CORVINUS UNIVERSITY OF BUDAPEST

A NOVEL APPROACH FOR INFORMATION SECURITY RISK ASSESSMENT MATURITY FRAMEWORK BASED ON ISO 27001

Ph.D DISSERTATION

Supervisor: Andrea Kő, Ph.D.

Blerton Abazi

Budapest

2020

Blerton Abazi

A novel approach for information security risk assessment maturity framework based on ISO 27001

Department of Information Systems

Supervisor: Andrea Kő, Ph.D.

Corvinus University of Budapest

Business Informatics Doctoral School

A novel approach for information security risk assessment maturity framework based on ISO 27001

Ph.D Dissertation

Blerton Abazi

Budapest

2020

Contents

Table of Figures

Table of Tables

Acknowledgment

First and foremost, I have to thank my parents **Sefedin** and **Letafete,** for their love and support throughout my life. Thank you for giving me the strength to reach for the stars and chase my dreams. My brother **Bardhyl** deserve my wholehearted thank as well.

This dissertation is dedicated to my wife **Saemira** and my little boy **Shkëmb** whose unyielding love, support, and encouragement have enriched my soul and inspired me to pursue and complete this research

I want to thank my supervisor, prof sincerely. **Andrea Kő**, for her expertise, guidance, and support throughout this study, especially for her confidence to me, made it possible for me to work on a topic that was of my great interest. It was a pleasure working with her.

I am grateful to prof. **Edmond Hajrizi** Rector of the University for Business and Technology – UBT for being a constant source of motivation and for helping me shape up my academic skills.

To all my friends, thank you for your understanding and encouragement in my many moments of difficulties. Your friendship makes my life a wonderful experience. I cannot list all the names here, but you are always on my mind.

Thank you, GOD, for always being there for me.

1. Introduction

The overall infrastructure of Information Technology (IT) is nowadays of central importance for nearly all organizations and companies, even those outside of the IT sector. After all, almost all business processes in organizations are supported by information technologies, including both core processes and supporting processes. Core processes can be considered in terms of mechanisms such as manufacturing, purchasing, or distribution, whereas supporting processes exist and function, such as the working time administration or payroll. Notably, every organization is responsible and accountable for safekeeping of confidential information, such as employee data or secret construction plans, and these are managed with the help of effective IT systems.

Numerous regulations and laws dictate and guide secure and reliable IT operations. In many sectors, there is a desire for a consistent level of security, primarily due to networking with suppliers or partners. Current threats, complex espionage programs, and data theft, such as the ones experienced by Sony, Yahoo, Visa, Deutsche Telekom, and Hotmail, demonstrate information security risks have become a real corporate threat. To prevent the unwanted outflow of business-critical information, it is not only vital to consider concrete technical measures, but it is also necessary to find a total package of technical, organizational, physical, procedural, and personnel measures. These must be implemented on a consistent and holistic basis and managed efficiently and effectively. Therefore, to address the many aspects of such holistic protection of business-related information, and an organization's information security activities, it is critical to have in place an information security management system.

Security risk and metrics monitoring approach and solution should be available to IT and other business leaders, supporting risk identification quickly, and providing recommendations according to that. Data is the key element of most businesses today, and the volume of data continues to grow by fifty percent a year, along with an increase in server numbers by twenty percent each year. According to Gartner (2016), the data center develops, in the same way, the risk of data manipulation opportunities increases. The rapid development of IT and the transformation of society and digital businesses results in the tremendous growth of data security. As such, more and more information security challenges are faced, and the more sophisticated they become. Information security within an organization requires information to be protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access

when required (availability). Businesses and organizations are therefore responsible for information security, and continuously develop systems and update their existing systems to provide secure solutions that are attack ready. The majority of software newly launched to the market possess new and unique features. However, they also carry with them several weaknesses that can be harmful. The problems experienced cannot be fixed quickly, as the systems are complex. Making changes within the system structure need to be verified, as it can affect some other part of the system, requiring a deep level of knowledge to address and implement.

In recent years, businesses and organizations have increased their use of cloud services, narrowing the gap between internal and external networks, to the point where the difference is almost non-existent. However, an unwavering trust in the cloud will increase the possibility of more attacks in this system. Additionally, the advent of many new digital devices in the market has made it difficult for organizations to use traditional, widespread methods of data protection. McAfee (2017) report on threat predictions, recognizes seven major challenges facing the information security industry:

- Threat defense effectiveness
- Reducing the asymmetry of information
- Making attacks more expensive or less profitable
- Improving visibility
- Identifying the exploitation of legitimacy
- Protecting decentralized data
- Detecting and protecting without agents

For this reason, businesses and organizations in the private and public sectors must deal with risk management and develop and maintain the related processes for their systems in a proactive manner.

The main research goal of the thesis is to provide a new framework for a maturity model in the field of information security risk assessment. The new framework supports the enterprises analyzing their security maturity level and is based on the ISO 27001 but also could be further utilized with the related standards. This related risk management solution is a web-based software application and is validated by companies from banks, IT, and insurance companies. As part of the research, I have developed a questionnaire with organizations' experts to identify the current level of security in the sectors mentioned

above. The survey was filled in by organizations from the banking sector, IT industry, and insurance organizations and showed a significant difference between sectors in the risk assessment practice. The detailed explanations of the results are shown in Chapter 6 – Need Identification – Survey about the current level of security in enterprises.

2. Literature Review

2.1 Information Violation

The violation of information and data breaches is not a new concept and did not first emerge when companies began to convert their protected data digitally. Violations have existed as long as individuals, companies or organizations have kept any data, or stored private information. For example, before information technology was easily accessed and widely used, violations of confidentiality and data protection were commonplace. For example, paper-based medical files could be easily shared without authorization and sensitive documents not correctly stored. At these times, many businesses and organizations did not have policies and procedures in place to protect individuals and guide employees in the safe handling of data. According to De Groot (2019) publicly disclosed data breaches increased dramatically in the 1980s, 1990s, and in the early 2000s when public awareness of the potential for data breaches began to grow.

The bulk of information regarding data breaches focuses on the period from 2005 to the present day. This is mainly due to the advancement of technology and the spread of electronic data across the globe. The result of this is the threat of data attack regarded as a significant concern for organizations, companies and consumers. Due to the advancement of technology, a violation of today's information can impact on hundreds of thousands, if not millions of individual consumers and even more personal data, all from a single attack on a company. By 2020, over one-third of all data will be stored or pass through the cloud. In 2020, data production is estimated to be forty-four times higher than that in 2009 while experts estimate a four thousand and three hundred percent increase in annual data production by 2020 (Groot, 2019). While individuals are responsible for the majority of data creation (around seventy percent),eighty percent of all data is stored by companies according to De Groot (2019). Security experts always try to keep up with the changes over time, but with technology changing fast, it is impossible without external aid as a "third party" to help improve future security.

Table 1 Data Violations over three years (Groot, 2019)

Year	Number of Violations	Violations that are made public
2016	4,814,941,681	823
2017	2,051,572,640	853
2018	1,038,130,252	699
Total	7,904,644,573	2,375

In 2005, only one hundred and thirty-six data breaches were reported by the Privacy Rights Clearinghouse. However, more than 8,908 data breaches have been made public since 2005, with more than 11,239,817,282 individual data having been violated up until 2018. In the last three years alone, there have been 7,904,644,573 data breaches, showing a comparatively high value compared to previous years. However, it is essential to note the Privacy Rights Clearinghouse only reports the offenses where the number of documents violated is unknown. Therefore, these figures are not a comprehensive summary of all data violations, with the total violated data likely to be much higher.

While organizations spend millions of dollars on developing security systems at the highest level, one of the most significant areas of weaknesses, and loss remain their employees. Lack of employee training and security expertise, therefore, can cause a huge loss, despite other measures being put in place. Cyberattacks are often able to commit cybercrime due to a lack of qualified cyber-security staff and the limited number of IT staff employed to keep pace with continuing security development and advancement. Testing, training and employing staff therefore is a critical measure for all organizations to reduce the vulnerabilities yet seems to be an area still not fully addressed. Businesses and organizations need to provide training to promote understanding for staff at every level, so they are aware of their roles and responsibilities in protecting against security threats. However, this is a colossal undertaking, and until this learning gap is resolved, financial institutions must continue to fight and efficiently manage cybersecurity threats.

Over the past few years, the risks of enterprises that include information technology and the information systems have increased exponentially. There are two common types of problems in IT. Firstly, a fundamental issue exists within the technology and IT industries, where users can penetrate a company's proprietary software or e-mail servers. Additionally, almost all companies and enterprises have a significant online presence and

use email to transact and communicate, making them particularly vulnerable to cybercrime. This crime is increasing in regularity, especially since hackers and malware grow more and become more sophisticated. Compromised companies may harm their products, reputation, customer service, growth, employees, and suffer in other areas. Companies that experience hacking or information violation must take prompt and transparent action through proactive strategies such as contacting customers to report and update on how they plan to deal with any breach of confidentiality. As such, all companies and organizations must have policies and procedures in place that outline how they will deal with any confidentiality of data protection breaches, and how these are reported. Likewise, senior-level executives need a clear vision and insight into all cyber threats to their organization. However, the IT department alone within an organization cannot fight these sophisticated hackers solely but need the support of an organizational structure behind them. The powerful and widespread nature of cyber threats emphasizes the need for an enterprise risk management system across all enterprises. Therefore, each company, regardless of industry, should cultivate and maintain strong relationships between IT risks assets, processes, and controls by defining them in terms of description, category, hierarchy, ownership, and visibility. Companies should empower IT departments to assess, determine, monitor and manage IT risks. Issues and recovery policies, including investigative protocols and root cause analysis, should exist and become part of the critical process to ensure best practice.

Industries such as the financial sector, IT and insurance organizations continue to be severely hit by cyberattacks due to the nature of the sensitive data held by them. These organizations possess an extensive database of high-value, customer records to include credit card information and email addresses. Information hackers can use when planning future attacks. Hackers, on the other hand, recognize one of the biggest money-makers from organizations and companies is through deception and selling information to a third party. Worryingly, cybercriminals have gained new and advanced levels of knowledge and intentions, and these came to fruition in 2017. This was a year characterized by a series of extraordinary attacks, including threats against malware, credit crunches and debit card, phishing efforts, data breaches and information violation.

However, cyberattacks have become a regular phenomenon in recent years and it is not possible to read the news without any mention of a business or organization that has been the target of a new attack. Most attacks are triggered by criminals seeking to steal valuable

information, but the question is what types of information are stolen the most? According to a report conducted in 2018 by Verizon (2018), the most common data stolen are:

- Payment Details: This information likely to be of utmost importance to a hacker who is motivated by gaining direct access to individuals or an organization's financial information in several different forms and can access cash quickly. Bank account information can be compromised in many ways, allowing funds to be removed and cards used for several purchases without the knowledge of the person who is ultimately the victim of the crime. Perhaps the most shocking aspect is how card information can be sold on the black market as well as in DarkWeb. Here a person's account can be used for the most dangerous purposes, alarming all users in the digital world.
- Authentication Details: Unauthorized access to online systems is incredibly valuable on the black market. Authentication details that include usernames and passwords are highly sought after by criminals. If a password is used across accounts, information is accessed freely. Imagine the value of the credentials of a celebrity, their email address details, for example. Or the president of an international bank. Unfortunately, users' passwords are more easily attacked due to them being 'light'. The result, if cybercriminals manage to gain Facebook's password, they will probably have access to the passwords of every other account of this person, allowing free access to all manner of information
- Medical Records: Personal medical records contain information that is not only confidential but highly sensitive, and criminals may sell stolen personal health information to the black market. Also, hackers can use credentials to obtain medical services and equipment for themselves or for medical insurance companies for services that have never been received on behalf of the person. Stealing medical ID can have worse outcomes for victims than financial identity theft, as less legal protection exists for consumers in these situations. Many victims are forced to pay for the health services received by thieves, or else they risk losing their insurance.
- Classified Information: Classified information encompasses a range of things, and includes new emerging technologies, product ideas or security information, where such data is often very valuable. Depending on how the classification is defined, this may include information such as the main idea of the organization's secret product,

product design, or security door code. However, if the information is classified then no company would want this information to be in the hands of cybercriminals.

When it comes to information security and data breaches, the financial aspect of the information must also be considered. Thus, according to the latest IBM and Ponemon Institute report (2018), the cost associated with data attacks has increased dramatically since 2013. In the United States, the attack price on data is estimated to average $7.35 million, whereas, worldwide, this attack price is $ 3.62 million on average according to Poneom Institute (2018). These reported costs data are for the financial year 2017, and a significant increase is further seen according to the 2018 report. It is estimated that the cost has also increased to $ 3.9 million in attack data. Moreover, the cyberattack concerns are gripping as big as small businesses, such as IBM offers a calculator to allow business and organizations the tools to calculate how much attack businesses and organizations can dedicate to their data by factorizing a set of factors. Undoubtedly, this cost includes both Facebook and Google, which have been targets of cyber-attacks in recent years.

