that was stored and processed through artificial intelligence tools or statistics, as is the case of Bayesian networks. This model

supports the decision maker by including the knowledge management components that allows to find solutions in decision support systems and sub-systems (Power, 2007). The author states that Knowledge-Driven is considered the most sophisticated decision support system for its peers, not only because contains specialized components, but also because it can use applications capable of identify and extract knowledge. In addition, Knowledge-Driven is updated more frequently than the others, to cover their domains with recent information.

2.1.3 Model-driven DSS

Power (2001) states that the Model-driven Decision Support System uses algebra and optimization simulations in order to assist an organization's decision-making in business processes. The models used in this system must have a simple description of a given situation, so that the decision maker is able to perform changes in the model with the purpose of personalizing views to increase the process of analysis (Power and Sharda, 2007). The implementation of a Model-driven DSS includes real-time information from situations focused on business events. Studies carried out indicate that in the future this type of system will be more realistic and such reality will not increase in proportion to its complexity and understanding.

2.1.4 Data-driven DSS

A Data-driven DSS is a decision support system that has as main purpose the creation of reports, data warehouses and systems analysis. Its function is to access and manipulate a large amount of internal and external data information from the organization (Power, 2000). This happens because the Data-driven is based on a storage and processing technology, where is possible to perform analysis tasks and information exploration to improve the decision making. An example of implementation of a Data-drive DSS in a organization can be through spreadsheets. When this happens, large amounts of information are transferred from a database to a DSS application. After this step, pivot tables and graphs are created to help the analysis and decision making (Power and Sharda, 2007). A Data-driven DSS has a better acceptability in situation where there are multiple data sources, offering multidimensional data analysis.

2.1.5 Communication-driven DSS

Power (2000) states that Communication-driven DSS is a decision support system that uses network and communication skills, to facilitate the collaboration of several employees of an organization into the decision-making process. In this type of systems, communications technologies such as groupware, video conferencing and information panels have a relevant role within an organization, as it promotes communication with different teams and employees. In addition, it is possible to include important components such as communication, collaboration and coordination support to projects. These components allow a greater flexibility with regards to the decision making of a task with the collaborative help of several individuals. According to Power (2001), Communication-driven allows a better quality of internal communication, so that decision-making is done in a coherent and not in a careless way.

2.2 Security controls selection

The work of (Nunes et al., 2015) presents a decision model oriented to assess the value of risks in Information Systems of several organizations in Portugal. This article aims to provide an alternative to mapping strategic planning to risk management in information systems, as well as promoting the involvement of all stakeholders in the project. The methodology used in this present work is as follows:

- Collect a detailed list of values decisive for the intended context;
- With the list of values proceed to their classification as sub-objectives, and group those as main objectives;
- The main objectives are classified as "means objectives" and "fundamental objectives", critical objectives for the context are the fundamental objectives. The selection process is based on the 'Why is this important task?' Test;
- For each of the key objectives it is given a weight;
- Attributes are developed to measure objectives;

According to the authors, there is still work to do in order to create a decision model to minimize and find the best alternatives to mitigate risk in information systems.

Sawik et al. (2013) elaborated a portfolio that contains a set of reactive measures to predict or mitigate computer threats to an organization, always keeping in mind the

level of confidence / preference of risk for the different cases. The decision model used is intended to minimize the cost of each measure, while maximizing the efficiency of repelling/resist a set of threats. For a greater effectiveness of the model in question, a multi-objective model is used that allows the decision maker to visualize the decision model with different cases generated (e.g., expected case and worst case). In one of the exemplified cases, it is possible to verify the probability that an action mitigates for each threat, where the value 1 corresponds to full coverage of the threat and the value 0 corresponds to the lack of coverage for the same threat. The author concludes that the model used allows the decision maker to control the risk of losses resulting from a successful computer attack by selecting a certain level of confidence. The larger the budget available and the level of trust, the more risk-oriented the measures in the portfolio will be. For a more limited budget and a lower level of confidence, riskier measures that are less likely to occur are rarely present in the portfolio.

According to Fielder et al (2016), there are difficulties on the part of the decision makers in choosing security controls for an organization, taking into account a limited budget. In support of this assertion, a survey was conducted in which 75.5% of the respondents indicated that the main limitation for the purchase of computer security products was largely due to budget constraints. Another fact that deserves to be highlighted by the author, and which will be the subject of a more detailed investigation throughout the article, is that 72% of attacks on computer vulnerabilities have occurred in small-medium enterprises (SMEs).

After investigating local companies, and complementing with what was previously referred, Fielder et al. (2016) indicate that the great restriction is the lack of budget to implement cybersecurity controls that can mitigate the risk in vulnerabilities of the organization. It adds that the only solution found by these enterprises is the trade-off between the level of cost inherent to the implementation of the security control and the impact that it has in mitigating the identified vulnerabilities.

Three scenarios were applied throughout the article:

- Game theory - This scenario is based on two phases: The first stage intends that a penetration tester tries to use commonly available attack vectors against known defensible vulnerabilities that SMEs may have. In a second step, the cybersecurity

manager has a budget to implement security appliances to protect the SME's assets from vulnerabilities that the attacker might exploit.

- Hybrid method - This scenario consists in the use of a multi-objective multiple choice Knapsack based strategy, thus removing some limitations verified in the previous scenario, by considering the particular game solutions as part of an overall combinatorial optimization.
- Pure knapsack representation - Considers that the cybersecurity manager can only consider implementing solutions that include the indirect costs of each cyber security plan.

The article presents only results for the Hybrid Method. The results indicate that for the lowest budget, the optimized solution is the choice of Patch Management and Network Firewall in level two, Anti Malware and Secure configurations in level one. With this kind of low budget, it is not suggested to have Web App Firewalls and User Access Controls at a higher level than the other controls. It is also suggested the implementation of Incident Response Policy, since it covers most of the vulnerabilities to be exploited by social engineering, for a low cost of implementation.

With the average budget, the optimized solution, in addition to containing the above products at a higher level, indicates that the implementation of Patch Management with a daily patches check should be implemented as a priority. For this type of budget, it is also recommended to implement an Account Management Control, in order to limit the misuse of user accounts. Other recommendations include the introduction of Web App Firewalls in addition to Network Firewalls, Automated Inventory Scanning and Management, and IDS.

The highest budget maintains the strategy used in the average budget, with the addition of Inventory Management Tools that is implemented at a higher level, from an annual to a weekly log checking. There is also the exchange of IDS for IPS, since it acts on more vulnerabilities than the Network Firewalls, although the implementation costs are superior and only supported with this type of budget. Finally, it is recommended to include yearly user education and training, by improving user awareness about social engineering based attacks.

Khatavakhotan (2012) argues that the risk management process in software presents threats, and that ignoring these same threats causes the efficiency of software

systems to be influenced, thus leading to an improper risk mitigation process. In order to contest this, the author presents a model that can create a risk mitigation plan, focusing on the risks and opportunities that this mitigation can bring. Khatavakhotan (2012) also emphasizes that most risk analysis processes usually begin their analysis with risk identification, thus making mitigation a continuous process. Although the model presented by the author contradicts the above, he is able to create an integrated mitigation plan, which will have high costs in the mitigation of risks, but the benefits are expected to be able to offset all these costs.

According to Haufe et al. (2016), Information Security is a very important aspect in which organizations must invest. To achieve this, organizations can rely on Information Security Management Systems (ISMS), an approach that can establish, implement, monitor and maintain all existing information within a given organization. For this reason, the authors present a work that is based on a set of ISMS, governed by the standards of International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27000), Control Objectives for Information and Related Technologies (COBIT) and Information Technology Infrastructure Library (ITIL). To prove their theory, Haufe et al., (2016) implemented an ISMS process program so that they could demonstrate that these processes are able to help protect all the existing information in the organization. To conclude, the authors indicate that there are three functionalities that need to be developed in the future: Improve the framework, develop a method that fits and makes the ISMS cost processes transparent, and obtain a basic process framework for lower maturity levels.

According to the article (Kiesling et al., 2016), organizations and their infrastructures are exposed to constant threats, and deciding the better way to respond to them is a difficult task for IT security managers. For that very reason, the work aims to combine the concept of security with a simulation of an infrastructure capable of fighting attacks and providing decision support components. As a way of putting the results into practice, interviews were carried out with specialists from various branches of Information Security, who were satisfied with the final result, since the combination of the concept of security with the infrastructure requires the evaluation of the assets of the organization and the identification of the inherent threats. In addition, it was pointed out that the simulated infrastructure is able to reveal attacks more clearly, in order to prevent and react to them. For these authors, the infrastructure that was created can be

implemented in any real environment, but this of course has costs. In addition, the model requires constant updates so that the entire system security is assured. The authors argue that creating a model that works manually is useless, since a process that consists of managing the information has a great connotation in the organization, because all its data and information can be lost when an attack occurs. In order to create a model capable of dealing with attacks, it is necessary to have knowledge beyond technology, because psychological, sociological or economic parameters should not be forgotten. To conclude, Kiesling et al. (2016) argue that in the future a method must be integrated that simulates the impact of attacks on an organization's business process.

According to Yevseyeva et al. (2016), in order to protect a system from attacks and computer crashes it is necessary to select controls that are able to meet the needs of the company. For this, it is recommended to perform two tasks: Firstly, managers should establish a budget, and secondly, the same budget should be distributed among the various types of security controls, so that it is possible to decide which process should be adopted. In addition, it is argued that risk assessment should be based on quantitative and qualitative analyses, based on several standards such as, ISO/IEC 27001: 2013 and ISO/IEC 27002: 2013. Yevseyeva et al. (2016) argue that one of the biggest challenges that companies face is cybersecurity, since there is reluctance on the part of managers to invest in this area. For this reason, factors such as budget definition, risk / return analysis and selection of different controls should be taken into account. Having that into account a formula was developed, which should be based on realistic data, so that managers can establish a budget and make decisions that bring benefits to the company.

According to Yeveseyava et al. (2015), the easiness with which information is available today allows for possible exposure or even leakage of confidential data and information. In order for this exposure or leakage to be avoided, it is necessary to develop security policies that are adopted by all companies. This proposal is classified as risky due to the objective of each company being different, but also by the complexity that the risk assessment entails to the complexity of idealizing all possible risk scenarios. In order to mitigate these tasks, it is argued that companies should rely on the chief information security officer to ensure that both enterprise resources, devices and data are protected from possible security breaches that may arise within the organization. To do so, it is necessary to identify risk behaviours that may arise on the part of the employees and to develop security policies to which they must obey. Concluding, Yeveseyava et al. (2015),

suggest that if uncertainties arise in deciding which security controls a company should choose, the chief information security officer should propose several alternatives for cost reduction and to minimize the risk of possible attacks.

Brenner (2007) created an ISMS using a PDCA (Plan, Do, Check, Act) model. In a first step, the ISMS should be established and be able to identify which method of risk assessment should be adopted, in order to analyze possible occurrences of risks. The second step concerns the implementation and operation of the ISMS, whose main tasks are to define actions, sources, priorities, responsibilities, what measures to take, and to implement controls and procedures for detecting incidents. In the third stage, which is called monitoring and reviewing the ISMS, and as the name implies, is where the ISMS monitoring and review procedures should be carried out regularly to measure the effectiveness of the controls. The fourth and last step, regarding the maintenance and improvement of the ISMS, stipulates which actions and tasks the ISMS must adopt, so that all company information and data are protected, always with the purpose of improving the security procedures of the ISMS information.

2.3 Review of the Standards

As it has been mentioned throughout the dissertation, the standards in focus are ISO / IEC 27001:2013 and ISO / IEC 27002:2013. These standards were created by the International Organization for Standardization along with the International Electrotechnical Commission with the main purpose of assisting people or organizations who wish to acquire products or services in the area of Computer Security. These standards are developed by experts from Computer Security companies or scientific institutions, and must take into account parameters such as quality, safety and reliability.

On a side note, the ISO/IEC 27005 standard has several options with respect to the treatment of the risk, which are: Risk avoidance, risk acceptance, risk mitigation through the application controls and risk transfer.

2.3.1 Standard ISO/IEC 27001:2013

In the article of Brenner (2007), which reviews the ISO/IEC 27001, the author begins by highlighting the main difference between the ISO/IEC 17799 and the ISO/IEC 27001. While the 17799 standard is a set of guidelines, ISO 27001 consists of a set of multi-component requirements in both of which have as main objective to ensure that

when implementing an information security management system, all information within the company can achieve the concept of compliance with the standard. Brenner (2007) gives a more detailed description of the ISO/IEC 27001 standard and establishes three factors that must be met when companies are faced with risk management situations:

- The organization shall define and evaluate possible risks that may occur in the future;
- The selected risk assessment methodology should ensure that the risk assessment produces comparable and reproducible results and the risk assessment must be carried out continuously;

For Mattes & Petri (2013), the implementation of an Information Security Management System should follow the ISO 27001 standard that uses a *Plan-Do-Check-Act* model as an approach, which is represented in Figure 2.

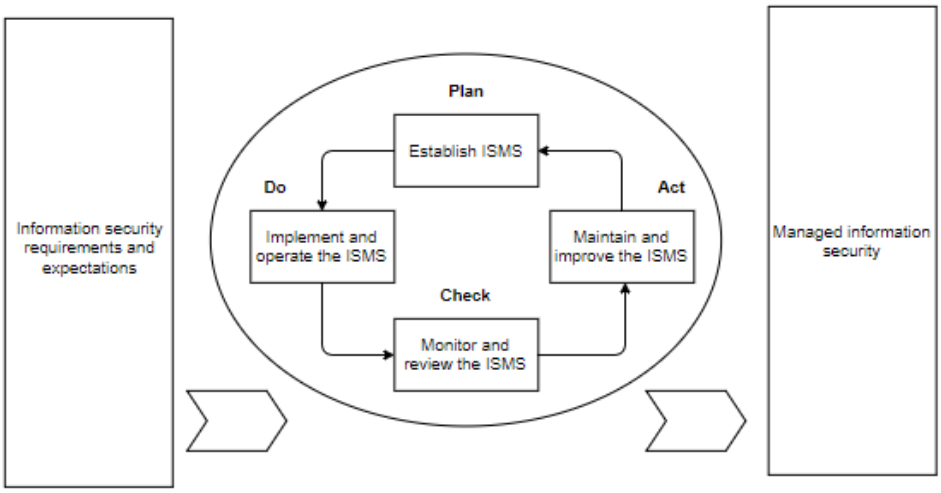

Figure 2 – Plan-Do-Check-Act Model. Extracted from Mattes & Petri (2015)

The first step, which concerns Planning is essential for the implementation of the information security system, because it concerns to the creation of security policies and objectives, taking into account the requirements of the company.

The second step, which concerns to the implementation of the Information Security Management System, discriminates which processes and procedures should be followed and applied.

The third step, which aims to monitor and critically analyze the ISMS, has as the main objective the evaluation of the performance associated with ISMS when it is proposed to a certain task.

The fourth and final step, focus on the preventive updates that may occur on audit tests, which may help on the continuous improvement of the Information Security Management System.

As far as organizations are concerned, the standard ISO/IEC 27001 has been implemented more frequently as safety standards, according to Boehmer (2016). However, for Kosutic (Unknown Year) with the implementation of this standard, internal or external challenges may arise, for example:

- Difficulties in implementing information security standards when the information selection process occurs incorrectly;
- When implementing the ISO / IEC 27001 certification runs at the same time as a project, this can be seen as less important.

Although there are challenges in the implementation of controls and processes using the ISO / IEC 27001 standard, according to Susanto and Tuan (2011) there are several advantages in this implementation process, namely:

- It proves to third parties that there is security within the organization;
- Security becomes of greater importance when working with business processes;
- Promotes awareness of residual risks;
- It increases employees' awareness of their security knowledge and is thus able to implement standards in business operations.

In order to highlight the importance of using the ISO/IEC 27001:2013 standard, a survey was carried out to determine how many are the organizations accredited by this standard in Portugal (IPAC, 2017).

Nº Certificados	2014	2015	2016
ISO 9001	5661	5538	5589
ISO 14001	1051	1107	1123
SST (18001&4397)	297	568	561
ISO 22000	249	299	295
ISO/IEC 27001	11	20	35
NP 4457	153	179	170
NP 4406	9	11	12
NP 4512	3	2	1
TOTAL	**7434**	**7724**	**7786**

Figure 3 – Number of accredited organizations in Portugal, extracted from (IPAC, 2017).

According to information gathered through the Portuguese Accreditation Institute, it is possible to know the number of organizations that are accredited by International Standards in Portugal. According to Figure 3, although there are still few organizations accredited with ISO / IEC 27001:2013, there is a gradual increase in the number of accredited organizations. For example, in Portugal, organizations like Fujitsu Technology Solutions, LDA, Associação DNS.PT, Turismo de Portugal, I.P and others, are aware of its importance to the compliance with integrity, confidentiality and availability of data and systems.

Concluding, Brenner (2007) defends that the ISO/IEC 27001 is an international standard that can assist a IT worker in the decision of what controls should a company adopt to create a safety environment. This can be achieved by combining risk management, safety policies or procedures and compliance. In addition, it helps a company to define which people should access the system and which processes and technologies should be adopted, so that there is a correct management of security and risk within a organization.

2.3.2 Standard ISO/IEC 27002:2013

The Standard ISO / IEC 27002 aims to establish guidelines and general principles for creating, implementing, maintaining and improving Information Security Management. Palhares (2011) indicates which are the elements that must be applied for the protection of information of a certain organization, focusing on the fact that information must be protected from all threats, to ensure business continuity, minimize business risk, maximize return on investment and business opportunities.

In order to be implemented properly, a set of controls must be chosen based on an evaluation of the risks and assets of the organization, being: Information Security Policies; Organization of Information Security; Asset Management; Human Resources Security; Physical and environmental security; Operations and communications management; Access control; Acquisition and development; Management of information security incidents; Continuity management and finally, compliance. These controls make the information security policy objective to find its guidance and support according to business requirements and with relevant laws and regulations (Santos, 2012).

Pandini (2016) also reviews the ISO/IEC 27002 standard has several benefits such as: raising awareness about Information Security, ensuring a greater control over assets and sensitive information, providing approaches for the implementation of control policies; Improve organization in processes and management mechanisms, promoting cost reduction in conjunction with prevention of information security incidents, ensuring the compliance with legislation and regulations.

Concluding the analysis of the two standards, Palhares (2011) states that their use can be considered a structured and internationally recognized method for information security. Taking into account characteristics and implementation requirements, both standards can develop a process to evaluate, implement, maintain and manage information security.

According to (Mattes & Petri, 2013), the implementation of the ISO/IEC 27001 and ISO/IEC 27002 standards leads to greater security with regard to the standardization of services and the information management existing in an enterprise.

But what procedures should be adopted to develop an information security policy? To answer this question, Mattes and Petri (2013) distinguish three points that must be taken into account: Survey of problems and threats that may arise within the company; Identify and relate the main points of the ISO/IEC 27001 and ISO/IEC 27002 standards, taking into account problems and threats previously identified; Outline an example of information security management that meets the needs of the enterprise.

According to what has been reviewed in several scientific articles, there is a necessity to develop new approaches that allow not only the decision support regarding security controls, but also the prioritization of security products depending on the available budget, and the needs of the organization to ensure business continuity and

information security. This motivation fostered the development of a decision support tool that could lead to the creation of a secure business environment in which information security concerns.

3 Framework for optimization of security controls selection

This chapter presents the framework developed, thus revealing all the steps taken until the development of a decision support tool for selection of information security controls. A special focus is given to the optimization model that was developed.

Figure 4 illustrates the developed framework. The study and analysis of the Standards led to the identification of vulnerabilities, and controls to mitigate them. The relation between the vulnerabilities and security controls, permitted the development of a optimization model that allows the identification of a security control portfolio.

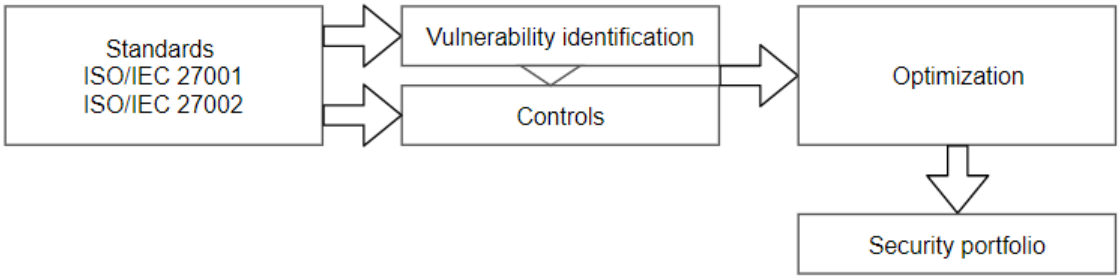

Figure 4 – Schematization of the framework

3.1 Methodology

Figure 5 illustrates the methodology used throughout the implementation of the framework that leads to the optimization of a portfolio of computer security products.

As previously mentioned, the main objectives resulting from the implementation of the framework are a continuously improvement of controls and information security rules of an organization, as well as giving the choice to the senior managers to prioritize the implementation of security appliances, policies and procedures through the identified vulnerabilities, as well as their cost and impact.

As can be seen in Figure 5, the first step in the methodology concerned the identification of clauses in the international standards ISO/IEC 27001:2013 and ISO / IEC 27002:2013, where it was possible to establish the scope to determine the security portfolio. For this, an analysis was made of several scientific works that are related to the topic, and to the standards themselves in order to guarantee a greater knowledge.

Next, we developed an optimization model that allows the user to quickly and easily check the appliances that mitigate the identified vulnerabilities. There are several

features that are available in the tool, such as an objective function which relates the bi-objective model that was developed, in regard to the expected loss with the total cost of the suggested appliances.

After the research of some existing appliances in the market and the development of the optimization model was finished, it was possible to begin the implementation of the tool. Here, we will explain the environment that were used during the implementation of the tool.

In the last phase, a discussion will be presented. This will be achieved by performing case-scenarios on the tool to determine if it met the objectives outlined at the beginning.

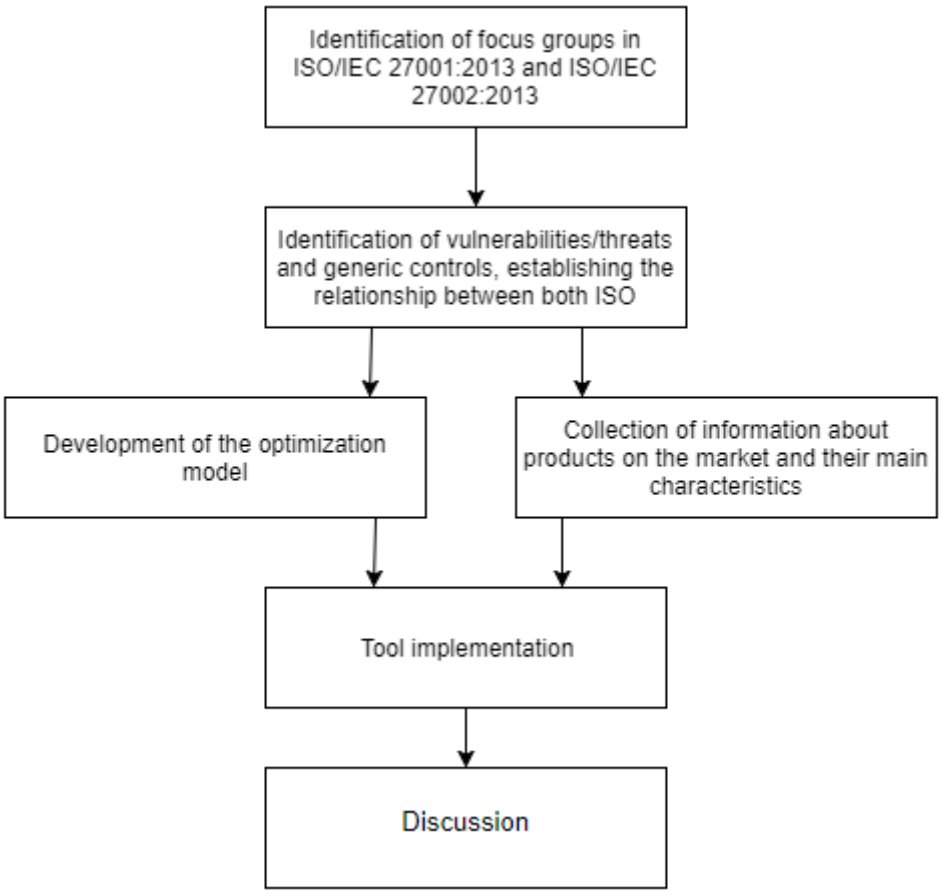

Figure 5 – Methodology used in the present work

It is important to highlight that the decision support that was developed in the tool corresponds to the model that was emphasized in section 2.1.3, Model-Driven DSS, since a bi-objective model was developed to minimize the cost of security controls and

minimizing the impact that a successful attack may have on a vulnerability, after selecting the optimal control by the Solver.