In general, data attacks jeopardize:

a) The user's personal data becomes public
b) Loss of company/platform reputation
c) Financial cost each time the company is attacked, including a drop in the company's shares
d) Legal penalties for companies that are targeted among others

Given these consequences, each business or organization must take the necessary measures to protect itself from such cyber-attacks.

2.2 Information security requirements and controls

Once security and risk requirements have been identified, and risk management decisions have been taken, appropriate controls must be selected. Once selected, measures are implemented to ensure that risks are reduced to an acceptable level. ISACA (2006) defines controls as processes that help detect, correct and prevent cases of unauthorized attacks or attempts at the organization's information. These controls can be selected or can be designed to meet the specific needs of each case. The selection of security controls is dependent on organizational decisions based on the criteria for risk acceptance and risk treatment options. The overall risk management approach must be applied to the

organization and should also be subject to all legislation and relevant national and international rules. Controls can be considered as guiding principles for information security management and apply to most organizations. Organizations that have an undefined status concerning risk measurement are potentially vulnerable to possible attacks. Risk assessment is usually directly linked to the metrics.

To protect information assets, such as IT systems first, a need to identify what to protect, what should be protected, and based on the risk assessment how it is to be protected exists. Risk assessment allows an organization to "recognize itself" about their risk exposures (Talabis & Martin, 2012). For this reason, the first step to determining the necessary protection measures for the information system is the process of risk identification. Risk identification is an essential step in risk management, to determine what could cause a potential loss, and to gain insight into how and why the loss might happen. Thus, if a corporation expects to perform risk assessment successfully, finding the appropriate threat and vulnerability pair of each set is a crucial step. However, in the process of identifying threat and vulnerability pairs, it is difficult for the risk assessor, especially one who lacks information security competence, to recognize the feasible combinations (Wei, Wu, & Chu, 2017).

The first step of determining the necessary protection measures for the information system described above is also crucial for creating the documentation and requirements needed to increase the level of security. Regular assessments allow for greater control over the system, through continuous monitoring and implementation of the necessary measures, and will also be tailored to meet internal and external security requirements (Talabis & Martin, 2012). Dependence on the growth of information systems is widely accepted among banks. Information systems can generate many benefits as well as direct and indirect risks. Electronic information is needed to achieve the organization's objectives. Reliability, integrity and availability are major concerns in most audits. The use of computer networks, especially the internet, is revolutionizing the way business is conducted.

While the benefits have been tremendous and large, amounts of information are at the fingertips, and these links also pose significant risks to computer systems, information and critical operations, and the infrastructures they support. Elements of infrastructure such as telecommunications, energy distribution, national defense, law enforcement, government and emergency services are subject to these risks. The same factors that

benefit from the speed of operations and access if not adequately controlled, can leave them vulnerable to fraud, harm, and harmful actions. Also, natural disasters and untrustworthy errors by authorized computer users may have devastating consequences if information sources are not adequately protected. Recent virus-wound breaks, "worms," and denial service attacks on websites, show the potential for damage. Computer security is essential in minimizing the risks of malicious attacks by individuals, groups and protecting the information. These risks include misuse of resources, unauthorized access to downloading sensitive client information, termination of critical operations through viruses or hacker attacks, and modification or destruction of data. From the perspective of information security, the nature and type of compromise are not as material as the fact that security is damaged. To achieve effective information security governance, organizations management should establish and maintain a framework to guide the development and maintenance of a comprehensive information security program. Each of these factors significantly increases the need to ensure the privacy, security and availability in the organization. Information security is the protection of information from a wide range of threats to ensure business continuity, minimizing risk and maximizing return on investment.

Information security is important and decisive from the protection of organizational assets' view. Information is an asset, and like any other asset of an organization it has its value. According to (Maule-Ffinch, 2015; SANS, 2008) information security refers to the processes and methodologies which are designed and implemented to protect the print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. The existing and new businesses must face with the fact that information security risks may have a negative impact on the process of business continuity, public image, the relationship between organizations, financial loss, affect relationships with clients, partners, and may create problems with legal authorities in case of discrepancies with the law. Information, support processes, systems and networks are important business assets. Defining, achieving, maintaining, and improving the security of information is essential to maintain a competitive edge, cash flow, profitability, legal compliance and trade image. Organizations, systems and networks face security threats from a wide range of areas including computer fraud, espionage, sabotage, vandalism, fires or flooding. Causes of malware such as malicious code of programming, computer

piracy and Denial of Service attacks (DoS) have become more common, more ambitious and more sophisticated. Information security is vital for both types of public and private sector organizations, and it serves to protect critical infrastructures. In both sectors, information security will function as an incentive to avoid or reduce the risks involved. The relation between public and private networks and the sharing of information sources increases the difficulty of achieving access control. The tendency to use distributed IT systems has also weakened the effectiveness of centralized and specialized control. Many information systems have not been designed to be safe. The security that can be achieved by technical means is limited and should be supported by appropriate management policies and procedures. Identifying which security control should be active requires careful planning and attention in every detail. Information security management requires participation by all employees in the organization. Participation of shareholders, suppliers, third parties, customers or other external parties may be required. Advice from specialists or organizations outside the leading organization has often proved to be necessary.

In general, information security can be defined as the protection of data that is threatened by threats and risks to an organization or individual. According to (Webster, 2014), security is generally the quality or condition of being safe, which means to be free from injury. Consider that security is about preventing unwanted consequences from deliberate actions and unjustified actions of others. Schneier (2004) considered that security is about preventing undesirable effects from the intentional and unreasonable actions of others. Therefore, the purpose of security is to build protection against the enemies of those who would harm, intentionally or in any other way.

According to Mattord (2008), information security is the protection of information and critical elements, including systems and devices that use, store and transmit that information. Information security is the collection of technologies, standards, policies and management practices that apply to the information to keep it safe. According to Whitman and Mattord (2012), information security performs four essential functions for an organization that enables secure application functionality implemented in the organization's information technology systems, protect data that organizations collect and use, protect technological assets in use in the organization and ultimately protect the organization's ability to function. Providing information also enables the safe operation of the organization's information technology systems. This is because to protect the data,

the organization will apply or install appropriate software that will provide data such as antivirus and other protected applications. Therefore, information security is paramount in an organization to protect applications that are applied to organizations and to protect computer data. In addition to data protection, the installed application must also be protected because it may contribute to loss of information or damage. Information security protects the data that the organization collects and uses. If information is left unprotected, it can be achieved by anyone. If the information falls into the wrong hands, it can destroy life where it can be used to do damage. Information security programs will ensure that proper information is protected from both business and legal requirements from the steps taken to protect the organization's records. In addition, steps taken to protect the organization's information are privacy-related issues and help prevent identity theft. In an organization, information is an important and essential asset for business and so it must be carefully safeguarded. This is particularly important in an increasingly interconnected business environment in which information can now be seen against a wide variety of threats and weaknesses that are on the rise and in variety. So, by applying information security to an organization, it can protect technology assets that are in use in the organization. To protect the functionality of an organization, overall management and IT management are responsible for enforcing information security that protects the organization's ability to function. Information is the most important element in the organization to do business. Because an organization is responsible for keeping its customer’s information, which is important for them to protect the information. Without information, the business cannot work. With the provision of the information store, it also enables the organization to do business. That is why information security is important in organizations.

The purpose of the current literature review is to assess the current state of play in the field of information security in regard to risk assessment. The contributions of the existing literature have been explored by collating information to date, and examining case studies that have been implemented concerning the research subject. The aim of the literature review is to identify gaps that have been previously studied in the field of information security and risk assessment. The identified gaps would provide a basis to direct further research, methodologies, and aims. The primary data security objectives are structurally based on confidentiality, integrity and availability (CIA Triad Model.) (Maiwald et al., 2002; McCumber, 2004; Solomon & Chapple, 2005). For the purpose of this study,

confidentiality will be taken that the assets of a computing system are accessible only by authorized parties. The type of access is read-type access: reading, viewing, printing, or even just knowing the existence of the information. Confidentiality is sometimes called secrecy or privacy. Integrity means that assets can be modified only by authorized parties or only authorized ways. In this context, modification included writing, changing, changing status, deleting and creating of the information. Availability is defined as assets that are accessible to authorized parties. An authorized party should not be prevented from accessing objects to which he or she has legitimate access needs. A "perfect" system could preserve absolute confidentiality by preventing everyone from reading information. However, this does not meet the requirement of availability for proper access. Availability is known by its opposite, denial of service (Maiwald et al., 2002). The completion of the three above-mentioned requirements does not imply that the company has reached the desired level of security (Rigon & Westphall, 2013). Security requirements can only be satisfied by protecting the company from the attacks in the data and by meeting the company's objectives despite the challenges that can arise with the security of data. It is imperative to note that one of the most common problems facing companies is the lack of interconnection of the data security goals with the business objectives of the company. In these cases, internal conflict about the assessment of information and the form of their treatment is being dealt with.

According to literature, information systems security has evolved on three waves as it is described by von Solms (2000). The first wave of evolvement is known as a technical wave, which has been oriented on the technical approach to information systems security. The second wave is known as the management wave which came as a result of the involvement of the management by understanding the importance of information and the need to protect that information. The third wave is the institutional approach where the code of conduct and the best practices have been adopted. The third wave according to von Solms (2000) underlines that information security as a process that should be included in all the daily processes of employees, and this must be developed as an information security culture across the organization. Organizations are facing more security risks, including organizations and technical risks when there are digitalizing their services (Amberg, Markov, & Okujava, 2005; Brown, 2005). Information security should be a concern for all computer users as nobody can avoid online attacks. That underlines,

why it is important to know about the latest online security-related issues. Table 1 and Table 2 list the top threats for 2017 and 2018 (Mcafee.com, 2018; McAfee, 2017).

Top 5 Cyber Security Threats for 2017
Information Theft The act of information theft is not new, but the methods that hackers are using to steal information are becoming sophisticated.
Mobile Payment System Hack With mobile payment systems such as Apple Pay, Google Wallet, etc., people do not need to carry their wallets to make transactions, which is an excellent malware for hackers who want to steal funds.
The attack on Chip-and-Pin Cards Each card has a chip that proves it is a legitimate bank card and generates a one-time transaction code with each purchase. While the chip-and-pin cards help to prevent in-store purchase fraud, they cannot do much for online purchases.
Cloud Hacks Cloud hacks were one of the headlines on the tech news during 2016, starting from celebrities' cell phones to significant corporation's data storage. Even in 2017, this was an issue.
Extortion Hacks For hackers that do not feel like taking the time to use the data they steal from significant corporations, extortion hack or cyber shakedowns are the new trends. And this is not talking about the type of cyber shakedown that locks out of an account until you pay a ransom but are talking about threatening to release data from significant corporations unless a ransom is paid.

Table 1 top 5 Cyber Security Threats for 2017 ("Top 5 Cybersecurity Threats to Watch Out for in 2017 - An Infographic," 2018)

– **Top 5 Cyber Security Threats for 2018**
– **Fallout Exploit Kit** – This exploit kit was discovered in August 2018 and took advantage of flaws in Adobe Flash Player and Microsoft Windows. A successful infection will allow the attacker to download additional malware onto the victim's computer

Operation Ocean salt – This campaign reuses a portion of code from the Sea salt implant (circa 2010) that is linked to the Chinese hacking group Comment Crew. Ocean salt appears to have been part of an operation targeting South Korea, the United States, and Canada in a well-focused attack
Thread Kit Exploit Kit This exploit kit is used to create malicious Microsoft Office documents in an attempt to exploit a range of Microsoft vulnerabilities. The builder is sold on the Dark Web and has been used to infect victims with various malware including FormBook, Loki Bot, Trickbot, and Chthonic.
Scarab - Ransomware – This ransomware uses AES encryption and adds various extensions to infected files. In November 2017 it was discovered that the Necurs botnet was used to spread the malicious software. Multiple variants of the ransomware continue to appear on the threat landscape.
– **GandCrab 5 – Ransomware** – This ransomware appends random extensions to encrypted files and directs the victim to an HTML file for instructions on how to decrypt infected files. The threat actor demands $800 in either bitcoin or DASH for the decryption key. GandCrab 5 also scans network shares and mapped drives to find files to encrypt. The threat actors behind the ransomware use a variety of infection vectors including PowerShell, botnets, exploit kits, Trojanized programs, spear phishing, and remote desktop.

Table 2 top 5 Cyber Security Threats for 2018

One of the biggest concerns for any organization is to achieve its goals by having their data protected.

2.3 Potential Attacks and Threats

In 2017, the sector faced several changes in the world of financial threats and the emergence of new actors. As previously noted, fraudulent attacks on financial services have become increasingly central-accounted. User data is a crucial factor for large-scale attacks, and frequent data breaches, among other types of successful attacks, provide cybercriminals with valuable personal information resources to use in purchases accounts

or false identity attacks. These account-centric attacks can result in many other losses, including those of further customer data and trust. Attacks on ATMs continue to increase in 2017, attracting the attention of many cybercriminals, with attackers targeting banking infrastructure and payment systems using sophisticated malware. In 2017, Kaspersky Lab researchers (Petr Komarevtsev, 2018) discovered attacks on ATM systems that included new malware, remote operations, and an ATM targeting malware called "Cutlet Maker" that was being opened in the DarkNet market for several thousand dollars. Kaspersky Lab has released a report outlining possible ATM attack scenarios targeting ATM authentication systems.