3.2 Group identification of ISO/IEC 27001:2013 and ISO/IEC 27002:2013

As background documents for this work, scientific papers, academic works and technical works were analyzed, with the aim to present a state of the art with different points of view on Decision Support Systems, as well as their functions and methodologies. In addition, as already mentioned, the present work and the developed framework are based on ISO / IEC 27001:2013 and ISO / IEC 27002:2013 Standards. Through the study and analysis of their main characteristics, it was possible to specify the importance of each of them in an organization's security management system.

Both ISO / IEC 27001:2013 and ISO / IEC 27002:2013 are part of the ISO / 27000 family which has as primary objective the understanding of the information security standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The main purpose of ISO / IEC 27001:2013 is to specify the requirements to establish, implement, maintain and continuously improve an organization's ISMS. Within this standard there are requirements that must be fulfilled for this same implementation, such as the attribution of responsibilities or the stipulation of standards and terms related to Computer Security.

For this standard to be implemented correctly and without losses to an organization, it is necessary to answer some questions, for example: How much will a failure cost when an effective loss of information happens? What are the key areas that an organization should leverage to be successful? How heavy is the occurrence of incidents about an organization's information? This is some key information that an organization should consider in order to effectively prioritize the implementation of security controls.

The main purpose of ISO / IEC 27002:2013 is to establish guidelines that can create, maintain and improve the ISMS. In addition, it is a standard that can establish a direct relationship of which generic controls should be applied for the vulnerabilities identified in ISO / IEC 27001:2013, for protecting the information of an organization.

For its proper functioning, the ISO / IEC 27002:2013 standard identifies controls that must be chosen based on an assessment of the risks and assets of the organization. Within these controls we can find several categories such as: “Physical and environmental security”; “Management of information security incidents” or “Information security organization”.

Due to the large extension of the standards and as long as the present work will act as a concept proof, the scope of this work will be restricted to three clauses.

Therefore, we will briefly make a description of the clauses in evidence for this work, based on ISO / IEC 27001:2013 and ISO / IEC 27002:2013.

The ninth clause objective of the standard, Access Control, consists of: Business requirements for access control; User access management; Responsibility of users; Control access to systems and applications. Business requirements for access control aim to limit access to information and resources of various information processing within an organization. Access control of systems and applications has as main objective to ensure the correct access of authorized users and to prevent access to unauthorized and non-authenticated users in the system. Responsibility of users has as the primary goal to ensure that all users of an organization are held responsible for protecting their information for authentication. Finally, Control access to systems and applications controls are intended to prevent unauthorized access to systems and applications of an organization.

In the twelve clause, referred by both Standards as Operations Security, are contained seven discriminated topics, which are as follows: Operational procedures and responsibilities; Protection against malicious code; Data protection; Event logs; Monitoring; Control of software in production systems; Technical vulnerability management; Considerations for audits of information systems. Operational procedures and responsibilities ensure the correct and safe operation of an organization's information processing capabilities. The main objective of protection against malicious code is to ensure both the information and the processing resources are protected against malicious code. The purpose of the data protection topic is to protect against data loss. In event and monitoring logs, it is intended to record events and generate evidence about user activities, failures that may arise in information security, and unauthorized access by outsiders. The purpose of software control in production systems is to ensure the integrity of an organization's information systems in tasks such as software installation. In the management of technical vulnerabilities, it is intended that there is prevention regarding

the exploitation of vulnerabilities in the information systems used in an organization. Finally, considerations for auditing information systems are intended to minimize the impact of audit activities on production systems, and make sure that they do not interfere with an organization's business processes.

The last clause in study is the Communications Security. This clause consists in two topics: Network security management, and Information transfer. The first topic relates to the protection of information in the organization's network and in its information processing resources. The second topic has as main goal the maintenance of the security of any information transmitted from within the organization to any external entity. Therefore, there must be policies or controls to protect the transfer of information through the use of any means of communication.

3.3 Establishment of relations between ISO/IEC 27001:2013 and ISO/IEC 27002:2013 with their generic controls

Although the characteristics and advantages of using the Standards under study have already been highlighted, it is necessary to establish the relationship between both Standards in order to be able to fully understand the scope and capabilities they can provide to an organization.

The use and implementation of the two standards within an organization has several advantages, namely in corporate processes, since they are able to develop a process capable of evaluating the degree of maturity in relation to information security, maintaining and managing the various processes related to security of information - This results in an increase of the reliability, integrity and availability of information within an organization processes.

As we have already seen, both standards are very similar in the area which they are inserted, however their usefulness and purpose are different. The ISO/IEC 27001 standard is a standard for management. Basically, it is a standard that defines how information security is planned, implemented, monitored and improved. This Standard also allows obtaining certifications (as demonstrated in Figure 3). Although ISO/IEC 27002 contains more detailed information for each control, it is not possible to obtain certifications for this standard.

To be able to visualize a symbiosis relationship that exists between both standards, it will be presented an example where both complement each other.

ISO/IEC 27001:2013	ISO/IEC 27002:2013
13 Communications Security	**13** Communications Security
13.2 Information Transfer **Objective** to maintain the security of information transferred within an organization and with any external entity	**13.2** Information Transfer **Objective** to maintain the security of information transferred within an organization and with any external entity
13.2.3 Electronic Messaging	**13.2.3** Electronic Messaging
Control Information involved in electronic messaging should be appropriately protected.	**Control** Information involved in electronic messaging should be appropriately protected.
	Implementation guidance Information security considerations for electronic messaging should include the following: a) Protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organization; b) Ensuring correct addressing and transportation of the message; c) Reliability and availability of the service; d) Legal considerations, for example requirements for electronic signatures; e) Obtaining approval prior to using external public services such as instant messaging, social networking or file sharing; f) Stronger levels of authentication controlling access from publicly accessible networks.
	Other information There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

Table 2 – Relation between ISO/IEC 27001:2013 and ISO/IEC 27002:2013 in clause 13.2.3 – Information transfer

As can be seen in Table 2, both standards are quite similar until the description of each security control clause. However, ISO/IEC 27002:2013 is characterized by being a standard that offers a much greater level of detail, as it provides an ‘implementation guidance’ with some considerations to take into account during the implementation of

controls for this clause, as well as a ‘other information’ that are relevant to IT workers when trying to implement this clause in the organization.

3.4 Optimization model

The main objective of the optimization model is to offer an optimized choice of security controls for vulnerabilities that are identified.

The objective function is composed by two objectives. The first objective it to minimize the value of investment needed to mitigate all the vulnerabilities that were selected. The second objective is to minimize the expected loss. The expected loss is related to the percentage of mitigation that is not covered by a security control and the impact that an attack can have in the organization. This relates to the residual risk that is inherent to the implementation of a security control.

In order to fulfill the aforementioned objective, the optimization model has to guarantee several functionalities in order to speed up the decision making on the part of the user, being:

- The optimization model assumes the identification of a set of vulnerabilities that were previously identified using ISO / IEC 27001:2013.
- In the case where computer products mitigate more than one vulnerability, the optimization model must ensure that products with a lower price are chosen. However, all computer products are available for consultation.
- The impact (expected loss) of each vulnerability is also taken into account for the optimization function.
- The model was developed in an incremental way.

After summarizing the general features of the linear optimization model, it will be described in detail.

Model 1 minimizes the value of investment assuring the mitigation of the vulnerabilities, and Model 2 minimizes the expected loss assuring mitigation of the vulnerabilities. Finally, Model 3 combines the two objective functions of Model 1 and Model 2 using weights for the previous objectives.

The model uses the following variables and parameters:

bi – Existence of vulnerability (i = 1, …, m);

cj – Cost of the control j ($j = 1, \dots, n$);

n – Number of available controls;

m – Number of vulnerabilities;

im_i – Impact loss of vulnerability i;

a_{ij} – Represents if the control j acts on vulnerability i;

nm_{ij} – Percentage of the vulnerability i that stays unprotected after the implementation of a security control j;

$$xj = \begin{cases} 1, If\ the\ control\ j\ should\ be\ chosen\ (i = 1, \dots, m) \\ 0, Otherwise \end{cases} \quad (1)$$

Equation (1) indicates that the value of xj is going to have the value 1 if the control j is the chosen to integrate the security portfolio, 0 otherwise.

Model 1 – Optimization model for the minimization of cost

$$\min \sum_{j=1}^{n} cj\ xj \quad (2)$$

s.t.:

$$\sum_{j=1}^{n} aij\ xj\ \geq bi\ , \qquad i = 1, \dots, m \quad (3)$$

$$xj = 0, 1, \qquad i = 1, \dots, m, \qquad j = 1, \dots, n \quad (4)$$

Equation (2) is the objective function which corresponds to the minimization of the total cost of the controls that should be implemented.

Equations (3) and (4) ensure that the number of controls that cover a vulnerability is at least 1 if the vulnerability exists.

Model 2 – Optimization model with the minimization of expected loss

$$min \Sigma_i \left(\Sigma_j\ nm_{ij}\ xj \right) im_i \quad (5)$$

s.t:

$$\sum_{j=1}^{n} aij\ xj\ \geq bi\ , \qquad i = 1, \dots, m \tag{3}$$

$$xj = 0, 1, \qquad i = 1, \dots, m, \qquad j = 1, \dots, n \tag{4}$$

Equation (5) represents the total expect loss for all the vulnerabilities and their security controls.

To combine both models in a bi-objective optimization model we developed Model 3.

Model 3 – Bi-objective model:

$$Min\ (\ w1\ \Sigma\ cj\ xj + \ w2\ \Sigma_i \left(\ \Sigma_j\ nm_{ij}\ xj\ \right) im_i\ ) \tag{6}$$

$$\sum_{j=1}^{n} aij\ xj\ \geq bi\ , \qquad i = 1, \dots, m \tag{3}$$

$$xj = 0, 1 \qquad i = 1, \dots, m \qquad j = 1, \dots, n \tag{4}$$

Where:

$$w1 + w2 = 1 \tag{7}$$

$$w1, w2 \geq 0;\ w1, w2\ \leq 1 \tag{8}$$

Equation (6) gives the final optimization function in regard to the combination of cost optimization and expected loss minimization.

In this problem, w1 is the weight that is given to the importance of minimization of the cost, and w2 is the weight that is given to the importance of the minimization of the expected loss.

Equation (7) with the inclusion of the Equation (8) allows to tune the weights w1 and w2. If we want to maximize just the optimization of the cost, we set w1=1 and w2=0. In the counterpart, if we are not concerned with cost minimization, but just with minimization of the expected loss, we set w1=0 and w2=1. In the multiplicity of values that can be chosen for w1 and w2, we can establish scenarios of importance for both objectives.

So, we can say that the objective of the optimized function is the combination of the both objectives, optimization of the cost and minimization of the expected loss.

In the next chapter, it will be explained how this model will be implemented into the tool to optimize a portfolio of security appliances that mitigate the vulnerabilities that had already been identified with the standards previously cited.

4 Description of the tool for the optimization of security portfolio

In this Chapter, it is described all the details related to the developed tool.

In the first section, we will briefly describe the environment in which the tool was implemented, as well as the parameters that are contained in the spreadsheets. Next, an insight about the programming of the optimization model will be given in order to identify the related information and parameters. Lastly, the correct utilization of this tool and the visualization of results are provided.

The second section of this chapter focuses in the implementation of the model that was developed in the Section 3.4.

With this, the tool that was developed aims to assist an organization in the decision-making process, with the purpose of mitigate several vulnerabilities that could compromise the performance and objective of several business processes.

4.1 Model implementation

As described in Chapter 3, a model was developed to support a decision for the choice of security controls that mitigate the identified vulnerabilities, using the ISO/IEC 27001:2013 and ISO/IEC 27002:2013 standards.

The output of the tool will be a portfolio of security controls. The controls will be chosen by the optimization of their costs, and also their impact in the company.

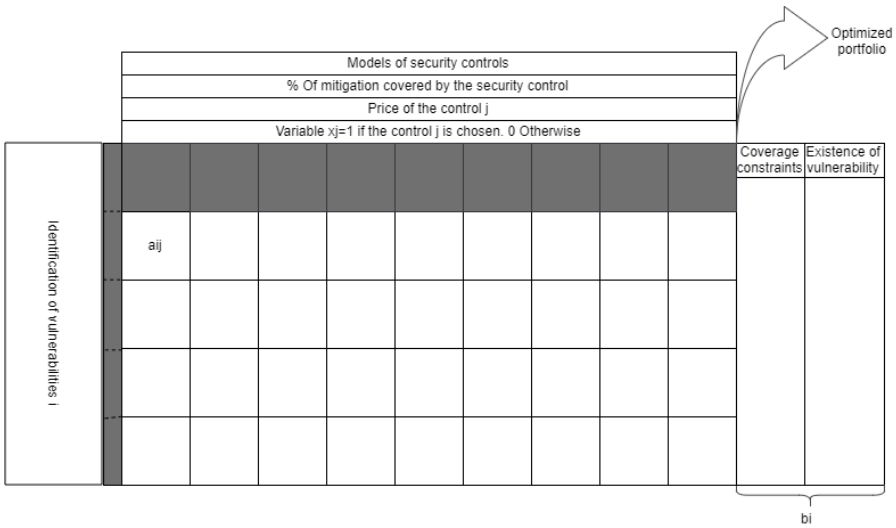

Figure 6 – Implementation of the optimization model in the Excel

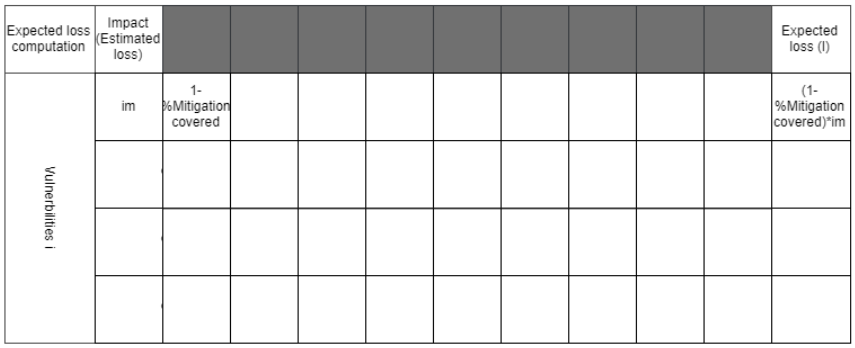

Figure 7 – Implementation of the expected loss computation

Figure 6 shows the layout of the tool for the optimization of the cost for the security products, and how the parameters relate in the table. With this, it is possible to visualize how the output of the table will be organized as well as all the important information.

Figure 7 shows the layout of the table for the minimization of the expected loss, as well as the parameters needed for that.

In the next sections, we will focus on the description of the tool.

4.2 Description of the tool

The implementation of the tool was done through Microsoft Excel, as long as most senior managers of an organization have a high utilization proficiency in this software.

In addition, Excel freely provides an add-in names Solver, which allows to solve optimization problems. With this, the optimized portfolio will be generated regarding the bi-objective model that was developed.

The tool that has been developed can be found in the following Google Drive link: https://drive.google.com/open?id=1BaP01UmjnUq3jHTT_bYbfbUBZDcXDrpO.

Additionally, the layout of the Tool that was developed can be found in Annex A.

4.2.1 Spreadsheets in the framework

The tool contains several spreadsheets that are important to the optimization of the portfolio. They can be categorized into two categories: Auxiliary spreadsheets and Functional spreadsheets.

The auxiliary spreadsheets are the ones that increases the user awareness to better understand how the tool works, namely: “Scope”, “Controls_By_Group”, “Fortinet_Product” and “Checkpoint_Product”, as represented in Table 3.

The “Scope” spreadsheet provides a short description of the tool as well as its purpose. It also provides an overview of the other spreadsheets in the framework, providing a set of details of the main features available.

The “Controls_By_Group” spreadsheet increases user awareness about which vulnerabilities are present in the tool, as well as the generic and specific controls can be used to mitigate them.

“Fortinet_Product” and “Checkpoint_Product” provide detailed information about each commercial product suggested in the tool, to ensure a weighted and complete decision for the user, as presented in Section 4.2.1.

In order to provide conscious use and focus on the best interests of an organization, two of the leading brands of security appliances have been chosen to mitigate the proposed vulnerabilities and threats, such as Fortinet and Checkpoint.

With regard to Fortinet, several types of appliances were considered, namely “FortiManager”, “FortiAnalizer”, “FortiAuthenticator” and “FortiGate”. “FortiManager” stands out by offering a network of identification and management throughout the Fortinet product infrastructure in order to identify possible security incidents occurring within the organization, and to optimize the way to deal with them. With regard to “FortiAnalizer”, it focuses on providing a set of reports creating real-time alerts of anomalies and possible computer attacks that occur within the organization. It is also able to offer a historical view of the activity that took place in the network of an organization. “FortiAuthenticator” stands out by managing access to users and services within the network, in order to strengthen the security and integrity of an organization's data. Regarding “FortiGate”, it stands out as a Next-Generation Firewall (NGFW). FortiGate is able to defend an organization's network from multi-layered computer attacks against

advanced threats and the ability to optimally scan the secure sockets layer against encrypted malware.

With regard to Checkpoint, two major products were considered: “Security Gateway Appliances” and “DDoS Protector”. With regard to the category of “Security Gateway Appliances products”, all have as security base a comprehensive threat prevention in order to offer protection against advanced threats and new vulnerabilities. It also provides an inspection of all encrypted connections such as Secure Sockets Layer and Transport Layer Security. “DDoS Protector”, stands out for ensuring a more focused security in relation to Distributed Denial Of Service attacks in a multi-layered protection environment.

The functional spreadsheets are the ones that are fundamental to the creation of the portfolio, namely: “ListOfVulnerabilities”, “SelectedVulnerabilities” and “TableFrameworkWSolver”.

The “ListOfVulnerabilities” spreadsheet contains a table that crosses the vulnerabilities identified with the set of several selected appliances. With this, is possible to indicate which vulnerabilities can be mitigated with the security controls that are provided. Taking into account the aforementioned in the Section 3.4, to establish the mapping between the identified vulnerabilities and the security controls, the “ListOfVulnerabilities” creates a matrix mapping with vulnerabilities and controls in columns, filling the number ‘1’ whenever the control mitigates the selected vulnerability. With this approach, we provide a model that is easy to understand and to be modified by the user afterwards.

The “SelectedVulnerabilities” spreadsheets have the exact same purpose as the previous spreadsheet (ListOfVulnerabilities). However, as long as it was identified 73 vulnerabilities, and most of them can be mitigated through the implementation of procedures and policies, “SelectedVulnerabilities” contains just the vulnerabilities that are mitigated through the implementation of physical security controls.

The “TableFrameworkWSolver” spreadsheet contains the fundamental table of this tool, since it contains the representation of the model and over which the solver will act.

Auxiliar spreadsheets	Functional spreadsheets
• Scope	• ListOfVulnerabilities
• CheckpointProducts	• SelectedVulnerabilities
• FortinetProducts	• TableFrameworkWSolver
• ControlsByGroup	

Table 3 – Categorization of the spreadsheets in the framework

4.2.2 Parameters

The tool has a set of parameters that allow the user to better personalize the portfolio. Next, we will describe these parameters.

Figure 8 displays part of a spreadsheet where it is possible to observe that some of the cells are coloured, and others are not. The coloured cells are the ones that must not be changed (an analysis of these cells and what they represent will be in the section 4.1.3), as long as they have formula that are important for the optimization function. The cells with no background colour are the ones that can be changed and correspond to the parameters.

- Weight expected loss - This can be translated in the importance that is given to the expected loss that are present in the portfolio with the selected security products. The higher the value that is given to this weight, the more importance is given to this objective.
- Weight cost - This can be translated in the importance that is given to the total cost of the security products that are present in the portfolio. The higher the value that is given to this weight, the more importance is given to this objective.
- Available budget – The maximum value the organization has available for investment in the security controls that are chosen in the portfolio.
- Impact (Estimated Loss) – This parameter indicates the expected loss that can occur if a specific attack happens in one of the identified vulnerabilities.

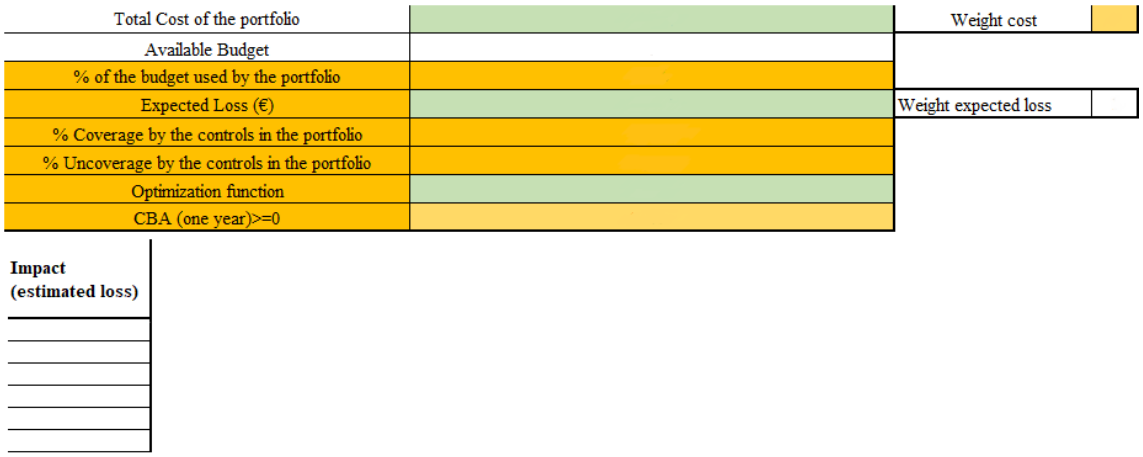

Figure 8 – Parameters in the framework

4.2.3 Programming the optimization model

The tool has a set of functions that are important to the optimization of the portfolio, as long as they implement the model into the tool. Next, we will describe the functions and how they integrate the aforementioned model. Also, it is important to notice that the model that was developed is linear integer programming.

In the Section 4.1.2 a description of the parameters (white cells) was made to reveal what they represent in the tool. In this section, the other indicators (colored cells) will be described in order to highlight how they implement the mathematical model that we developed.

- Total cost of the portfolio – The value of this cell will be obtained by doing the sum of the cost of each security control that is selected to be in the portfolio.
- % of the budget used by the portfolio – As the title of this cell says, it represents the percentage of the Available budget that is utilized for the suggested portfolio.

To achieve this value, we used the formula: $\%\ of\ the\ budget\ used\ by\ the\ portfolio = \frac{Total\ cost\ of\ the\ portfolio}{Available\ budget} * 100.$

- Expected loss – This cell indicates the sum of the expected losses for all the vulnerabilities that the portfolio of security products provides.
- CBA (One year) >=0 – The Cost-Benefit Analysis determines if the security controls represented in the portfolio are worth its associated cost. The higher the value, the better is the solution represented. To achieve this, we used the following formula: $CBA\ (One\ year) = Sum\ of\ impact - (Sum\ of expected\ losses + Total\ cost\ of\ the\ portfolio)$.
- % Covered by the controls selected in the portfolio – This cell represents the average coverage of the selected security products in the portfolio.
- % Uncovered by the controls selected in the portfolio – This cell represents the average value that is uncovered by the security products selected in the portfolio. The sum of Covered and Uncovered percentages is 100%.
- Optimized function – The cell with the Optimized function implements the Function (8) of Model 3, and considers both objectives: minimization of the total cost of the portfolio and the expected loss.

4.2.4 How to correctly use the tool

In this section we describe how to successfully work with the tool that was developed. Figure 9 displays the steps that are required to use the framework.

In Figure 9 it is demonstrated the steps that are fundamental for the use of the tool. The steps can be divided between three spreadsheets: 'ListOfVulnerabilities', "SelectedVulnerabilities" and 'TableFrameworkWSolver'.

In the spreadsheets 'ListOfVulnerabilities' or "SelectedVulnerabilities" takes place the 1st, 2nd and 3rd steps. Next, we will briefly describe each one.