1. Internal Threats - Internal threat is a critical security problem. Intimidation of intrinsic persons may be presented inadvertently or intentionally by injured persons. Internal threats are defined as the threat posed by a person who has authorized the access privileges and knowledge of an organization's computer systems and is inspired to adversely affect the organization (Brackney & Anderson, 2004). Interns can be employees, contractors or business partners. They have abilities that they do not have outsiders, enabling them to embark on intricate attacks. According to various surveys (Gordon, Loeb, Lucyshyn, & Richardson, 2005; Littlewort et al., 2011), the internal risk is as risky as the threat of foreigners (hackers) due to the extreme damage it may present. The FBI's Computer Crime Analysis (Gordon et al., 2005)reported that trusted persons were responsible for about 33% of all security breaches in 2005. Similarly, the Cyber Security Survey (Littlewort et al., 2011) attacks are caused by foreigners, while 21% of attacks are caused by interns. Moreover, the survey shows that the internal threat is as costly as an external threat.
2. External Threats - These are threats from foreigners and can usually be done by hackers. Someone who uses the internet bank for transactions should be cautious of hackers. Security numbers and passwords are vital information for your online transaction (Morin, Thomas, & Debar, 2006).
3. Phishing - includes an email message that is sent to the email addresses of the internet that the swindler can provide. Usually, these emails claim to come from a bank. Email requires the recipient to update or verify his personal and financial information, including the date of birth, identification information, account details, credit card numbers, PINs, etc. The email contains a link that leads you to

a website that looks identical or similar to the bank's website. The deceiver can then retrieve personal data such as passwords when writing. With one click malware can be download onto a computer, and this will record all future use of the web and will convey even more information to the swindler. Deceivers will use this information to endanger bank accounts, credit cards.

4. Pharming - attacks include installing malicious code onto a computer. However, pharming attacks can happen without any conscious action on the part of the user. With pharming attacks, a user should open an email or email attachment to become unprotected. By then visiting a fake website and without the user's permission, they provide information that compromises the financial identity of the user. Online banking scams can be performed internally by staff or outsourced by customers or suppliers. Online banks are the distribution channel to carry out banking activities, for example, transferring funds, paying bills, viewing balance and savings accounts, paying mortgages, purchasing financial instruments, and deposit certificates. In e-banking, customers have access to their accounts from a browser, the software that runs banking programs on the bank's "World Wide Web" server. Customers can choose any online banking service. The traditional bank branch model is now giving the country an alternative ATM distribution channel. Once the branch offices of the banks are interconnected via networks or satellite connections, there would be no physical identity for any branch. It would be a boundless entity that allows anytime, anywhere and anyway banking. The online bank has become increasingly popular globally because it is so easy and convenient for users to manage their bank accounts from anywhere in the world at any time. Banks have encouraged this trend for years, as online banks also save many resources such as staff training, ATM and branch investment, and other operating costs. Banks must continually advance their security systems, which means that banks should always continue to invest in security systems.
5. Data Breach - Organizations should be aware of the threats that will affect the system's security in their organization. A data breach, one of the existing threats that allow information and data to emerge from the system, making it visible to others. A data breach is a well-known phenomenon involving sensitive and confidential data that may have been seen, stolen, and used by any person or organization without being authorized to do so. For example, in violating security records, a case involving five banks in Connecticut is the result of a breach of

security data affected by the New Jersey company processing credit card payments, according to newspaper and internet reports. The effect of data breach takes many losses for the financial institution, where their credit card companies like Visa and MasterCard have contacted them for the violation, according to the BankinfoSecurity.com website. Banks affected by default are Litchfield Bancorp, Apple Valley Bank of Cheshire, Dime and Norwich Bank, Liberty Bank of Middletown, Chelsea Groton Bank and 230 other financial institutions. It is essential for an organization to identify its security requirements. Based on literature there are three primary sources of security requirements for any organization (Beckers, Faßbender, Heisel, Küster, & Schmidt, 2012; Everett, 2011; Lee, 2014; Rigon & Westphall, 2013; Shamala, Ahmad, & Yusoff, 2013).

6. Risk assessment, considering the overall strategy of the business organization and objectives. Through a risk assessment, threats to assets are identified, vulnerability estimates and likelihood of incidents are assessed as well as the potential impact assessed.
7. Legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers must fulfill.
8. The security requirement is a set of principles, business objectives and requirements that the organization has developed to process information and support its operations.

Security requirements are identified by a methodical approach to the assessment of security risks. Costs for controls should be balanced with the likelihood of business damage resulting from security failures. Risk assessment results help to guide and determine appropriate management measures and priorities for managing information security risks, and also for implementing selected controls to protect against these risks (Vancouver Coastal Health (VCH), 2016). The risk assessment should be repeated periodically to address any changes that may impact on the risk assessment results.

2.4. Information Security Management System and its integration to the organization

Diversity of opinions and factors influencing the process of IT adaption to information security needs is emphasized in many papers (Businge, Serebrenik, & van den Brand, 2010). The literature has identified several factors affecting this process, and most of them have listed factors such as senior management, government, IT consultants,

organizational behavior, and so on (Joshi, Bollen, Hassink, De Haes, & Van Grembergen, 2017).

Organizations are often affected by the models and standards that are implemented on information security within the same industry, but not all the models and standards are implemented in the same way. For small organizations that operate with a small staff and which distribute information with key staff only, the implementation of information security does not seem to be a necessary option. However, companies where information is distributed to more people simultaneously, it is impossible to manage them without a proper system, thus, presenting the problem of data vulnerability. The third group of organizations is on where the main product is information (Burgeois, 2014).

Information Security Management System is defined by ISO 27001 as a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. Organizations have different approaches when deciding to implement an information security system. Some organizations see information security systems as a competitive edge in the market that can provide them with greater credibility in their client relationship, as well as an increase of credibility in their organization and products. Another group of organizations implements information security systems only when they see that their competitors are operating in the same way. The aforementioned views create cultural diversity within organizations of the same industry, and no doubt enable them to improve.

2.5 Maturity Models

To ensure security, it is essential to build security in both: design phases and adaptation of a security architecture that provides that security rules and connections are set up accurately. Security requirements must relate to business goals through a process-oriented to access. The process should consider many of the factors that affect an organization's goals. Four areas that affect security in an organization are identified. First, governance organizations are a factor that affects the security of an organization. Second, organizational culture affects the implementation of security changes in the organization. Thirdly, system architecture may pose challenges for enforcing security requirements. Finally, service management is considered as a challenging implementation process.

The concept of maturity models is increasingly being implemented in the area of information systems as an approach to organizational development or as an organizational assessment tool. Any systematic framework for performing benchmarking and performance improvement can be considered as a model, and if there are continuous improvement processes than it can be viewed as a maturity model. In general, in the constituent literature, maturity means a definite or explicitly defined, managed, measured and controlled definition. It is also a breakthrough in demonstrating a specific skill or achieving an objective from an initial stage to the desired end. To identify and explore the strength and weaknesses of a particular organization's security, several models have been developed. The goal is to identify a gap between practice and theory which then can be closed by following a process-oriented approach. The current study presents a method that provides a starting point for enforcing security, a common security vision, and a framework for prioritizing actions.

Recently, there has been a growing trend towards the collection of personal data from the private and public sectors (Talabis & Martin, 2012). This can also be described from the high use of social media networks through which people share many informations either from their private life, professional activities or other important events. Some organizations which operate with many services think that using single sign-on (SSO) techniques as an authentication process service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications increases the efficiency and time on their daily operations. Using single sign-on authentication (SSO) creates the ideal opportunity for your data to be easily distributed from one organization to another (Bazaz & Khalique, 2016). Additionally, the growing trend in cloud computing, which is seen as more secure for storage of data, creates the opportunity for everybody and organizations to extract information from their services or lives. But yet organizations are concerned about the security issues, especially organizations from the banking sector, insurance companies or IT industry. This concern has been shown as well, on my research where 40% or the interviews do not store any data on the cloud platforms, which means that they have all their services onsite. Discussing with them this issue, the reason this with the argument that, it is lack of trust to the cloud companies, especially when you decide to terminate the contract, and you are not sure if the data information has been permanently deleted. A similar case has been shown with the Facebook and Cambridge Analytica scandal where Facebook claims that Cambridge Analytica didn’t

delete information stored on the request of Facebook. In the technical aspect, the cloud platform is nothing more than storing data on another computer. However, it is challenging to create or use a security maturity model if there is not a method in advance to evaluate our needs to select the most suitable maturity model which will determine the level of security for our organization based on any scoring system model. There are several maturity models for risk assessment in information security that could be applied in any organization to determine a more précised level of security (Ge, Yuan, & Lu, 2011). Large organizations usually have in place several risk assessment processes at the same time. Those risk assessment processes are decentralized from management and led by departments.

For this reason, the need to create a centralized system of information security risk assessment across different processes and in this case, in the field of information security is necessary. The centralization of the process enables the creation of more accurate reports through which potential threats and vulnerabilities within my system can be identified. To evaluate the security of information, various developments have been seen through mechanisms that are adapted from the recognized engineering field. One of these mechanisms is the measurement of information security process maturity (Dzazali & Zolait, 2012) in order to elaborate on the concepts of information security maturity where three maturity models have been analyzed, respectively: COBIT, SSE-CMM and ISM3. Although the aim and scope of coverage for maturity appraisal differ, however, maturity models are process-oriented standards, which are based on maturity levels. Processes adhere to a quality standard for each maturity level while documenting and document management is required to ensure that the selected processes comply with the standard. To determine a maturity level through a risk assessment process (Schneier, 2004) influenced the improvement of preconceptions about information security domination as a discipline where "security should be a process rather than a product". (Schneier, 2004) describes this process must understand all the real threats to the system, and by creating security policies tailored to existing threats, easier mechanisms for data protection can be developed. Maturity Models are considered as a standardized approach to driving activities, processes and commitment to the desired destination and goals. (Ngwum, 2016). In recent years, many maturity models have been developed, with the same aim to improve processes.

2.6 Levels of Compliance

It is difficult for security practitioners and decision-makers to know what level of protection they are taking from their investment in security. It is even more challenging to assess how well these investments can be expected to protect their organizations in the future as a security policy, regulation and threatening environment are continually changing. An information system would pass between some vulnerable states of vulnerability. The first thing is hardened and occurs when all security patches, usual updates, have been uninstalled. The second is unlocking and occurs when there is not at least an installed security correction. The final status is compromised and occurs when it is successfully exploited. Within these situations, a system must show how secure the organization is so that the detection window can be minimized by security operations teams in an organization by following a standard patching process to eliminate the risk-related vulnerability. The security team either places patches after weakness first discovered or adds attack-related signatures. The longer the exposure window, the more organizations are exposed to attacks and exploitation. The size of risks is minimized if organizations are aware of their security needs. Therefore, Information Security Maturity Model (ISMM) proposes five levels of compliance. Security is believed to be improved as a moving organization at these five levels:

No Compliance

This situation is characterized by no existence of policies and procedures to secure business. Management does not consider investing in the security-related systems required for overall business strategies. Also, the organization does not value the business impact of its weaknesses and does not understand the risks involved due to these weaknesses.

Initial Compliance

This condition is the starting point for each organization. While an organization is aware of the threats their information systems face, then that organization is considered in the initial state of compliance. This state is characterized by being chaotic, contradictory, ending for one goal, in response to the attacks and perhaps because of the loss of resources due to an attack. Organizations that recognize business risks due to weaknesses do not have policies or procedures designed to protect the organization. In addition, the organization would have little practical implementation in security systems. Most of the

implemented controls are reactive and unplanned. Initial Goals usually focus on the organization's business activities and little focus on organization assurance. Goals will change in response to attacks by applying a kind of defense but will not be persistent.

Basic Compliance

This is the starting point for any organization that wants to protect its investments and ensure continuity. Application and network security are implemented, but changes are not managed centrally and security where the requirements are standard. In this situation, organizations believe in the interaction between users and systems. Security awareness programs are being considered only for the primary sources. IT security swapping procedures are informal from some risk assessments that are taking place. In addition, IT security responsibilities also apply, but implementation is not compliant. Intervention and detection testing can also be performed. A necessary process for most systems is the interaction between the system and the user. According to what interaction is the most significant risk. Organizations do not classify their users as threats to their systems. The user does not always pose a threat to isolation; Rather, user actions are the starting point for some attacks, and in some cases, users themselves can launch attacks. Poor passwords, vulnerability to social engineering attacks, and failure to install security updates are some examples of why the user is classified as a poor human factor, and user interaction with systems creates threats. Goals at this level usually focus on the organization's business activities and the protection of these key systems. Typically, an organization will consider the security of a system after system implementation. At this stage, two constraints are faced: First, financial constraints and costs for systems that do not add value to business income. Secondly, organizations classify their initial investments in completed security. The organization will have a perception that their systems are protected and become aware of threats and weaknesses.