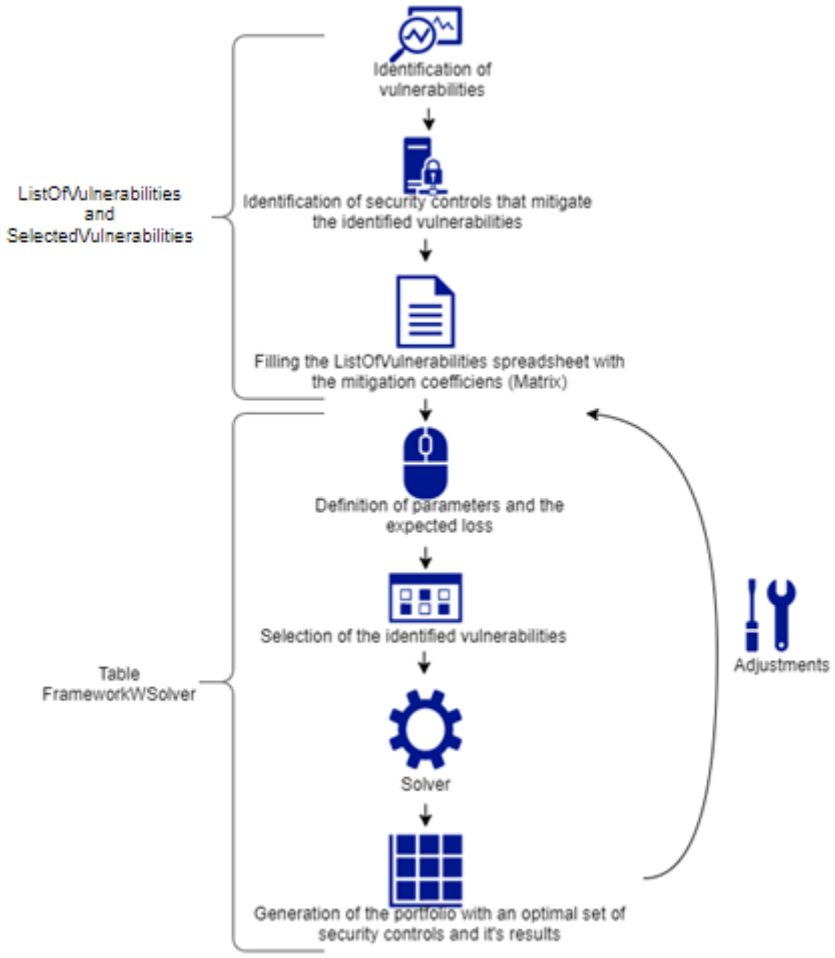

Figure 9 – Main steps to use the tool

The first step to use the tool consists in the identification of the vulnerabilities that will be considered in the Model. The second step consists in the identification of security controls that mitigate the vulnerabilities identified in the previous step. The third, and final step, corresponds to the filling of the Matrix table with 1 whenever a control mitigates a selected vulnerability, otherwise nothing will appear in the cell. For further knowledge, this tool contains a detailed list of vulnerabilities based on the study of both ISO/IEC Standards, more specifically on clauses nine, twelve and thirteen (Access control, Operations Security and Communications security).

In the spreadsheet 'TableFrameworkWSolver' takes place the fourth, fifth, sixth, seventh and eighth steps. Next, we will describe each one of them.

The fourth step consists in the definition of the parameters by the user, as it is presented in the Figure 9. The parameters that need to be defined are: Weight expected

loss, Available budget and Impact (Estimated Loss). The fifth step involves the selection of the vulnerabilities that were previously identified. With this, the cells will be mapped with '1' whenever a security control mitigates a vulnerability.

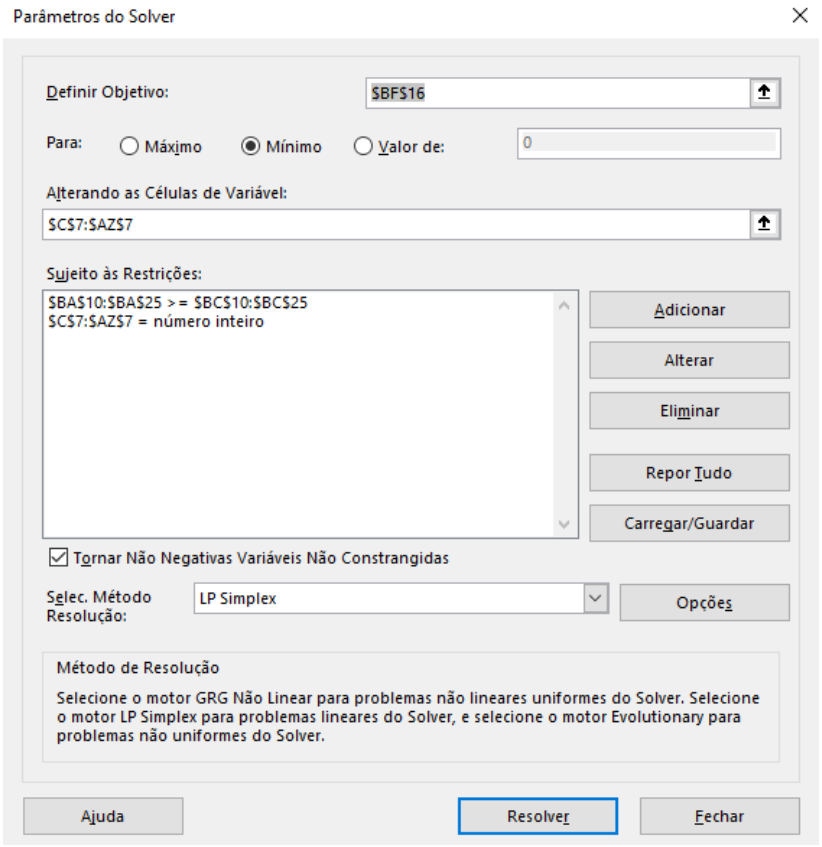

Figure 10 – Solver parameters

The sixth step consists on the execution of the Solver. Figure 10 shows the constraints that are used in the developed tool, which are important for the final result of the optimization function. Next, it will be described the meaning of each Solver component.

- $\$BF\$16$: This cell has the optimization function, in which the Solver will try to find the optimization value solution for the scenario that was defined.
- $\$C\$7:\$AZ\$7$: This is the range of cells that are going to be filled with '0' and '1', whenever a security control is selected to be in the portfolio that is generated with the Solver and corresponds to the variables values in the solution.
- $\$C\$7:\$AZ\$7 = número\ inteiro$: This constraint means that the cells between the range $\$C\$7:\$AZ\$7$ can only contain integer numbers.

- $\$BA\$10:\$BA\$25 \geq \$BC\$10:\$BC\$25$: This restriction means that for every vulnerability that is identified, there must be at least one security control that is chosen to do the mitigation of that same vulnerability.

The seventh step corresponds to the generation of the results for the portfolio. The eighth step involves all the adjustments that need to be made in order to have a more personalized output.

4.2.5 Visualization of results

After the user concludes the steps that are described in the previous section, 4.1.4, a personalized portfolio is proposed to match the data inserted.

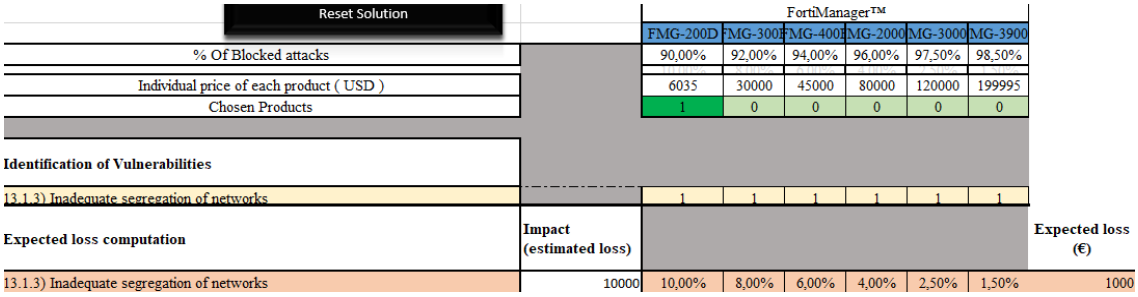

Figure 11 – Example of portfolio with security products for a proposed vulnerability.

Figure 11 represents the optimized solution of the portfolio that has been selected as solution. In this example, the first product was the optimal control selected (FMG-200 D) to mitigate the corresponding vulnerability (Inadequate segregation of networks).

Figure 11 also represents the table that corresponds to the computation of the expected loss. In this example, we defined the impact of this vulnerability with the value 10000. As long as the optimal security control for this solution is the first product, the expected loss will be 1000, because this product only assures 90% of coverage, leaving 10% of loss without mitigation. It is also important to emphasize that the percentages that are presented in the expected loss table, relate to the residual risk that is inherent in the implementation of the security control

Total Cost of the portfolio	6035	Weight cost	0,5
Available Budget	60000		
% of the budget used by the portfolio	10%		
Expected Loss (€)	1000	Weight expected loss	0,5
% Coverage by the controls in the portfolio	90,00%		
% Uncoverage by the controls in the portfolio	10,00%		
Optimization function	3517,5		
CBA (one year)	2965		

Figure 12 – Visualization of the parameters after the portfolio elaboration

This table is the most important tool in the framework. It allows the user to have an overall view of the suggested portfolio solution. By analysing Figure 12, we can see that there are important details such as the Expected Loss, Cost-Benefit Analysis, % of the budget available that were used in the current portfolio, the total cost of the portfolio and the % of both covered and uncovered protection that the products provide.

To make the evaluation of the optimal selection of security products to be included in the portfolio, the tool relies on the parameters total cost of the portfolio, expected loss and both of their weights. The Cost-Benefit Analysis(CBA) can also be important to assess the viability of the solution that is selected by the Solver. The Cost-Benefit Analysis determines if the security controls represented in the portfolio are worth its associated cost. That being said, the higher the value of the CBA, the better is the suggested solution.

% blocked attacks by FortiManager	Cost of FortiManager
90,00%	6035
% blocked attacks by FortiAnalizer	Cost of FortiAnalizer
0,00%	0
% blocked attacks by FortiAuthenticator	Cost of FortiAuthenticator
0,00%	0
% blocked attacks by FortiGate	Cost of FortiGate
0,00%	0
% blocked attacks by CheckPoint Security Gateway Appliances	Cost of CheckPoint Security Gateway Appliances
0,00%	0
% blocked attacks by DDoS Protector	Cost of DDoS Protector
0,00%	0
% blocked attacks by Policies 9.1.1	Cost of Policies 9.1.1
0,00%	0

Figure 13 – Overview of the security products selected in the portfolio

Figure 13 represents a table which is automatically filled when Solver selects the optimal security products that mitigate the vulnerabilities that were identified.

In the next Chapter, we will focus on the analysis of the tool, using three case-scenarios.

5 Discussion of case-studies

After the development of the tool was concluded, three case-scenarios were developed to compare and evaluate the output that the optimal portfolio offered to the framework user.

Case studies

The scenarios were elaborated in order to demonstrate how different weight values influence the final output of the optimization function. For a better consistency in the results that are provided, all the scenarios use the same vulnerabilities and the same value of impact for every vulnerability. Figure 14 shows the vulnerabilities that were used for those scenarios and Figure 15 shows the value of impact for every vulnerability that was selected.

Identification of Vulnerabilities
13.1.3) Inadequate segregation of networks
9.4.2) Inexistence of procedures to protect against brute force log-in attempts;
13.2.2) Inexistence of levels of access control;
9.1.1) Lack of policies for information dissemination and authorization
9.4.2) Inexistent records of log attempts;
12.2.1)Lack of procedures and responsibilities in case of malware attacks

Figure 14 – Vulnerabilities that were selected for the case scenarios

Expected loss computation	Impact (estimated loss)
13.1.3) Inadequate segregation of networks	15000
9.4.2) Inexistence of procedures to protect against brute force log-in attempt	15000
13.2.2) Inexistence of levels of access control;	15000
9.1.1) Lack of policies for information dissemination and authorization	15000
9.4.2) Inexistent records of log attempts;	15000
12.2.1)Lack of procedures and responsibilities in case of malware attacks	15000

Figure 15 – Expected loss of each vulnerability that was selected

Case scenario 1

In case scenario 1 we created a situation in where the priority was the minimization of the security controls cost. For that, we set the Weight cost parameter to 0, and the Weight of the expected loss parameter to 1.