Eligibility Compliance

This situation is characterized by the central management of all security-related issues and policies. Users are trusted, but their interactions with systems are considered weaknesses. No change in the central configuration templates, from which all settings are extracted, are not applied. Security policies and procedures are now in place, along with adequate distribution mechanisms to help awareness and compatibility. Entry controls are mandatory and closely monitored. Security measures are introduced into a cost/benefit,

and the concept of ownership is in place. There is a school of thought that claims that it is not the fault of the users that they make a move easier; Rather, it is the blame of the projectors who have made the operation more insecure the smoother operation. Since user actions are the starting point for some attacks, there is a need to embed a "security culture" on users. Many users need to remember multiple passwords. They use different passwords for different applications and have frequent password changes, which reduces users' ability to remember passwords and increase unsafe work practices, such as writing passwords down. For organizations to ensure interactions with their systems, communication between the security team and users should be made by users aware of possible threats. In addition, users do not understand security issues, while the security team makes no sense of user perceptions, tasks, and needs. The result is that the security team informs users of threats that need to be controlled and managed, in the worst case the enemy is inside. Users, on the other hand, perceive many security mechanisms as a height that takes their true way of working.

Comprehensive Compliance

This situation is characterized by control over the organization's security needs, monitoring systems, being aware of threats and comparing the organization itself with other similar organizations and international standards. In addition, a full security function has been established that is both cost-effective and efficient that ensures high-quality implementation. This comprehensive plan has official policies and procedures in place to prevent, detect and correct any security issues. Also, corporate governance is in line with the security needs of a corporate organization; governance has internal audit policies, which is an independent and objective activity to increase value and improve the organization's security. The outcomes of each audit activity are published, and the actions are implemented. For the organization to have full compliance security managed by identifying safety and security concerns incidents are systematically traced. The organization should have proper security policies in a formal sense, and business plans would have security articles. The use of specific technologies throughout the organization is in a uniform manner, and implementation came into being outside of a business plan. Full compliance also considers security architecture in an organization. While business architecture considers all external factors in an organization, security architecture considers all users in the application. Policies are created to meet the needs of users, but the information at or outside the organization is captured. There is a system for tracking

information through the organization. Users are also involved in architectural analysis, and the organization provides user training on security issues.

Regarding security management, policies consistent with state of the art have a preventive, detective and corrective control. The organization should have a system for reporting incidents of security and tracking the status of each incident. Installing anti-virus software and firewall is not enough to control the threats of organizations face. Email filters and intrusion detection systems should also be used to prevent many types of incidents.

Measurements

Metrics are often used to predict future behaviors, based on historical data and trends. Arguing that safety metrics have been created and monitored as a way to get knowledge about the work of these controls and to identify failure points or abnormalities is very important. However, metrics are gathered across organizations, and they are operational metrics without the context of overall security processes. On the other hand, the measurement of any complex, operational system is challenging, and security risks represent another dimension of complexity.

Risk management and the availability of different measurements and their properties will vary throughout the cycle of the system cycle. Each metering frame should be able to adapt to both changes in the metering objective and the available metering infrastructure. Security measurements often require the collection of some metrics because direct measurement of relevant properties is not usually possible in complex systems of practice and collection strategies may vary from time to time, depending on the environment and many risk factors.

2.7 Risk Management

Each enterprise faces different risks. Historically, the most severe risk is business risk. The roots of business risk penetrate numerous business sources like; loans, strategies, markets, competition, various operations, etc. Increasing integration, globalization, complexity, and dependence on IT have resulted in the emergence of other significant risks: likelihood, finance and technology. Each of the management structures has a different approach to risk categorization. We are living the time where the dependency on computer systems with an emphasis on information that is continually being processed,

circulated and made accessible by these systems is immense. With the globalization of economies, the continuous interaction of organizations, governments and other stakeholders in principle is facilitated and enabled by information and communication technology. Therefore, with this dependence on information systems that are already deepening day by day, the need for information security management increases, thus organizations, institutions and all stakeholders are dependent on the computer systems they have and offer this information. These developments have made information security risk management a sensitive area that needs to be addressed. It is almost impossible for you to hear or read every day about different articles and reports where organizations around the world have been attacked and at the same time has suffered data loss or something related to the security of information. Therefore, the information security risk management process is also aimed at balancing these resources and efforts to minimize and prevent theft of information, interception, alteration, or dissemination by unauthorized parties. According to Schneider, information security in principle is a problem of risk management (Schneier, 2000). So, it is logical that for companies and organizations with limited resources it is almost impossible to guarantee the complete security of information because and attackers who usually have considerable resources, time and great willpower available, there is also the possibility of attacks being successful. Even with the taking of all security measures, there is still a risk; so, instead of eliminating all the risks (which is impossible to achieve), it is recommended to have a more practical approach to regulate the protection and minimize or prevent the risks. This is achieved through information security risk management which is a process that interacts with the use of information technology; which involves identifying, assessing and addressing risks along the triangle of security for the needs that the company or organization has. In the market there are numerous models and tools on how to manage the risk of information security. However, among the researchers in this area is the goal of this process is to address the risks by the risk tolerance that the organization or company in question has (Elky, 2006).

A recent study on the risk management solutions provided that enterprise risk management maturity is calculated by Risk Maturity Models and add 25% to a business organization's bottom line value (Sarah Beals, Carol Fox, n.d.). (Siponen, 2002) suggested the term "software maturity criteria", by which the scholar proposed and explained that existing maturity standards must lead the way toward the management of

information security in organizations. (Poeppelbuss, Niehaves, Simons, & Becker, 2011), explained maturity models as a conceptual model that describes a way of how the organization will outline the logical and desired evolution toward maturity, while Bruin and Rosemann (Bruin & Rosemann, 2005) described the maturity as an evaluation measure for the organizations capacity to follow a specific discipline (Bruin & Rosemann, 2005). Another opinion regarding the maturity has been provided by (Mettler, 2009) who described the maturity as a process of evolution on demonstrating the ability to accomplish a targeted activity from beginning to the final stage. The risk management process coordinates activities and efforts to direct and control an organization concerning risk (Standardization, 2009). Various approaches were suggested; the main differences between these approaches are how they are adopted into existing workflow and safety structures.

Risk management process consists of five steps (Häring, 2015)

- Step 1 – Establish the context
- Step 2 – Identify the risks
- Step 3 – Analyze the risks
- Step 4 – Evaluate the risks
- Step 5 – Treat the risks

The following, diagram shows the scheme of the risk management process and the brief explanation of each step.

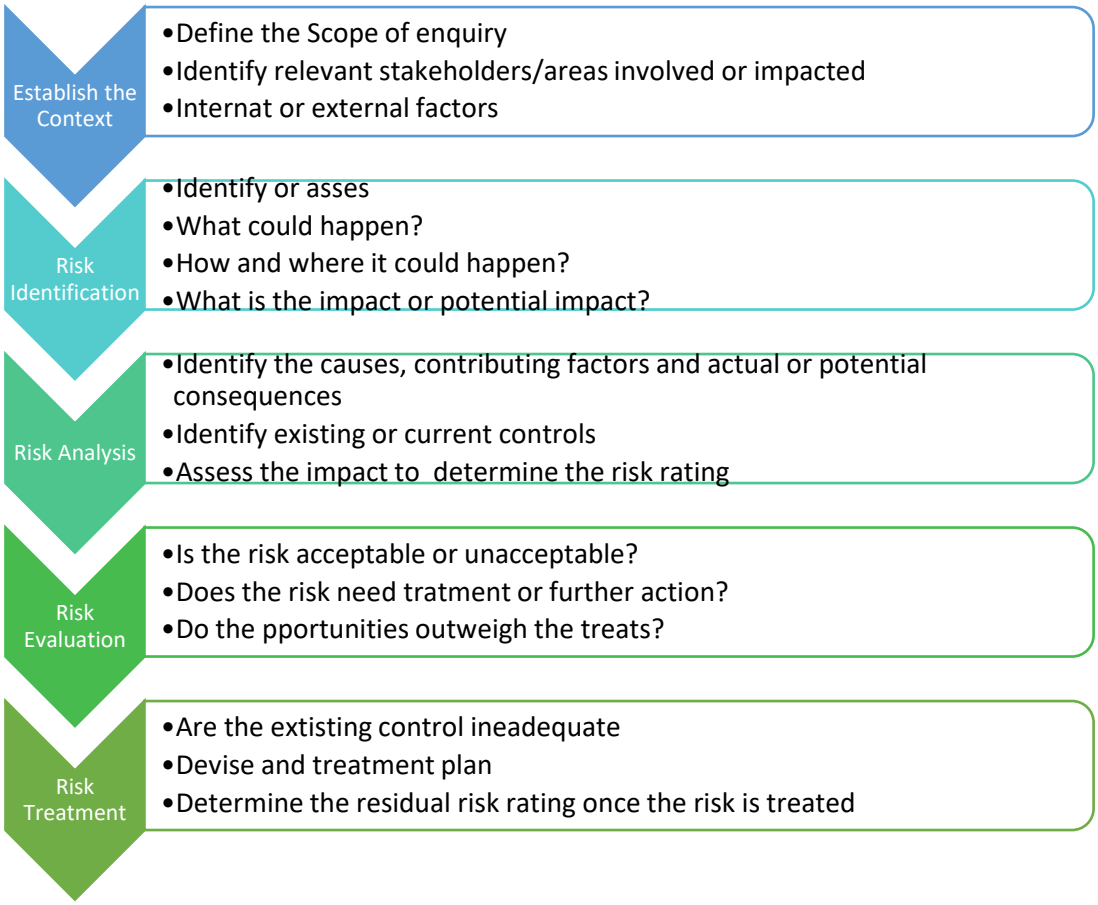


Figure 1 The Risk Management Process (The University of Adelaide, 2009)

The risk of information security is inevitable, regardless of the type or size of any organization or company. This risk is daily, varied and of different forms where there is no single mechanism or form of control through which it is possible to forward that complete and sustained risk identification is made. As explained and discussed, according to frequent sources of information and good practices, the risk can't be treated 100% because there is no such level to consider the risk. Therefore, identifying and achieving an acceptable level of risk to information security is a continuous process to manage the risks. It can be said that risk management is essentially a decision-making process. As a process, it is accumulating the resources of an organization, whether it is the technical or human factor, to manage the threat posed to information systems or equipment. The risk assessment stage is where information is gathered and is included as a factor in decision-making. The risk mitigation stage is the actual decision making and implementation of the strategy resulting from the findings. Effectiveness assessment is a continuous reaction to decision-making. Although current methods have space for improvement, risk management undoubtedly serves a valuable and practical function for organizations. Organizations face many pressing needs, including security, and risk management

provides a method to determine and justify the distribution of limited resources to security needs. Therefore, it is essential to re-emphasize that risk management should evolve alongside the organization's development, and at no time the organization should not be considered as being sufficiently managed to manage the risk. Risk is a fundamental factor of decisions taken by the company along with the decision to use information systems. Any company or organization of any level should consider that the use of information systems itself is a risk, and this risk is not only in terms of security alongside risks such as unauthorized theft, distribution, or modification of information. Risks are also considered threats of other natures that may not be human. Therefore, senior management should understand that everyday operations should also have the security of information. In the management of information security risk, communication of stakeholders is crucial, and decisions are taken regardless of whether they are proper, these decisions should be communicated quickly and accurately at all levels. The most important fact is that organizations are aware of the available capabilities, systems they use, and the risk they deem to threaten systems and information in these systems. When these are clear, there are many forms and methods of risk management available that have the idea that the risk should be incorporated into the decisions taken; so, decisions are based on acceptable risk. When an organization or company respects the basic practices for good information security management, then it can be said that management of this risk affects the riskiness and probability of damages to information and equipment. Literature review and good practices show that information security risk management is expected to identify risks, identify vulnerabilities, and then identify adequate controls for these risks and then in other phases are also set for the form that needs to be addressed in response to these dangers. However, as a process is a long process, it cannot be used and does not ensure that at a certain stage a satisfactory result is achieved and there are no risks. During this process the organization, staff and professionals in the field are aware of the dangers they face, inform management and make jointly good risk-based decisions. While the risk is acceptable then it can be concluded that good risk management is being done, when the risk is not acceptable then management decisions should reflect something like this. Risk management is a mandatory part of any related framework and standard such as ISO 27001, NIST, ISM3, COBIT, CMMI.

2.8 Information Security Risk Assessment

As part of the Risk Management structure, the risk assessment process identifies and evaluates the risk to information security by determining the probability of occurrence and the resulting impact. Through the risk assessment process, it is possible to identify threats, classify assets and rate the system vulnerabilities because it helps us with information and guides us to effective implementation of controls (Macedo, 2009). According to literature, I can separate risk assessment models into quantitative and qualitative. Quantitative models are those which are based on measurable data to determine the asset value and associated risk to calculate objective numeric values for each of the components that are collected during the risk assessment process. On another side, qualitative methods are based mostly on the descriptive categories such as low, medium, high, or any other method of scaling. This method assesses the impact of the likelihood of the identified risk (Macedo, 2009). Both methods have their advantages and disadvantages to the risk management approach, which also depends on the size of organizations. Organizations usually try to adopt the quantitative methods, because it is more easily measurable, but many times small-sized organizations with limited resources decide to use a qualitative approach as the best methods for their needs.

The deliverable from a qualitative assessment should be a report of which assets and systems are most important to various parts of the business. The assessment committee won't necessarily know the financial impact of these systems were compromised, but they will understand which business units would be affected and how much productivity would be lost in different risk scenarios. Additionally, the assessor would understand the impact on the company's reputation and any PR considerations if a risk were realized and became publicly known. When developing the information security risk assessment methodology for your organization, it's essential to realize that both quantitative and qualitative analyses are needed for a well-rounded view on the risk management process. Risk management processes require not only understanding impact but creating a risk management framework that sets the acceptable level of risk to enable functioning business operations.

The advancement and complexity of technological networks create opportunities for more attacks and breaches into security systems, causing large direct and side damage such as financial loss, reputation damage, etc. (Hu, Hart, & Cooke, 2007). Adding this to the need for a proper organization data protection strategy that is most important to us, information security management is one of the most important assets. While organizations are offering

their clients access to multiple information systems, security threats are growing, and the need to have secure systems gets special and important treatment (Nazareth & Choi, 2015). While many researchers and organizations deal with the issue of information security mainly in the technical aspect, respectively its integration into corporate governance, non-technical issues are rarely considered as one of the issues to be included in business strategies (Lapke & Dhillon, 2006). According to several researchers (Stanton, Stam, Mastrangelo, & Jolton, 2005), most of the security information "shakes" are caused by incidents inside the organization, which means that the internal staff is identified as the first and most security threat to information security (Gaunt, 2000; Stine, Barker, & Gulick, 2008). Increasing the need for more secure systems and the need for our data to be handled with the utmost security is that the information security study surpasses the technology gap by increasing awareness of the role of management in data security (Singh, Picot, Kranz, Gupta, & Ojha, 2013; Soomro, Shah, & Ahmed, 2016). Also, given the fact that security information systems development is not enough to stop attacks and damages to information's, an effective information security system that includes policies and a robust review of information security policies are key factors for good protection (Ezingeard & Bowen-Schrire, 2007; Johnston & Hale, 2009). As a result, management's role is more focused on the development and execution of information protection policies, training delivery, investment in information infrastructure development and business and IT alignment (McKinsey, 2014; Siponen, Adam Mahmood, & Pahnila, 2014). Information and Communication Technology has created a wealth of business ventures through the provision of services, but at the same time, huge challenges have been created, and a result of these challenges, many organizations that offers online services or handling sensitive information have been forced to change the approach and scope of addressing the data by implicating the technological aspect as well as the security of the information's.

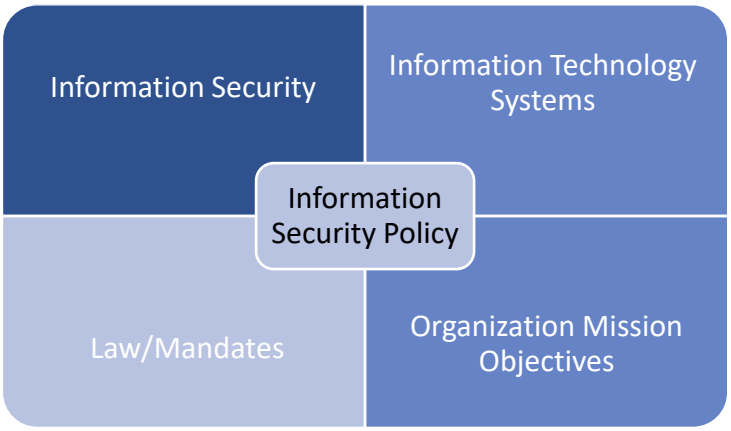


Figure 2 - Information Security Policies (Diver, 2007)

2.9 Information Security Management Systems

An important issue to be discussed is whether information security is a business or organizational problem that needs to be addressed seriously as part of the organizational strategy, including mission, purpose and objectives (Dzazali & Zolait, 2012). However, according to (Von Solms & Von Solms, 2005), the organization should protect its information as a business and not a technical issue. Conversely, (Sohrabi Safa, Von Solms, & Furnell, 2016) consider information security management as a multi-dimensional discipline that should take into account all dimensions and provide a safe environment for information as a significant asset in an organization. Adaptation and costs are key elements for a successful ISMS. Processes in ISMS, as the core elements of an ISMS, should be in line with its organization and mission and its business strategy (Haufe, Colomo-Palacios, Dzombeta, Brandis, & Stantchev, 2016). Generally, the best ISMS standards have been developed by gathering together the best security measurement practices (ISO/IEC 27001:2013, 2013). (Susanto, Almunawar, & Tuan, 2011) forward the three most international standards for development and operation with ISMS are ISO 270xx, ITIL (Lloyd & Rudd, 2011) and COBIT (Stoll, 2014), which are also relevant to management secure but also with cloud governance (Stantchev & Stantcheva, 2012). Even as ISO 27001 determines the requirements for planning, implementation, operation and continuous monitoring for the process-oriented ISMS improvement, however, Disterer (2013) states a framework of processes does not appear in ISO 27001. Almost all standards of security information focus on the existence of processes, but not on their content (Siponen, 2002). Compliance with the information security management guidelines is essential, but according to (Siponen & Willison, 2009), the existing

guidelines have two problems: the first is that they are very generic in the field, while organizations need more optimized methods that may be adapted to their organizational environment and the second problem is that these standards have not been validated but are driven by usage practices which are unusual for a true standard (Siponen & Willison, 2009). According to Subashini & Kavitha (2011), an Information Security Management System is desirable to address the following issues:

1. Data confidentiality.
2. Web application security.
3. Data breaches.
4. Virtualization vulnerability.
5. Availability.
6. Data access.
7. sign-on process and Identity management.
8. Network security.
9. Data security.
10. Data segregation.
11. Authentication and authorization.
12. Data locality.
13. Backup.
14. Data Integrity

Each of the standards has a special and important role in the implementation of ISMS. This is also related to the standard implementation area standards such as Prince 2, OPM3 and COSO focus on project management and risk management, while ISO 27001 standard focuses on security information while DSS is more popular with more secure data as secure transactions such as secure processing of credit and debit cards, while on the other hand, standards such as ITIL and CMMI are well-aligned with service management and development. While the two standards that are directly focused on maintaining online trust between the client and the servers of IT Governance are SOA and COBIT (Islamia & Delhi, 2018). From the comparisons already discussed, it can be concluded that ISO 27001 is the most appropriate standard for the implementation of best practices in information security.

2.10 Semi-Automated Risk Assessment Solutions

Organizations have a broad set of security requirements. For organizations security and information security management is built from a complex interconnection between business objectives, IT strategy, institutional arrangements and requirements from, while for public institutions, security requirements are mandatory (Montesino & Fenz, 2011a; Radack & Kuhn, 2011). According to my current research conducted with organizations, completing these requirements is a waste of time and the likelihood of error is large because organizations lack digital, automatic or semi-automatic processes to perform tasks related to information security management. The risk assessment process should be related to what you want to measure, and, in this section, I can interconnect the part of the security controls that I want to evaluate through the risk assessment. Based on the ISO 27001 specification, a total of 133 security controls represent all the areas for information security management. However, not all can be automated through certain tools. A security-control is automated if it can perform the required operations without human intervention in the process. This implies that the best way to automate security controls is through semi-automation. According to Montesino & Fenz (2011a) and based on the criteria outlined by Montesino & Fenz (2011b) the identification of semi-automated controls can be made through the following criteria:

- Actions and monitoring of audits require only readable resources that cannot be considered as potential training to understand the need to look at and interact with the human factor
- Controls can be automated using one of the relevant security applications.

(Montesino & Fenz, 2011b) has analyzed all the information security controls and came to a conclusion with the list of controls that could potentially be automated or semi-automated and are presented in the table below.

3. Information Security Standards and Models

Just as the use of information and communication technologies in businesses is generally not an end, the use of security standards should always be combined with - at best quantifiable - benefits. For example, the certification of an information security management system (ISMS) according to ISO / IEC 27001 - depending on the choice of scope - certainly involves a tangible human and financial outlay. This applies both to the certification process and to the subsequent operation of the management system and the

necessary audits to maintain the certificate. However, there are also undeniable advantages associated with the introduction and operation of an information security management system that is stringent and appropriate for the company. Internally, the use of established standards can help to improve the security-relevant IT processes for the benefit of the company, the customers, their products and their employees. They help with the development of generic measures at management level up to detailed technical implementations. They provide methods for efficient IT security management or define the IT security of designated products. They can be operated both independently and methodically embedded in another system continuously. An ISMS makes sense as part of company-wide risk management, which can be reduced in particular to the IT risks to a level appropriate for the company. In doing so, it is particularly important to comprehensively identify the risks and, for economic reasons, not to make the protective mechanisms costlier than the permissible risk requires. The selection and application of adequate IT security standards are part of IT security management. The variety and diversity of today's security standards have evolved from the diverse needs of organizations (e.g., different industries), as well as the roles and responsibilities of individuals in the organization. Considering the deep penetration of almost all business processes with IT, the large number of different roles and functions that have to deal with IT security is not surprising. In particular, it is already clear today that not only the IT department has to deal with the subject of IT security, but practically every business function dealing with personal or other sensitive data, or with the technical and organizational provision of infrastructures and services to support the IT.

Organizations can be guided by numerous information security standards and criteria sets in implementing and operating such an ISMS. At this point, a short overview of existing works is given. This chapter details and answers also the research sub-question 3. It deliberately renounces an explicit mention of the current standards, as this would go beyond the scope of this work. Instead, the ISO standards are classified into different areas based on the two dimensions' orientation and architectural level based on BITKOM / DIN (2006). Concerning the orientation, a distinction is made as to whether a standard is more likely to be located at the technical level, can be understood as a guideline or is suitable for evaluation. With regard to the architectural level, a distinction is made as to whether the corresponding standard applies at the product, system or process level or whether it also includes the environment.

All in all, the following is divided into the following five areas, which can be classified as follows:

1. Information security management systems
2. Security measures and monitoring
3. Evaluation of IT security
4. Cryptographic and IT security procedures
5. Physical security

This classification classifies the IT Infrastructure Library (ITIL) and the Control Objectives for Information and Related Technology (COBIT) as "standards with IT security aspects" between the areas of information security management systems and security measures and monitoring. COBIT exists in the literature a variety of different spellings.

Information Security is needed for every enterprise when it comes to multiple devices and data, especially the financial services industry. Without information security, organizations are at risk. Possessing a robust information security strategy is a massive advantage for the organizations they possess. Learning how to protect assets is essential to survival. Having a strategy is more than just a technical approach. It is a crucial tool that needs to be tailored to companies. There are different types of information security management approaches that target specific concerns and may be useful to any business sector, especially to the financial services industry, IT sector and insurance companies. These strategies should become the core of the organization to be successful. In principle, you can integrate security management into business operations as follow:

- Security management - begins with the use of resources to address the threats that occur on secure networks, otherwise known as cyber threats. Conducting a robust security strategy involves assessing your company's risks and weaknesses that are included in the current landscape. Understanding this can put you in a position to implement the right strategy that will protect data and networks through technology.
- Risk analysis - Risk Analysis helps you determine your level of risk tolerance and which you can accept, avoid, transfer, or prevent. Risk analysis can help determine the way the budget is better and prioritize security initiatives.

- Classification of Information and Assets - It is necessary to understand the data and assets that your organization holds and classification based on the importance of core business objectives. This helps you set priorities for security levels and set access permissions for information.
- Approval of Management - Adoption of executive management is the most important factor in the success of a successful information security system. It is vital to compare your security strategy with business objectives to ensure management approval. This can lead to improved employee compliance towards policies and the growth of security budgets that lead to the implementation of effective solutions that support the strategy. Once your organization gets on board with these tactics, you can assess what kind of security you need.
- Application Security - Application Security describes a type of security that includes hardware and software to protect organizations from external threats. As the organizations are moving towards digitalization, threats to an application are becoming widespread. Protecting the finance applications and information of the organization is essential. Many are at risk when it comes to application violations, particularly client records and assets of an enterprise. Various measures can be taken to ensure that applications are correctly implemented. For beginners, the prioritization of multiple threats that can be found through applications can be obtained. This may be anything from unplanned events to hackers or failure to store important information. Second, an organization can apply an application firewall that is a firewall that works to restrict access to a computer's operating system. It controls data derived from central processing units. By checking the data, it determines whether the data should flow to specific destinations, which creates a secure application environment.