Total Cost of the portfolio	1132395	Weight cost	0
Available Budget	60000		
% of the budget used by the portfolio	1887%		
Expected Loss (l)	1170	Weight expected loss	1
% Coverage by the controls in the portfolio	98,70%		
% Uncoverage by the controls in the portfolio	1,30%		
Optimization function	1170		
CBA (one year)	-1043565		

Figure 16 – Case scenario 1 results

Through the setting of both the weights, we can see the output of this scenario in Figure 16. If we take into account the Equation 8 (Section 3.4), and as long as we set w1 to 0, the result of the optimized function will be the same as the sum of the expected loss from each vulnerability, after the implementation of the security controls. As we can see in the expected loss metric, its value will be relatively low comparing to the total cost of the portfolio that was selected.

Doing an analysis to this solution, it is possible to say that this portfolio isn't viable because the total cost of the portfolio is higher than the available budget that was defined. Also, the cost-benefit analysis is negative, which translates in a bad portfolio solution.

Case scenario 2

In case scenario 2 was created a situation in where the priority will be the minimization of the expected loss from security controls. For that, we will set the Weight cost parameter to 1, and Weight expected loss parameter to 0.

Total Cost of the portfolio	54963	Weight cost	1
Available Budget	60000		
% of the budget used by the portfolio	92%		
Expected Loss (l)	11550	Weight expected loss	0
% Coverage by the controls in the portfolio	87,17%		
% Uncoverage by the controls in the portfolio	12,83%		
Optimization function	54963		
CBA (one year)	23487		

Figure 17 – Case scenario 2 results

Through the setting of both the weights, we can see the output of this scenario in Figure 17. Once again, if we take into account the Equation 8 (Section 3.4), and as long as we set the w2 to 0, the result of the optimized function will be the same as the Total cost of the portfolio parameter. As we can see in the total cost of the portfolio, its value will be relatively low comparing to the expected loss of the security controls that were selected.

Doing an analysis to this solution, it is possible to say that this portfolio is viable because the total cost of the portfolio is lower than the available budget that was defined. Besides that, the cost-benefit analysis is positive, which translates into a decent portfolio solution.

Case scenario 3

In case scenario 3 we created a situation in where both objectives will be balanced. For that, we will set the Weight % covered vulnerabilities parameter to 0.5 and Weight % uncovered vulnerabilities parameter to 0.5.

Total Cost of the portfolio	56463	Weight cost	0,5
Available Budget	60000		
% of the budget used by the portfolio	94%		
Expected Loss (l)	8700	Weight expected loss	0,5
% Coverage by the controls in the portfolio	90,33%		
% Uncoverage by the controls in the portfolio	9,67%		
Optimization function	32581,5		
CBA (one year)	24837		

Figure 18 – Case scenario 3 results

By the observation of this output, we can see that balanced parameters in both weights makes the optimized function hard to understand, as long as it can be used as a indicative value to compare different solutions. However, the higher the optimized function value, the worst is the solution that has been suggested by the framework.

Doing an analysis to this solution, it is possible to say that this portfolio is viable because the total cost of the portfolio is lower than the available budget that was defined. Besides that, the cost-benefit analysis is positive, which translates into a decent portfolio solution.

Scenario 2 and scenario 3 are the only ones that have a viable portfolio, as long as their cost-benefit analysis is positive and the total cost of the portfolio is lower than the available budget. However, doing a comparison to both those scenarios, we can say that the scenario 3 is a better solution than scenario 2.

6 Conclusions and future work

This chapter presents the conclusions about the work that has been developed for the present work, as well as the future work that could be done in the tool, in order to improve its functionality.

6.1 Conclusions

The work developed aims to respond to the existing need that can occur in organizations, by providing a decision support system to implement mechanisms that allow the creation or improvement of information security measures and products. With the approach of this work, it is expected that this tool supports the selection of the optimal portfolio solution for a set of vulnerabilities.

In the current work, it was developed a framework to support the decision making of an organization in mitigating various vulnerabilities that could compromise the natural behaviour of a company, with the implementation of a set of chosen security controls.

Throughout the work there were a number of challenges that were key to the development of the decision support tool. That been said, we will briefly describe why and when they existed.

One of the challenges was the need to structure the relation between both standards, ISO/IEC 27001:2013 and ISO/IEC 27002:2013, understanding the scope and purpose of the standards. This challenge becomes particularly relevant, since the identification of vulnerabilities will be obtained from the study that was done in both Standards.

The biggest challenge is due to the fact that initially it was designed to make a decision support for all the clauses present in both of the Standards. However, it quickly became apparent that it was not feasible due to the extensive research and knowledge of concepts that needed to be accomplished for the time available. Since the present work is a proof of concept and in agreement with the project Coordinator, the points related to Access Control, Operations Security and Security of Communications were prioritized.

A limitation that is present in this work is due to the fact that there is a lack of results that can be obtained. This is largely due to the fact that the current project acts as proof of concept and the absence of results that can act as a comparison.

The work developed in the present tool is intended to assist the decision making on an organization. The ultimate goal is to mitigate existing vulnerabilities that were raised through the analysis of the Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013, by a set of security controls. For this, it is integrated a linear programming bi-objective model in the tool, with the purpose of minimizing the cost of the security controls and the impact of an attack through vulnerabilities. The existence of weights for each objective makes it possible to have multiple scenarios for a more personalized and accurate environment.

The author believes that the developed work is capable of responding to the needs of an organization by doing an evaluation and prioritization of security controls for a set of vulnerabilities. With this approach, it is believed that the user can make different assessments and generate personalized scenarios by changing the available bi-objective weights.

6.2 Future work

This work can serve as a reference for organizations that want to use a decision support system, and that consider the ideas and functionalities implemented in the tool as interesting.

There's still much work to be done, especially if there is a need to incorporate more clauses that are present in ISO/IEC 27001:2013 and ISO/IEC 27002:2013. The developed tool only considers the clauses nine, twelve and thirteen due to the high volume of information that is obtained when using the tool, restricted by the Solver.

If an organization wants to adapt this tool and expand it to other clauses of ISO/IEC 27001:2013 and ISO/IEC 27002:2013, it would be possible by creating a spreadsheet for each of the clauses of the standards. With this solution, it would be possible to optimize a portfolio for security controls for each clause, by running the solver solution in each spreadsheet. In the end, the tool would incorporate the results with a set of weights, in order to prioritize the implementation of controls by each clause.

Other features that would improve the current tool would be the inclusion of other information for the optimal portfolio, besides the cost of each control and the percentage of mitigation provided by them.

7 Acronyms

COBIT – Control Objectives for Information and Related Technologies

DDoS – Distributed Denial of Service Attack

DSS – Decision Support Systems

E.g. – Exempli Gratia = For example

Et al. – Et alia = And others

IEC – International Electrotechincal Commission

IDS – Intrusion Detection Systems

IPAC – Instituto Português de Acreditação

IPS – Intrustion Prevention System

ISMS – Information Security Management System

ISO – International Organization for Standardization

IT - Information Technology

ITIL – Information Technology Infrastructure Library

NGFW – Next-Generation Firewall

VBA – Visual Basic for Applications

8 References

Boehmer, W. (2008). *Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001*. In Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference (pp. 224-231). IEEE

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk management*, *54*(1), 24.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13-23.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27-47.

IPAC (2017). Base de dados nacional – Sistemas de gestão certificados, Instituto Português de Acreditação. Retrieved November 02, 2017, from http://www.ipac.pt/pesquisa/pesq_empcertif.asp

ISO/IEC.(2013). ISO/IEC 27001:2013 *Security Technologies – Information Security Management Systems – Requirements*. International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC (2013). ISO/IEC 27002:2013 *Information Technology-Security Techniques – Code of practice for Information Security Controls.* International Organization for Standardization and International Electrotechnical Commission.

Kiesling, E., Ekelhart, A., Grill, B., Strauss, C., & Stummer, C. (2016). Selecting security control portfolios: a multi-objective simulation-optimization approach. *EURO Journal on Decision Processes*, 4(1-2), 85-117.

Khatavakhotan, A. S., & Ow, S. H. (2012). *An innovative model for optimizing software risk mitigation plan: A case study*. In Modelling Symposium (AMS), 2012 Sixth Asia (pp. 220-224). IEEE

Kosutic, Dejan (Unknown Year). *Four key benefits of ISO 27001 implementation.* Retrieved April 21, 2017, from

https://advisera.com/27001academy/knowledgebase/four-key-benefits-of-iso-27001-implementation

Mattes, Í. V., Petri, S. M., & da Rosa, M. M. (2015). *Segurança da informação contábil: Procedimentos para elaboração de uma política de segurança com base na ISO 27001 e ISO 27002*. In Revista Interdisciplinar Científica Aplicada, *9*(4), 39-60

Nunes, S., Dhillon, G., & Caldeira, M. M. (2015). Multi-Objective Decision Model for Information Systems Risk. In UK Academy for Information Systems Conference Proceedings (p. 7).

Palhares, C. (2011). *Governança de TI: Cenário Atual Das Instituições De Ensino Superior Brasileiras*. (Master Dissertation). Centro Estadual de Educação Tecnológica Paula Souza, Brasil.

Pandini, W (Unknown Year). *ISO 27002: Boas práticas para a gestão de segurança da informação*. Retrieved 21 April, 2017, https://blog.ostec.com.br/padronizacao-seguranca/iso-27002-boas-praticas-gsi

Power, D. J. (2000). Web-based and model-driven decision support systems: concepts and issues. *AMCIS 2000 Proceedings*, 387.

Power, D. J. (2001). *Supporting decision-makers: An expanded framework*. Proceedings of Informing Science and IT Education. PP 1901-1915

Power, D.J. (2007). *A Brief History of Decision Support Systems*. Retrieved 18 April, 2017, http://dssresources.com/history/dsshistory.html

Power, D. J., & Sharda, R. (2007). Model-driven decision support systems: Concepts and research directions. *Decision Support Systems*, *43*(3), 1044-1061.

Power, D.J. (2008). Understanding data-driven decision support systems. *Information Systems Management*, 25(2), 149-154

Santos, V. (2012). *Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001: 2006, 27002: 2005 e 27005: 2008*

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, *55*(1), 156-164.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology. IJET Publications UK*, *2*(1).

Veronica, R. R. (2007). Decision Support System Development. *Journal of the Facultyof Economics*, *2*, 882-885.

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & van Moorsel, A. (2015). Selecting optimal subset of security controls. *Procedia Computer Science*, *64*, 1035-1042.

Yevseyeva, I., Fernandes, V. B., van Moorsel, A., Janicke, H., & Emmerich, M. (2016). Two-stage Security Controls Selection. *Procedia Computer Science*, *100*, 971-978.