3.1 ISO 27000

According to ISO (International Organization for Standardization), ISO 27000:2013 refers to the standard family which provides organizations with a standard for information security management and a general structure for the management system. This standard is created by a wide variety of organizations and compiled by the International Organization for Standardization (Disterer, 2013; International Organization for

Standardization, 2014b). ISO 27001:2013 covers the establishment, implementation, maintenance and continual improvement of an information security management system. It also has requirements to assess and treat information security risks. All the requirements set in the ISO 27001:2013 are generic and intended to be applicable to all organizations, regardless of the size or nature (International Organization for Standardization, 2014a; Shojaie, Federrath, & Saberi, 2014). ISO 27001 is one of the most widely adapted information security management frameworks (Beckers et al., 2012; Wright, 2006). It is a framework for establishing an effective information security management system (ISMS). My research is based on this standard because this framework is widely accepted in the field of information security. It has a top-down approach, and it is based on risks, which means that the framework is technology independent. One of the first requirements during the implementation of ISO27001 is the definition of risk assessment within the organization. According to standard requirements, the risk assessment methodology should be based on business, information security as well as other legal and regulatory requirements that enable accurate identification of the level of risk. The ISO 27001 documentation also describes the need for the organization to be able to identify assets, risks and identify system weaknesses. The maturity model in ISO 27001 can be defined in several points such as by comparing and measuring the benefits with previous projects implements, circumstances that can gather different goals, the model for determining the priorities etc. Hence, it helps us to use the maturity models as a comparative tool to understand what we are expecting from the organization. The biggest challenge of organizations is to determine which maturity model to be used because different maturity models are used for various purposes. Another important aspect is that organizations have different business goals and processes which they want to measure.

As previously discussed, risk assessment is a process that can be considered as an independent process from technology implementation within an organization. Furthermore, the need for its centralization is significant, being a process that also helps to identify problems, risks and threats possible in organizations. As such, the security of information is considered a process that contains many activities within it, and this has driven the need for information security to be integrated into maturity models. Improving the security of information within the organization affects many other processes and may also affect changes in the business strategy, so it is known as an important and long-lasting process that cannot be changed and applied over the night. Management focuses

on proving the information security strength of the organization by implementing information security into the organizational culture, certification, and continuous measurement and monitoring of risk assessment processes. This is an information security approach from the wave's perspective, but it is essential that information security is viewed from the perspective of growth. This perspective enables us to have more detailed and extended information that will allow us to study further and also manage organizational change more efficiently and more valuable.

3.2 CMMI

The Capability Maturity Model Integration (CMMI) defined by the Software Engineering Institute (SEI) of Carnegie Mellon University is gaining importance in Europe. It is an effective tool that helps to improve the effectiveness and efficiency of development organizations (Tapia, Daneva, Van Eck, & Wieringa, 2008). One of the strengths of CMMI is its specialization in product development. This makes it possible to focus on specific aspects in a much more precise and in-depth manner than generalist models such as ISO 9000. For each proposed practice, CMMI provides one to two pages of bullet points and descriptions that can serve as a guide to improvement (Greiner, 2018). Compared to other specialized process models for development organizations, CMMI has the advantage of bringing together different views of the organization. It addresses project management, development, organizational support, process improvement, and management tasks in a common model. In addition to the ability levels, CMMI offers another rating scale. The "Maturity Levels" are the most well-known element of the CMMI. This sorts the process areas into five levels, each representing one of the typical development plateaus in an organization. This presentation helps organizations to improve their development process by suggesting a proven order and prioritization of process areas for improvement. Each level includes a defined set of process areas with a specific maturity level. The designations of the five maturity levels are based on maturity levels. They are as follows:

1. Initial: the initial stage, where all process areas have gaps and the projects have a high variation in estimation accuracy, on-time delivery and quality;
2. Managed: the stage at which the projects are managed and controlled, which means that the organization can manage estimates, on-time delivery, and quality, and successfully repeat a similar project without a standardized approach already in place;

3. Defined: the stage at which projects follow a customizable standard process and where continuous process improvement has already been established;
4. Quantitatively Managed: the level at which the operations are managed using a statistical process control;
5. Optimizing: the highest level at which continuous process improvement is controlled by data from statistical process control.

All reference models provide practices and methods that should assist organizations in the development and maintenance of high-quality products and services (SEI, 2010). Among other things, they affect the workflows of one or more specialist areas and describe an evolutionary improvement path from immature ad hoc Workflows (Maturity Level 1: Initial) towards systematic workflows (Maturity Level 5: Optimizing) with improved quality and effectiveness A CMMI model defines goals so that the desired improvement efforts take account of as many different groups within an organization as possible and achieve company-wide process improvement and practices, which as such represent quite abstract requirements (Kneuper, 2017). Both goals and practices can be generic and specific, but always refer to process areas, which in turn, bundle requirements in a thematic area (Heilmann & Kneuper, 2003). The process areas are summarized in CMMI to maturity levels so that the maturity level of an organization depends on the fulfillment of the (generic and specific) goals of certain process areas.

3.3 NIST

National Institute of Standards and Technology (NIST) maturity model focuses on the documentation of procedures (Ge et al., 2011; Johnson, 2011). This NIST framework is defined in five maturity levels such as Policy, Procedure, Implementation, Testing and Integration in which information security is considered as a risk that is managed through the enterprise risk management process. According to this I have identified the NIST framework as a risk-based framework (NIST, 2014). The focus area of the NIST maturity model is to check the level of documentation (Chapin & Akridge, 2005; Woodhouse, 2008).

Throughout the research conducted in the function of this topic, it has been very apparent that most of the scientific publications in the field of cybersecurity, information security and in general IT field as an essential reference have publications made by the National Institute of Standards of Technology in the US. Even so, these publications remained a common opinion on information security risk management and served as the most

frequent orientation point. As mentioned earlier, based on the research conducted there are models, forms of multiple tools for information risk management, the most common model is the so-called Risk Management Framework (RMF) developed by NIST (fig 3).

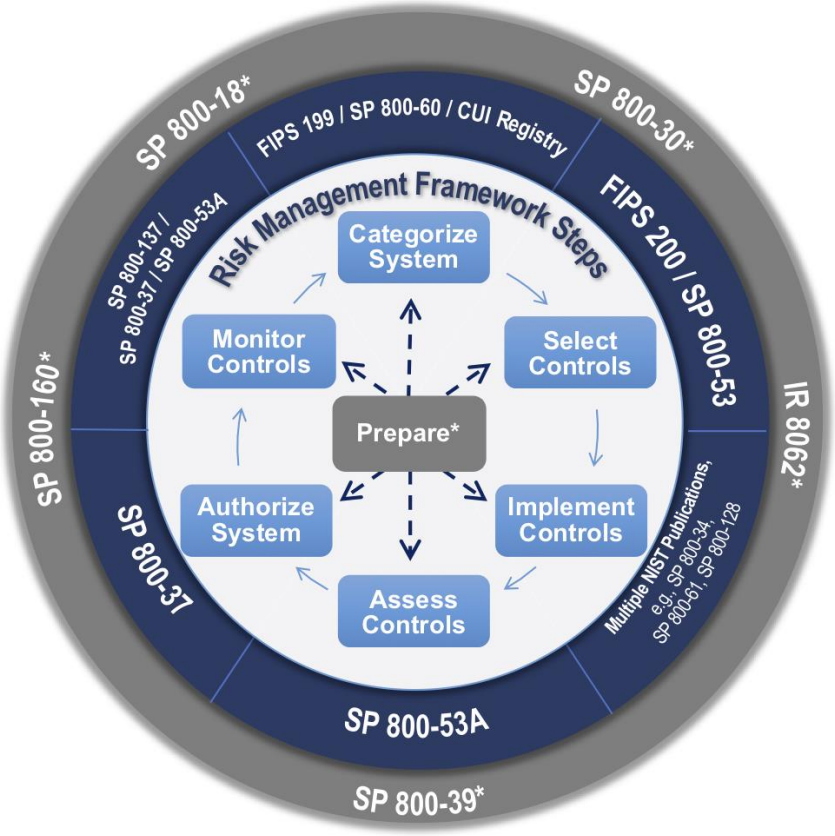


Figure 3 - Risk Management Framework (Nieles & Dempsey, n.d.)

RMF is one of the most commonly used risk management methods. The latter assists the risk management of information security at the system level. Because as mentioned above, there are other forms of risk management alongside this at the system level. In other methods, management is done at different levels, such as management level, organizational level etc. RMF provides an approach to risk management through continuous authorizations of the system and consistent implementation of monitoring processes. In addition, it also provides leadership information to have cost-effective and risk-based decision making (Nieles & Dempsey, n.d.). The management forms, tools and nature of the risk management all depend on the system we are talking about, and about the approach that management of the organization in question wants to have in risk management. Below I will outline the organization of this form of risk management, but without getting into the details.

3.4 Information Security Management Maturity Model ISM3

ISM3 represents one of the standards from the information security area whose main goal apart from achieving the admissible level of security is achieving the business goals. ISM3 is a process-oriented approach, and according to these management activities must follow different categories of the process such as Risk assessment which discovers the treats, attacks and vulnerabilities. The ISM3 was introduced to prevent and mitigate attacks, error and accidents that may risk security (Aceituno, 2007; Open Group, 2011; Stevanovi, 2011). In the beginning the ISM3 system was introduced as a model that can help to prevent and mitigate attacks, errors and accidents that may jeopardize security. Because the ISM3 model recognized three levels of management responsibility, it did not provide the best practices for the implementation of security

3.5 COBIT

According to (Wiesmann, Stock, Curphey, & Stirbei, 2005), COBIT is considered as a risk-management based framework. COBIT is classified as an IT Governance framework that consists of four main domains such as Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME). Each domain has different controls, and for this reason organizations consider using all the COBIT framework or in some cases to adapt specific controls that can fulfill their needs. Because COBIT controls are mainly related to the governance of business objectives, organizations usually point standards such as ISO 2700\0 to integrate it along with COBIT and maximize security controls (Wolden, Valverde, & Talla, 2015). The Control Objectives for Information and Related Technology (COBIT) (ISACA, 2013) defines a method for controlling risks that arise through the use of information technology to support business-related operations. The central basis of COBIT is the responsibility of the management of a company for the achievement of the business objectives, the control the resources used in terms of effectiveness and efficiency, compliance with legal frameworks and the treatment of risks associated with business and resource use (Heschl, 2006). This also applies to the use of IT systems as a resource for the realization of business processes. The COBIT Framework provides a framework that considers all aspects of IT system deployment from planning through operation to disposal, providing a holistic view of IT. Thus, COBIT is thematically in the field of IT governance to settle. Building risk management processes and methodologies is an important step towards aligning information systems with these standards and regulatory frameworks. Decision

making involving risk-taking is an integral part of the business. Choosing the most appropriate option is a challenging task, especially if there is an insufficient number of orientation indicators for assessing the risk. A similar problem is also present in information security. How to choose systems and controls that provide a sufficient level of security, but which are also justified from the business point of view? How to determine the strategy and objectives for information security, while at the same time achieving optimal results for the organization? These are just some of the questions that are raised in providing information and risk management can answer these questions. As a decision-making basis, risk assessment, as well as the entire risk management process, plays an important role in implementing a security management system. Based on the risk assessment, security audits are defined, which are both financially and commercially acceptable, to reduce the risk to an acceptable level. Through the risk management service, organizations aim to provide its customers with a basis for linking security management information management systems or business continuity management to business strategy and objectives. Procedures for registering business processes, identifying resources, vulnerabilities and potential threats to them are the critical parameters for risk assessment. The methods used are tailored to the needs and requirements of the customers within the organization. But despite the methodology used, the outcome of the results from such a process is transparent and repetitive, which is necessary to ensure the process of measuring and comparing results with the previous ones.

Risk management systematically enables timely planning and budgeting of current and future needs organization. The first version of this framework was released in 1996 (Van Grembergen, De Haes, & Guldentops, 2004), and was called “Control Objectives for Information and related Technology”, covering the area of audit (Kadam, 2012). The second edition with enhancements on control assessment was released in 1998 (Heschl, 2006). The third edition was published two years later, and according to (Kadam, 2012) the significant change came with the publication of COBIT Third Edition, with its business objective orientation. At this time, COBIT was termed as an IT management framework. The third edition identified that an organization needs IT not just for information processing, but also to achieve business objectives. In 2005 ISACA introduced a new, fourth version of COBIT with a clear focus on IT governance (Heschl, 2006). A further version of this framework is COBIT 4.1, released in 2007, accepting the

generally used frameworks such as IT Infrastructure Library (ITIL), ISO 27000 series and Capability Maturity Model Integration (CMMI).