9 Annex – Tool Layout

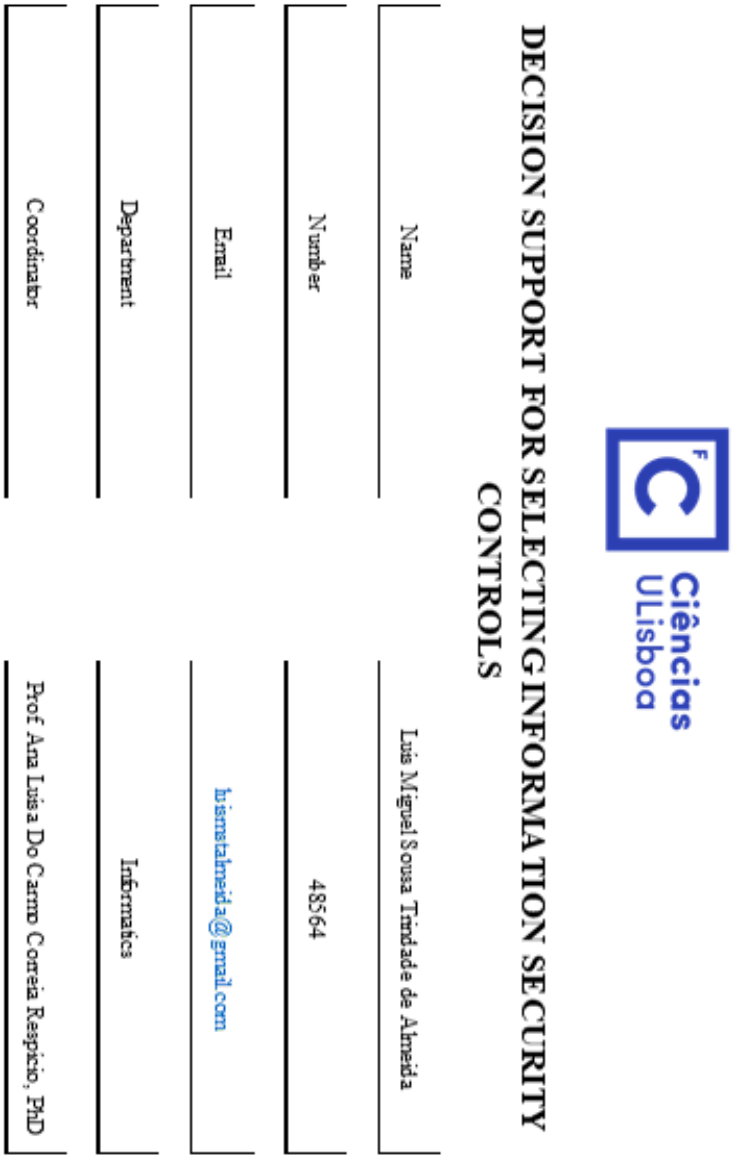

Figure 19 – Introduction spreadsheet

Ciências ULisboa

Introduction

The objective of this work is to optimize the security products portfolio and thus to provide decision support for selecting information security controls using international Standards such as the ISO/IEC 27001:2013 (ISO/IEC, 2013 a) and ISO/IEC 27002:2013 (ISO/IEC, 2013 b). It is intended that the use of this framework aims to assist decision making in order to prioritize information security controls, which have the ultimate goal of mitigate existing vulnerabilities that are already identified in the organization. For this, it is integrated a bi-objective model in the tool, with the purpose of minimizing the cost of the security controls and the impact (estimated loss) of an attack through a vulnerability that has already been protected.

Description of the spreadsheets

• CheckpoitProducts - This spreadsheet contains detailed information about the security products that are suggested from Checkpoint, as long as they mitigate some of the

• FortinetProducts - This spreadsheet contains detailed information about the security products that are suggested from Fortinet as long as they mitigate some of the vulnerabilities in study.

• ControlsByGroup - The "Controls_By_Group" spreadsheet increases user awareness about which vulnerabilities are present in the tool, as well as the generic and specific controls can be used to mitigate them.

• ListOfVulnerabilities - This spreadsheet contains a table that crosses the vulnerabilities identified with the set of several selected appliances. With this, is possible to indicate which vulnerabilities can be mitigated with the security controls that are provided. Taking into account the aforementioned in the Section 3.4, to establish the mapping between the identified vulnerabilities and the security controls, the "ListOfVulnerabilities" creates a matrix mapping with vulnerabilities and controls in columns, filling the number '1' whenever the control mitigates the selected vulnerability. With this approach, we provide a model that is

• SelectedVulnerabilities - This Spreadsheet have the exact same purpose as the previous spreadsheet (ListOfVulnerabilities). However, as long as it was identified 73 vulnerabilities, and most of them can be mitigated through the implementation of procedures and policies, "SelectedVulnerabilities" contains just the vulnerabilities that are mitigated through the

• TableFrameworkWSolver - This Spreadsheet contains the fundamental table of this tool, since it contains the representation of the model and over which the solver will act. After selecting the vulnerabilities that were discovered, the user is allowed to define the minimum mitigation percentage that is considerable for the choice of computer products, as well as the attribution of weights related to the importance that is given to the optimization of costs

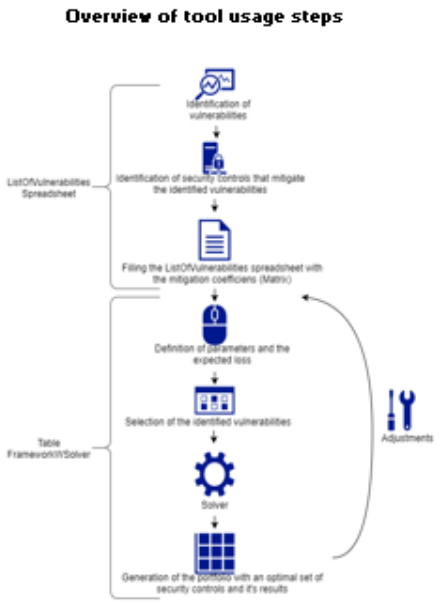

Figure 20 – Scope Spreadsheet

		DDoS Protector									
		506	1006	2006	4412	8412	12412	10420	20420	30420	40420
Performance	Capacity (Gbps)	0,5	1	2	4	8	14	10	20	30	40
	Throughput (Gbps)	0,5	1	2	4	8	12	10	20	30	40
	Max Concurrent Sessions (M)	2	2	2	4	4	4	6	6	6	6
	Max DoS Flood Attack Prevention Rate (M)(pps)	1	1	1	10	10	10	25	25	25	25
	Latency	<50 ms									
	Real-time Signatures	Detect and protect against attacks in less than 18 secs									
Network	10/100/1000 Copper	4	4	4	8	8	-	-	-	-	-
	1 GbE Fiber (SFP)	2	2	2	4	4	4	-	-	-	-
	10 GbE Fiber (XFP)	-	-	-	4	4	4	-	-	-	-
	1/10 GbE (SFP+)	-	-	-	-	-	-	20	20	20	20
	40 GbE (QSFP+)	-	-	-	-	-	-	4	4	4	4
Operation Mode	Network Operation	Transparent L2 forwarding									
	Deployment Modes	In-line; span port monitoring; copy port monitoring; local out-of-path; out-of-path mitigation (scrubbing center solution)									
	Tunneling protocols support	VLAN Tagging, L2TP, MPLS, GRE, GTP									
	IPv6	Support IPv6 networks and block IPv6 attacks									
	Policy Action	Block and Report; Report Only									
	Block Actions	Drop packet; reset (source, destination, both); suspend (source, source port, destination, destination port or any combination); Challenge-Response for HTTP and DNS attacks									
High Availability	Fail-open/Fail-close	Internal fail-open/fail-close for copper ports;		Internal fail-open/fail-close for copper ports;				Internal fail-close for SFP+ and QSFP+ ports;			
	Clustering	Active-Passive Cluster									
Physical	Enclosure	1U						2U			
Power	Dual Power Supply	Optional						Yes - Hot Swappable			
	Power Consumption (Max)	177W			476W			634W			
	Price	33000	40000	65000	120000	170000	210000	233350	333350	433350	533350

Figure 21 – CheckpointProducts Spreadsheet (1)

		Security Gateway Appliances			
		3100	15600	23500	23800
Real-World Production Conditions	SecurityPower	160	3250	5500	6300
	Firewall (Gbps)	2,1	30	34	43
	IPS Throughput (Gbps)	350 Mbps	8	10	12
	NGFW Throughput (Gbps)	220 Mbps	5,2	6,3	7,2
	Threat Prevention (Gbps)	130 Mbps	3	3,955	4,5
Ideal Testing Conditions	Firewall Throughput (Gbps)	4	76	116	128
	Connections Per Second (K)	40	185	200	200
	Concurrent Sessions (M)3	3,2	6,4/25,6	6,4/51,2	12,8/51,2
	VPN Throughput (Gbps)	1,7	15,8	26	26
	IPS Throughput (Gbps)	1,1	18	22	30
	NGFW Throughput (Gbps)1	850 Mbps	17	20	27
	Threat Prevention (Gbps)2	425 Mbps	13,11	17	18,6
Additional Features	CPUs/phtysical cores/virtual cores (total)	01/04/004	2/18/32	2/20/40	2/24/48
	Storage	x 320GB HDD or 240GB SSI		2x1TB HDD or 480GB SSD RAID1	
	Memory Options (GB)	8	16,32,64	16,64,128	32,64,128
	LOM Card	NA	INCLUDED	INCLUDED	INCLUDED
Power	Hot-Swappable Power Supplies	NA	AC or DC	AC or DC	AC or DC
	Power Input	110-240VAC, 47-63 Hz	110-240VAC (47-63Hz); -40.5VDC/24A -48VDC/19.2A, -60VDC/16.0A		
	Single Power Supply Rating	40W	AC(550W), DC(800W)	800W	800W
	Power Consumption (Max)	29,5W	297W\	383W	399W
	Price	4900	94000	142000	175000

Figure 22 – CheckpointProducts Spreadsheet (2)

Observation: Due to the size of this table, several columns have been hidden.

Source for prices:http://www.avfirewalls.com/	FortiManager™ - Centralized Management Platform					
	FMG-200D	FMG-300E	FMG-400E	FMG-2000E	FMG-3000F	FMG-3900E
Max Licensed Devices/Adoms	30	100	300	1200	4000	10000
Sustained Log Rates	50	50	50	50	150	150
GB/Day	2	2	2	2	10	10
Total Interfaces	4x GE RJ45	4x GE RJ45	4x GE RJ45	4x GE, 2x GE SFP	4x GE, 2x GE SFP+	2x GE, 2x GE SFP+
Storage Capacity	1x 1 TB	4x 3 TB	8x 3 TB	12x 3 TB	16x 3 TB	15x 1 TB
Price	**$6,035.78**	**$30,000.00**	**$45,000.00**	**$80,000.00**	**$120,000.00**	**$199,995.00**

Source for prices:http://www.avfirewalls.com/	FortiAnalizer™ - Centralized Logging & Reporting Solution						
	FAZ-400E	FAZ-1000E	FAZ-2000E	FAZ-3000F	FAZ-3500F	FAZ-3700F	FAZ-3900E
GB Logs/Day	200	600	1000	3000	5000	8300	4000
Analytic Sustained Rate (logs/sec)	6000	18000	30000	42000	63000	100000	72000
Collector Sustained Rate(logs/sec)	9000	27000	45000	60000	90000	150000	108000
Max. Licensed Devices/VDOMs/ADOMs	200	2000	2000	4000	10000	10000	10000
Max Number of Days Analytics	30	30	30	21	30	60	5
Total interfaces	4x GE RJ45	2x GE RJ45	GE RJ45, 2x GE S	GE RJ45, 2x GE S	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x GE SFP+	x GE RJ45, 2x GE SFP+
Storage Capacity	4x 3 TB	8x 3 TB	12x 3 TB	16x 3 TB	24x 3 TB	60x 4TB SAS	15x 1 TB (SSD)
RAID Support	RAID 0, 1, 5, 10	AID 0, 1, 5, 6, 10, 50,	AID 0, 1, 5, 6, 10, 50,	ID 0, 1, 5, 6, 10, 50,	RAID 0, 1, 5, 6, 10, 50, 60	RAID 0, 1, 5, 6, 10, 50, 60	RAID 0, 1, 5, 6, 10, 50, 60
FortiGuard Indicator of Compromise(IOC)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FortiManager Capabilities(up to 20 devices)	No	Yes	Yes	Yes	Yes	Yes	Yes
Price	**$9,000.00**	**$20,000.00**	**$30,000.00**	**$50,000.00**	**$60,000.00**	**$150,000.00**	**$99,995.00**

Source for prices:http://www.avfirewalls.com/	FortiAuthenticator™ - User Identity Management Server				
	FAC-200E	FAC-400E	FAC-1000D	FAC-2000E	FAC-3000D/3000E
Max Local/Remote Users/User Group	500 / 500 / 25	2,000 / 2,000 / 50	,000 / 10,000 / 2,0	0,000 / 20,000 / 2,0	40,000 / 40,000 / 4,000
Max NAS Devices	50	200	1000	2000	4000
Max FortiTokens	500	2000	10000	20000	40000
Interfaces	4x GE RJ45	4x GE RJ45	4x GE RJ45, 2x SFP	x GE RJ45, 2x SFI	4x GE RJ45, 2x SFP
Storage Capacity	1x 1 TB	2x 1 TB	2x 2 TB	2x 2 TB	2x 2 TB
Price	**$3,998.00**	**$8,495.00**	**$17,995.00**	**$27,500.00**	**scontinued/$38,500.00**