With the introduction of COBIT 4.1 in 2007, a new Maturity Model was proposed. According to (ISACA, 2007), this Maturity Model, whose aim is to improve the IT processes, assesses the process maturity to define the future level of process maturity needed to achieve (target maturity level) and finally evaluates the gap between these two levels. To do this, COBIT 4.1 uses a range of levels to assess maturity. According to (ISACA, 2007) COBIT offers approaches to measurement and control based on a maturity model. The individual processes come with six stages as following:

- Level 0: Non-existent
- Level 1: Initial/ad hoc
- Level 2: Repeatable but intuitive
- Level 3: Defined
- Level 4: Managed and measurable
- Level 5: Optimized

For the subject area ISMS relevant is the process "Ensure System Security", that of the domain "Deliver and Support" is assigned. A total of eleven "Control Objectives" also reflect the content of Annex A of the ISO / IEC 27001 standard. Information security is also a cross-cutting task within COBIT. Therefore, information security is additionally treated in several processes of different domains. An illustration of the overlaps between COBIT and the ISO / IEC 27001 standard can be found in (Falk & Falk, 2012). The combined use results in synergy effects. An advantage here is the significantly greater degree of detail of the requirements according to ISO / IEC 27001 [20]. In return, the control and measurement methods of the COBIT framework are used in the context of the ISMS.

The current version of the framework, COBIT 5, was released in 2012. It is built upon the previous version of the framework and two complementary frameworks from ISACA (Val IT and Risk IT); and is aligned with the current best practices such as ITIL and TOGAF (ISACA, 2013). In COBIT 5, the Maturity Model is changed, assigning more importance to the processes. The task of the new Process Capability Model is the same as the Maturity Model, but the structure of the framework is modified. The assessment task

in COBIT 5 is based on ISO/IEC 15504 underlining the strong alignment of this framework with the most generally accepted best practices and standards.

According to (ISACA, 2013), the six levels of the COBIT 5 Process Capability Model are:

- Level 0: Incomplete process
- Level 1: Performed process
- Level 2: Managed process
- Level 3: Established process
- Level 4: Predictable process
- Level 5: Optimizing process

In COBIT 5 to achieve a given level of capability, the previous level has to be completely achieved.

Table 3 Comparison between COBIT 5 vs ISO 27001 (Yadav, 2019)

COBIT 5	ISO27001
Domain 1 – Evaluate, Direct and Monitor Ensured Governance Framework Setting and Maintenance, Benefits Delivery, Risk Optimization, Resource Optimization and Stakeholder Engagement	6.1 Actions to address risks and opportunities, 8.2 Information security risk assessment, 8.3 Information security risk treatment, 7.1 Resources, 7.2 Competence, 7.3 Awareness, 7.4 Communication, 4 Context of the organization, A.15 Supplier relationships
Domain 2 — Align, Plan and Organize Managed l&T Management Framework, Strategy, Enterprise Architecture, Innovation, Portfolio, Budget and Cost, Human Resources, Relationships, Service Agreements, Vendors, Quality, Risk, Security and Data	6.1 Actions to address risks and opportunities, 8.2 Information security risk assessment, 8.3 Information security risk treatment, 7.1 Resources, A.15 Supplier relationships, A.7 Human resource security, A.13.2.4 Confidentiality or nondisclosure agreements
Domain 3 — Build, Acquire and Implement Managed Programs, Requirements Definition, Solutions Identification and Build, Availability and Capacity, Organizational Change, IT Changes, IT Change Acceptance and Transitioning,	A.14.1 Security requirements of information systems, A.14.2 Security in development and support processes, A.17.2.1 Availability of information processing facilities, A.12.1.3 Capacity management,

Knowledge, Assets, Configuration and Projects	A.12.1.2 Change management, A.8 Asset management, A.6.1.5 Information security in project management
Domain 4— Deliver, Service and Support Managed Operations, Service Requests and Incidents, Managed Problems, Managed Continuity, Managed Security Services, Business Process Controls	A.12 Operations security, A.13 Communications security, A.16 Information security incident management, A.17 Information security aspects of business continuity management, A.12 Operations security
Domain 5 — Monitor, Evaluate and Assess Managed Performance and Conformance Monitoring, System of Internal Control, Compliance with External Requirements, and Assurance	9.1 Monitoring, measurement, analysis and evaluation, 9.2 Internal audit, 9.3 Management review, A.18.1 Compliance with legal and contractual requirements, A.18.2 Information security reviews

As described in the literature review, there is a gap between the existing applications, the cost and the features that they possess. However, since such a system does not exist or the features that my proposed framework will have, they do not conform. The auditors and managers of the companies who are dealing with information security need a framework and support to evaluate the level of information security in that company. Because no such framework was found in the literature review. This framework will have some functions such as risk identification and other functions that have already been developed.

3.6 ITIL

The acronym ITIL was initially derived from the term IT Infrastructure Library and has further developed up to the current version 3. It is a best practice reference model for IT service management (ITSM). ITIL also considers security aspects as indispensable components of proper IT operations. The standard helps with numerous corporate process design recommendations so that the planning, delivery and optimization of IT services are supported in terms of corporate goals. The overarching goal is the optimization or improvement of both the quality of IT services and cost-efficiency. As the globally accepted standard for IT service management, the currently valid version 3 concentrates on five central topics:

- Service strategy,
- Service design,
- Service transfer,
- Service operation and
- continuous service improvement.

With the release of Version 3, the strategic planning process for integrating IT service management with the corporate strategy was further optimized, thereby ensuring compatibility with the IT service management standard ISO / IEC 20000 [18]. IT security management is seen in ITIL as a separate discipline outside of IT service management. The ISO 20000 standard only contains general specifications for setting up IT security management. In terms of content, however, there are many overlaps with the ISO / IEC 27001 standard.

Table 2 - Information Security Maturity Model Comparison (Aceituno, 2007; Dzazali & Zolait, 2012)

Basic of comparisons	**COBIT 5**	**SSE-CMM**	**ISM3**
Goals of ISM assessment/ranking	As a mean for an organization to enables an organization to establish a ranking for the way it manages information security as a means of identifying improvements and actions to take	As a tool for engineering organizations to evaluate their security engineering practices and define improvements	As an assessment tool to define maturity in terms of information security management processes
Target Domain	All aspects of information and its supporting ICT	Information Technology and Engineering	All aspects of information and its supporting ICT

Scope of Coverage	Covers all aspects of IT governance aligned with the business requirement of the organization. Involves six dimensions of maturity awareness, training, communication, processes and practices, techniques and automation, compliance and expertise.	Covers activities were crossing the entire trusted product or secure system life cycle. Three basic areas; risk, engineering and assurance	Covers the environment and mission of the organization in four areas; information security management system; organizations system, information system, security in the context
Maturity Levels	Six levels ranking of 0-5	Five levels ranking of 1-5	Five levels ranking of 0-4
Description of the Levels	Describe the attributes of information security management processes	Descriptions of the security attributes necessary to be achieved for the level	Describe the results of the information security processes
Basis of assessment or maturity criteria	Looks for evidence of the existence of information security processes in six domains	The maturity criterion is to identify industrial practices and form them info maturity standard	Searches for confirmation of the existence of processes at their three management categories; strategic, tactical and operational.

The literature has shown that in general, maturity models have been applied only in the documentary aspect without integrating any technology tool that would increase the speed of the results, the accuracy would be greater, and the easiest application to consider the possibility of mobility through computer equipment. This makes it essential for my proposal to have a semi-automated framework that would provide quick and efficient results with accurate descriptions of the steps that need to be taken to increase the security of information within the organization.

4. Risk Assessment Models and Software

Based on studies on risk assessment in information security, there is a wide range of models used in identification, assessment and risk analysis processes. Among them are the following models: FAIR, OCTAVE, CURF, CRAMM, CORAS, RISK IT etc. In the following I have described three of these models, which have more extensive use such as FAIR, OCTAVE and CURF and CRAMM.

FAIR - Factor Analysis of Information Risk - is a practical structure for understanding, measuring, and analyzing information risk and enabling informed decision making. This structure consists of many interrelated models that explain how the main elements of risk work. Information Risk Factor Analysis describes the dynamics of the risk event, why it happened, and how it happened. This analysis serves to measure the amount or magnitude of risk and management with it. FAIR is the only international quantitative model for cybersecurity and operating risk. FAIR classifies the factors that contribute to the risk and how they affect each other. Mainly takes care of finding the exact probability of the frequency and size of data loss events. FAIR points out that danger is an unsafe event, and we should not focus on what is possible but on how likely it is to happen. The probability approach applies to any risk analysis. The risk in my case presents the likelihood of losses in the form of assets. The potential loss of assets stems from the value it presents and the responsibility it poses to the company. The FAIR structure is used to reinforce existing risk analysis processes, rather than to replace them. Using a FAIR model for non-commercial reasons can be done with a simple creative license, but using FAIR to analyze someone else's personal risk requires a special license (Freund & Jones, 2014).

OCTAVE - Evaluating Operationally Critical Threats, Assets and Weaknesses - is a model used to improve and adapt the information security risk assessment process so that an organization can get enough results with a small investment in time, people and other sources. This makes the organization take into account members, technology and equipment in the context of their relationship with the information and business processes and services they support. When using Octave, design requirements should be considered based on field experience, guidelines, cases, and existing notes (Caralli, Stevens, Young, & Wilson, 2007). One of the goals of OCTAVE is to help organizations ensure that their information security actions are level with the goals and objectives of the organization. OCTAVE was created to help organizations make a risk assessment in information

security by relying on operational and strategic mechanisms to fulfill their mission. The way this model works and is highly efficient is based on the fact that the danger is identified and analyzed from the source at the point where the data is stored, transported and processed. Focusing on the operational risks of information assets, participants learn to see risk assessment in the context of the organization's strategic objectives and risk tolerance. The implementation cycle of OCTAVE is based on eight processes divided into 3 phases. The first phase is the development of initial security strategies, the second phase is the identification of infrastructure weaknesses from the technological point of view, and the third phase is the development of the strategy and the security plan. Apart from OCTAVE, there are also several newer generations like OCTAVE Criteria, OCTAVE-S and OCTAVE Allegro. All focus on giving proper attention to risk assessment but having different access to information assets and their elasticity. This approach improves the ability of the organization to evaluate the risk in such a way as to produce the right and fruitful results (Caralli et al., 2007).

CURF - The main structure of unified risk - is a comprehensive approach to comparing different risk assessment methods in information security. It is inclusive as it has grown organically, adding new issues and tasks from each of the reviewed methods (Wangen, Hallstensen, & Snekkenes, 2017). If any assignment or issue was used earlier in the risk assessment and was not present in the CURF model, then it was included in the model, thus achieving a complete set of risk-study methods. CURF has a bottom-up approach, and besides comparing and classifying different methods, it is used to measure their completeness. The use of CURF enables us to select the best method and technique for risk assessment in my case. CURF results can recommend applying a particular ISO standard, or even using one of the above-mentioned OCTAVE models. There are many competing structures with CURF, but the difference is that these structures use the top-down comparison approach, which limits them to the tasks and parameters within their criteria. The CURF bottom-up approach enables the examination of any risk assessment method in information security and uses all tasks as benchmarking criteria. The idea of the CURF structure is that all known methods are used in turn to identify the tasks that these methods contain, and all these tasks deriving from each approach join in a single set. The CURF model consists of three main activities: risk identification, risk measurement and risk assessment. From these main activities, CURF contains these processes: a preliminary assessment, definition of risk criteria, identification of parties,

identification of assets, identification of weaknesses, identification of threats, identification of controls and identification of results (Wangen, 2017; Wangen et al., 2017).

There are various software applications for different models, techniques and different methods of risk analysis. These software's use methods and techniques such as questionnaires, checklists, passive assessment, active evaluation in various versions to obtain appropriate risk analysis information. Before we decide which application to use, it is needed to define the testing process we want to apply. If we are dealing with the overall assessment of the company, we can use applications that have the form of the questionnaire, or if we want to test any organization software then we can use apps that make an active evaluation. In this case, active assessment means using an application to test the organization's software stability by making attacks in various forms such as password attack, database attack, phishing attacks, and so on. In some cases, applications are built on the functional structure of the models.

FAIRiq software is the "quantitative risk engine" for the FAIR model, which's primary goal is to find the source of risk. This software achieves this by taking measurements of risk factors and applying sophisticated mathematical principles to find the risk. FAIR provides a centralized "warehouse" of analysis to have a general overview of the risks, an overview of the accumulated risk, a simple view of risk comparison for their prioritization, a centralized asset database, potential risks, tables losses, users, graphs, etc. Like the FAIR model, this software is quite complete as it is a combination of some models and is complemented by some other software. This software delivers results of risk factors, why it happened and how it happened, but focuses on extracting accurate quantitative results. At the risk identification stage, FAIRiq receives an average rating because it does not consider the weaknesses or threats but at the stage of measurement and quantitative analysis gets maximum estimates. From these estimates together, this software is counted among the complete software for risk assessment (Freund & Jones, 2014; Jones, 2005).