Source for prices:http://www.avfirewalls.com/	FortiGate® - Network Security Platform					
	FG-30E	FG-90D	FG-300D	FG-1200D	FG-3100D	FG-3980E
Firewall Throughput (1518/512/64 byte UDP)	0.95 Gbps	3.5 / 3.5 /3.5 Gbps	8 / 8 / 8 Gbps	72 / 72 / 50 Gbps	80 / 80 / 50 Gbps	1.05 Tbps / 1.05 Tbps / 680 Gbps
Firewall Latency	130 µs	4 µs	3 µs	3 µs	3 µs	3 µs
Concurrent Sessions	900.000	2 Million	4 Million	11 Million	50 Million	160 Million
New Sessions/Sec	15.000	4.000	200.000	290.000	400.000	550000
Firewall Policies	5.000	5.000	10.000	100.000	200.000	200000
IPsec VPN Throughput (512 byte)	75 Mbps	1 Gbps	7 Gbps	40 Gbps	50 Gbps	400 Gbps
Max G/W to G/W IPSEC Tunnels	200	200	2.000	20.000	40.000	40000
Max Client to G/W IPSEC Tunnels	250	2.500	50.000	100.000	200.000	200000
SSL VPN Throughput	35 Mbps	35 Mbps	350 Mbps	3.6 Gbps	8 Gbps	9.5 Gbps
Concurrent SSL VPN Users (Recommended Max	80	200	500	10.000	30.000	32 Gbps
IPS Throughput 1 (HTTP / Enterprise Mix)	600/300 Mbps	275/50 Mbps	2.8 / 2 Gbps	11/6.8 Gbps	45/22 Gbps	82/32 Gbps
SSL Inspection Throughput (IPS, HTTP)	160 Mbps	18 Mbps	1.9 Gbps	6 Gbps	22 Gbps	32 Gbps
Application Control Throughput (HTTP 64K)	400 Mbps	100 Mbps	4 Gbps	15 Gbps	40 Gbps	55 Gbps
NGFW Throughput	200 Mbps	30 Mbps	1.7 Gbps	6 Gbps	18 Gbps	28 Gbps
Threat Protection Throughput	150 Mbps	25 Mbps	1.5 Gbps	4 Gbps	13 Gbps	18.5 Gbps
Max FortiAPs (Total / Tunnel)	2/1/	32 /16	512/256	4096/1024	4096/1024	4096/1024
Max FortiSwitches	8	8	48	128	256	-
Max FortiTokens	20	100	1.000	5.000	5000	5000
Max Registered FortClient	200	200	600	20.000	50000	20000
Virtual Domains (Default/Max)	5/5/	10/10/	10/10/	10/250	10/500	10/500
Interfaces	5x GE RJ45	16x GE RJ45	GE RJ45, 4x GE S	GE SFP, 16x GE SF	GE SFP+/GE SFP, 2x GE	x 100GE QSFP28, 16x 10GE SFP+, 2x GE RJ45
Local Storage	-	32 GB	120 GB	240 GB	480GB	-
Power Supplies	Single AC PS	Single AC PS	gle AC PS, opt. Ext	Dual PS	Dual PS	3 PS
Form Factor	Desktop	Desktop	1 RU	2 RU	2 RU	5 RU
Variants	WiFi, 3G4G	DE, LENC, High Port	LENC	-	DC	-
Price	**$430.00**	**$1,198.00**	**$5,000.00**	**$25,000.00**	**$60,000.00**	**$190,000.00**

Figure 23 – Fortinet Products Spreadsheet

9) Access Control	Control
9.1) Business requirements of access control	
9.1.1) Access control policy	
9.1.1) Inexistence of security requirements for business applications	Policy 9,1,1 #1 / Policy 9.1.1 #2 / Procedures 9.1.1 #1 / Procedures 9.1.1 #2
9.1.1) Lack of policies for information dissemination and authorization	Policy 9,1,1 #1 / Policy 9.1.1 #2
9.1.1) Lack of policies for periodic review and removal of access rights	Policy 9,1,1 #1 / Policy 9.1.1 #2
9.1.2 Access to networks and network services	
9.1.2) Lack of procedures for determining who is allowed to access which networks and network services	Procedures 9.1.2 #1 / Procedures 9.1.2 #2
9.1.2) Lack of policies to manage controls and procedures to protect access to network connections and network services	Policy 9,1,2 #1 / Policy 9,1,2 #2
9.2)User access management	
9.2.1)User registration and de-registration	
9.2.1) Not using/verifcation for single users Ids to control their responsibilities;	Procedures 9.2.1 #1 / Procedures 9.2.1 #2
9.2.1) Lack of procedures to remove the IDs of users who left the organization;	Procedures 9.2.1 #1 / Procedures 9.2.1 #2
9.2.2)User access provisioning	
9.2.2) Inexistent verification of the access level granted for a user.	FortiAuthenticator™ (Fortinet)
9.2.2) Inexistent of a central record of access to a user ID to access information system and services	FortiAnalizer™ (Fortinet)

12)Operations security	Control
12.1) Operating procedures and responsabilities	
12.1.1) Documented operating procedures	
No existence of backup	FortiManager™ (Fortinet)
The procedures aren't monitored	FortiManager™ (Fortinet)
Lack on scheduling requirements	Policy 12.1.1 #1 / Policy 12.1.1 #2 / Procedures 12.1.1 #1 / Procedures 12.1.1 #2
12.1.2) Change management	
Lack on scheduling requirements	Policy 12.1.2 #1 / Policy 12.1.2 #2 / Procedures 12.1.2 #1 / Procedures 12.1.2 #2
Poor planning or testing of changes	Policy 12.1.2 #1 / Policy 12.1.2 #2 / Procedures 12.1.2 #1 / Procedures 12.1.2 #3
Inadequate record of important changes in business processes	Policy 12.1.2 #1 / Policy 12.1.2 #2 / Procedures 12.1.2 #1 / Procedures 12.1.2 #3
Poor planning or testing of changes	Policy 12.1.2 #1 / Policy 12.1.2 #2 / Procedures 12.1.2 #1 / Procedures 12.1.2 #3
12.1.3) Capacity management	
Insufficient optimization for the resource-hungry services.	Policy 12.1.3 #1 / Policy 12.1.3 #2 / Procedures 12.1.3 #1 / Procedures 12.1.3 #2
12.1.4) Separation of development, testing and operational environments	
Development and operational software can only run in a single system/computer	Policy 12.1.4 #1 / Policy 12.1.4 #2 / Procedures 12.1.4 #2 / Procedures 12.1.4 #3
Single profile for both operational and testing systems	Policy 12.1.4 #1 / Policy 12.1.4 #2 / Procedures 12.1.4 #2 / Procedures 12.1.4 #4

13) Communications security	Control
13.1)Network security management	
13.1.1) network controls	
Inexistence of responsabilities and procedures for the management of networking equipment.	Policy 13.1.1 #1 / Policy 13.1.1 #2
Lack of system authentication over the network	FortiAuthenticator™ (Fortinet)
There is no network restrictions over the system connections	FortiManager™ (Fortinet)
13.1.3) Segregation of networks	
Inadequate segregation of networks	FortiManager™ (Fortinet)
13.2) Information transfer	
13.2.1) Information transfer policies and procedures	
Inexistence of procedures and policies for protection of malware, copying and modification of information	Policy 13.2.1 #1 / Policy 13.2.1 #2 / Procedures 13.2.1 #1 / Procedures 13.2.1 #2
Lack of guidelines to protect transferred information from interception, copying, modification, mis-routing and destruction.	Policy 13.2.1 #1 / Policy 13.2.1 #2
Inexistence of cryptographic techniques to protect the confidentiality, integrity and authenticity of information;	FortiGate™ (Fortinet) / Security Gateway Appliances (CheckPoint)
13.2.2) Agreements on information transfer	
Leakage of agreements of business information between organizations and external parties	Policy 13.2.2 #1 / Policy 13.2.2 #2
Lack of procedures to ensure traceability and non-repudiation;	FortiAnalizer™ (Fortinet) / FortiGate™ (Fortinet) / Security Gateway

Figure 24 – ControlsByGroup Spreadsheet

Observation: Due to the size of this table, several columns have been hidden.

Vulnerabilities\Threats	Security Appliances						
	FortiManager™ (Fortinet)		FortiAnalizer™ (Fortinet)		FortiAuthenticator™ (Fortinet)	FortiGate™ (Fortinet)	Appliances
	FMG-200D	FMG-300E	FAZ-400B	FAZ-1000E	FAC-200E	FG/FWF-30E	3100
9.1.1) Inexistent security requirements for business applications							
9.1.1) Lack of policies for information dissemination and authorization							
9.1.1) Lack of policies for periodic review and removal of access rights							
9.1.2) Lack of procedures for determining who is allowed to access which networks and network services							
9.1.2) Lack of policies to manage controls and procedures to protect access to network connections and network services							
9.2.1) Not using verification for single users Ids to control their responsibilities;							
9.2.1) Lack of procedures to remove the IDs of users who left the organization;							
9.2.2) Inexistent verification of the access level granted for a user.					1		
9.2.2) Inexistence of a central record to access a user ID information about utilized system and services			1	1			
9.2.3) Poor procedures to avoid the unauthorized use of generic administration user IDs.					1		
9.2.3) Disclosure of generic administration user IDs.						1	1
9.2.4) Lack of procedures to verify the identity of a user prior to providing new or temporary secret					1		
9.2.4) Inexistent procedure to require a user to sign a statement to keep personal secret authentication					1		
9.2.4) Poor level of power/multiple secret authentication information.					1		
9.2.5) Inadequate moving or re-allocation of user access rights to users.							
9.2.5) Lack of policies to review privileged access rights at a more frequent intervals.							
9.2.6) Inexistence of policies to remove access rights to internal/external users upon termination of their employment.							
9.3.1) Poor user awareness to keep secret authentication information confidential.							
9.3.1) Inadequate record of secret information secret;					1		

Figure 25 – ListOfVulnerabilities Spreadsheet

Observation: Due to the size of this table, several columns have been hidden.

Vulnerabilities/Threats	FortiManager™ (Fortinet)						FortiAnalizer™ (Fortinet)						
	FMG-2000D	FMG-300E	FMG-400E	FMG-2000E	FMG-3000F	FMG-3900E	FAZ-400E	FAZ-1000E	FAZ-2000E	FAZ-3000F	FAZ-3500F	FAZ-3700F	FAZ-3900E
3.1.1) Lack of policies for information dissemination and authorization													
3.2.2) Inexistent verifying of the access level granted for a user;							1	1	1	1	1	1	1
3.2.2) Inexistence of a central record to access a user ID information about utilized system and													
3.2.3) Poor procedures to avoid the unauthorized use of generic administration user IDs;													
3.2.3) Disclosure of generic administration user IDs;													
3.2.4) Lack of procedures to verify the identity of a user prior to providing new or temporary													
3.2.4) Inexistent procedure to require a user to sign a statement to keep personal secret													
3.2.4) Poor level of power/multiple secret authentication information.													
3.3.1) Inadequate record of secret information secret;													
3.4.1) Inexistence of menus to control access to application system functions;	1	1	1	1	1	1							
3.4.2) Inexistence of procedures to protect against brute force log-in attempts;													
3.4.2) Inexistent records of log attempts;							1	1	1	1	1	1	1
3.4.2) Lack of procedures to cover the password while it is being entered.													
3.4.3) Lack of procedures to ensure the quality of password;													
3.4.3) Lack of procedures to ensure regular password changes;													
3.4.3) Inadequate record of previously used password by each user, and prevent the re-use of													
3.4.3) Inexistence of procedures to store the password files in a separated location from the													

Figure 26 – Selected Vulnerabilities Spreadsheet

Observation: Due to the size of this table, several columns have been hidden.

Figure 27 – TableFrameworkWSolver (1)

Total Cost of the portfolio	0	Weight cost 0,5
Available Budget	0	
% of the budget used by the portfolio		
Expected Loss (€)	0	Weight expected loss 0,5
% Coverage by the controls in the portfolio		
% Uncoverage by the controls in the portfolio		
Optimization function	0	
CBA (one year)	0	

% blocked attacks by FortiManager	Cost of FortiManager
0,00%	0
% blocked attacks by FortiAnalizer	Cost of FortiAnalizer
0,00%	0
% blocked attacks by FortiAuthenticator	Cost of FortiAuthenticator
0,00%	0
% blocked attacks by FortiGate	Cost of FortiGate
0,00%	0
% blocked attacks by CheckPoint Security Gateway Appliances	Cost of CheckPoint Security Gateway Appliances
0,00%	0
% blocked attacks by DDoS Protector	Cost of DDoS Protector
0,00%	0
% blocked attacks by Policies 9.1.1	Cost of Policies 9.1.1
0,00%	0

Figure 28 – TableFrameworkWSolver (2)