Octave software is used to identify and assess the risk of information security. They try to help organizations set up quality risk assessment criteria that describe the level of company tolerance to operational risk, identify assets that are important to the organization, identify threats and weaknesses to these assets, assess potential damages to the organization if the risk is realized etc. For the OCTAVE model, there are several

software generations, created by CERT in a way that we have different access to information assets and the elasticity in their use. The latest models like OCTAVE Allegro have not been created to replace the pre-models, but to create selection varieties. However, each version of OCTAVE has broad applicability and users of these methods can choose the approach that best suits their security risk assessment information needs. So, based on the type of our organization and the sensitivity of the information we have in the database, it varies and selects the software generation in the OCTAVE model. This software proves that from risk analysis to bring qualitative results (Caralli et al., 2007)

CRAMM, as a matrix model, depends heavily on supporting software to provide full support. This software serves to analyze and manage quality risk. This tool was built by the UK government to provide a method for reviewing security information systems. The CRAMM Manager can be used to justify costs in the security of information systems and networks and testing of standards compliance for the certification process. CRAMM software is quite complete in the risk identification process, while in the risk measurement process it only gives some quantitative data based on past events, so it generally does not stand well in the risk measurement process (Yazar, 2002).

An analysis of some of the existing applications and frameworks that relate to information security and risk assessment processes have identified some gaps (see below). The applications and frameworks I have analyzed are quantitative risk assessment system, OCTAVE Allegro, FAIRq, CRAM.I identified the following gaps related to the comparison of the application:

Application / Framework	Gaps
OCTAVE	• It’s complex to use. • Organizations don’t have the ability to mathematically model risk. • It’s a solely qualitative methodology
FAIR	• It’s not thoroughly documented as other methods. • Virtually no access to existing material regarding the methodology or illustrations in what way the methodology is used.

CURF	• Lack of information to implement • Not well documented • Results are not very clearly explained • Miss of the scoring system
CRAMM	• Lack of documentation • Compatibility • Most of the activities are based on paper

Based on the above findings as well as the experiences it has been identified from the preliminary results, the security risk assessment framework will cover the above-mentioned gaps by creating a model that is compatible with all platforms. Additionally, the system will offer the possibility of comparing the results from two different assessments that would also enable the identification of improvements.

4.1 Vulnerabilities Rating System

For companies, a comprehensive information security strategy is, therefore, becoming increasingly important. On the one hand, this takes into account the complexity of the networks, but also developments in the threat landscape. It also determines which information security vulnerabilities require immediate attention. To use data collection and analytics to respond to threats and make strategic information security improvements, organizations need to focus on automation. Transforming pure data into useful and, most importantly, relevant information improves security measures, reduces IT costs, and cushions the organization's growing security shortage. Information security vulnerabilities and are a complex issue, but with a robust model, you can achieve a lot of results. To have a qualitative information security risk assessment, I provided a scoring metric which is separated for different security controls. It does not only provide a quantitative baseline which can help the organization to make improvements, but it also provides the ability for everyone in the organization to have the prevailing opinion about security. The results generated by my proposed framework are based on a system of estimation of the probabilities which are calculated in the backend of the system. This system is designed to provide organizations with a better understanding of which identified high-priority vulnerabilities need to be closed. In my research I have analyzed

the CVSS (Common Vulnerability Scoring System) which is a risk assessment tool designed to identify the common attributes of several security issues. The reason I choose to analyze CVSS is that it includes a standardized vulnerability score that may be meaningful across the organization and also it is essential that CVSS is an open framework model and any metric is open and available to all users while also it helps organizations to prioritize the risk. The common vulnerability scoring system, or CVSS for short, is an industry standard that severity of a software security vulnerability or risk, as well as the priority and urgency to respond accordingly. This is reflected in a numerical score, from 0 [no threat] to 10 [very critical], which is calculated using defined criteria (metrics). The numerical score can be in one of four qualitative representations that can be translated. The qualitative presentations should help companies to correctly assess and prioritize their vulnerability management processes. So, there is one critical severity of a software vulnerability a greater and faster need for action than with low severity. CVSS enables different, incompatible rating systems to share their information with one another change. In CVSS, the various assessment criteria for vulnerability are divided into three different metric groups such as: Base Metric Group, Temporal Metric Group and Environmental Metric Group and this group contains each other's metrics.

4.1.1 Base Metric Group

In the Base Metric Group, the essential characteristics of vulnerability are defined, which remain constant over a period of time and a user environment. There are two types of metrics in this group, the exploitability metrics and the Impact metrics. The exploitability metrics reflect the lightness and the required technical means, which were necessary to exploit the vulnerability, whereas the impact metrics the direct consequences of successful exploitation of the Represent vulnerability. The base metric group's metrics are specified by software providers and information security and vulnerability analysts, since they usually have the most precise information about the properties of a vulnerability.

4.1.2 Temporal Metric Group

The temporal metric group represents the characteristics of a Vulnerability that can change over time. This will make the time-dependent Vulnerability characteristics reflected and the CVSS score is corresponding to the adapted to current risks. The characteristics of the Temporal Metric Group include the availability of exploit kits or techniques, the progress in fixing the vulnerability and confirmation of the technical

details of the vulnerability. The three metrics can CVSS score even in the worst case (no exploit necessary [E: H], no solution available to fix vulnerabilities [RL: U], confirmation of the vulnerability [RC: C]) not increase. For example, releasing a patch can reduce the risk of a vulnerability, resulting in a reduction in the CVSS score of 5.0 affects 4.7. As with the Base Metric Group, the metrics of the Temporal Metric Group are specified by software providers and vulnerability analysts.

4.1.3 Environmental Metric Group

The environmental metric group represents the vulnerability characteristics that are relevant to a user environment. In this case, the implementation properties and the user environment are dependent on Vulnerability characteristics captured. The Environmental Metric Group's metrics allow an analyst to incorporate security controls that can mitigate various consequences, as well as a higher or lower downgrading the weight of a vulnerable system depending on the business risk.

There are two types of metrics in the Environmental Metric Group, one of which is related to the user environment and the other deals with security requirements. These metrics allow analysts to tailor the CVSS score for specific user environments. How strong this adjustment can be on the one hand because of the importance of an affected IT for the users of a company, measured in terms of Confidentiality, Integrity and Availability, on the other hand by determining the consequences of a successful exploitation of the vulnerability, such as the proportion of PC workstations affected and potential of collateral damage. This is achieved, among other things, by rebalancing the impact metrics from the base Metric Group. For example, the integrity requirement determined in the Environmental Metric Group influences the assessment of the Base Metric Group's integrity impact. The metrics of the Environmental Metric Group are specified by Information Security and IT experts who are responsible for the corresponding system, because they are best able to assess the potential impact of a vulnerability in their own IT infrastructure.

According to the structure and function of CVSS and as well based on my proposed framework, I have created a score-based model 1 to 5 as follows:

Table 3 - Risk Assessment Proposed Scoring Model

Level	Numerical
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 - 10

Each of the security control groups will have a summarization of their result based on the user selections. The resulting score serves to guide the affected organization in the allocation of resources to address the vulnerability. The higher the severity rating, the more significant the potential impact of an exploit and the higher the urgency in addressing the vulnerability. While not as precise as the numeric CVSS scores, the qualitative labels are very useful for communicating with stakeholders who are unable to relate to the numeric scores.

5. Research Overview

5.1 Research scope and questions

The study is aimed to propose a risk assessment framework and a related workflow that can be automated for the organization to create a report and evaluate the security risks. The proposed framework is intended to utilize the model of ISO 27001 and its technical implementations for the current study. The objective of the study is to analyze the assessment methods of vulnerability in information security and to propose an effective model after analyzing the existing maturity models. My research is based on the evaluation of four maturity model frameworks i.e. ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model. The gaps in the current maturity models identified through the literature review are such as the price of

implementation because of the commercial standards (ISO 27001 and ISM3) (Stevanovi, 2011), then lack of customization and the attempt to implement one-size fits all standard through which small organizations face difficulties because there are processes which are not used on organization and also the period of implementation which takes a long time because of many administration procedures until the final implementation (NIST, ISO 27001, SSE-CMM) (Becker, Niehaves, Poeppelbuss, & Simons, 2010). Another important issue, mentioned in the literature review as weaknesses is the lack of guidance and complex structures of implementation (COBIT 5) while at the same time the number of case studies on COBIT is very limited (Zhang & Fever, 2013). The gaps in the current maturity models identified through the literature review and with the investigation of the related standards. Additionally, I collected information about the gaps through surveys at the investigated companies. I developed a new risk assessment framework using the information gathered in the gap analysis. The framework will take ISO 27001 as a base framework and the focus will rely on technical parts of the framework rather than the documentation process. The currently prevailing IT risk management approaches as a good example witnessed through the literature. It is necessary for risk professionals and auditors to have a maturity model through which they can check if the investigated risk management practice meets with the expectations and produce the required results. Many risk management programs have built on risk maturity model which can be broken down into many other sections focusing on core attributes (Wright, 2014). Recently, there is an increased interest in the maturity models in the research community and its practical implications (Mettler, 2009; Poeppelbuss et al., 2011). The most popular maturity model is Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for software development and the successor Capability Maturity Model Integration (CMMI) (Poeppelbuss et al., 2011). Since now, several new maturity models have been developed for different sectors and industries including, IT/business alignment (Khaiata & Zualkernan, 2009; Luftman, 2003); business process management (Bruin & Rosemann, 2005), business intelligence (Hewlett, 2007); project management (Kent Crawford, 2006); information lifecycle management (Sun Microsystems, 2005) digital government (Gottschalk, 2009); inter-organizational systems adoption (Ali, Kurnia, & Johnston, 2011) and enterprise resource planning systems use (Holland & Light, 2001). There are several risk assessment systems that help the companies, but these are usually not dedicated to an audit report preparation and they do not provide recommendations according to the risk assessment results. According to the literature (Von Solms & Von

Solms, 2005), there is a gap between the implementation of the information security standards in business sector needs and objectives of the standards.

5.2 Research Questions

In this regard, the current research will try to find the answer for the following main research question which is followed by three sub questions:

Main Research Question: How can we develop the semi-automatic risk assessment system? How risk assessment systems can be extended to provide a list of recommendations by identifying the list of areas with a lack of suitable security measures through an automated risk or semi-automated assessment solution?

For the mentioned research question, a software application is developed that will apply a semi-automated information security risk assessment method that will compile a list of recommendations from the assessment findings **(Chapter 7 – Risk Assessment Maturity Framework Prototype)**. The system prototype is created based on the findings from the literature, comparison of maturity models and interviews with individuals of the companies from the IT sector, banking sector and insurance companies.

Sub-question 1 (followed by Main Research Question): How is the risk assessment process in the context of the information security management systems' implementation handled within the organizations (specifically on the IT sector, banking sector and insurance companies)? What are the key elements of the maturity framework in the field of risk assessment, how can it be described conceptually?

For answering this question, I performed a survey and have interviews to explore how organizations implement information security management systems. Discussion of the answer to sub-question 1 is available in **chapter 6**. The survey is based on ISO 27001, because that is the main standard of information security management. The other three maturity models, which I reviewed, are counted as well.

Respective factors reviewed i.e. what standard is used, how effective is the usage, and how they determine the level of risk within the organization? Also, at this point, I also reviewed the part of the controls that are applicable in each sector. The questionnaire is divided into several groups of controls, from the ISO 27001, which are analyzed by the control group and the sectors, where after a detailed analysis I aim to identify the most important controls for each sector, and simultaneously identifying problems and gaps of the mistakes that exist between the sectors.

Sub-question 2 (followed by Main Research Question): How can we map the findings of the risk assessment process for the information security maturity models?

To answer this question, interviews are conducted from the participants employed for the study and data were collected from organizations of IT, banking and insurance. The result of this phase is a conceptual model of the semi-automated risk assessment system describing the information security maturity levels, I detail it in chapter 7.1.

I have developed the framework prototype to determine the level of maturity within the organizations **(see chapter 7)**. My framework does not provide only the general maturity about the organization, but also maturity for each sector such according to the information security control objectives of the ISO 27001.

Practices show that it is necessary to have a level of maturity (usually 5 levels where 1 is the most undeveloped and the 5 is the highest maturity) where the organization can define the following issues:

- generate reproducible and valid measurements
- establish actual progress in the security
- rank themselves against a range of organizations
- determine the order in which security controls should be applied
- determine the resources needed to apply to the security issues

My approach combined ISO 27001 Control Objectives and Common Vulnerability Scoring System in order to offer a unique solution on measuring information security maturity level for the above-mentioned sectors.

Sub-question 3 (followed by Main Research Question): Is it possible to measure the maturity of the risk management practices within a company through a semi-automated risk assessment system according to the literature?

To answer this research question, first the relevant literature describing the digital maturity models in the context of information security has been reviewed (**see Chapter 3**). In most cases, automated processes have been used mainly by audit firms. However, the different organizations are represented in the same way as the standardization models are, and the processes are the same as the ones that are in the aspect of time, as well as the financial aspect. A survey was being used in order to identify the customized model needs of auditors in **Chapter 6.**

After a detailed analysis of the literature and the feedback from the survey, the most appropriate approaches are listed that made easy to use and efficient for the identification of audit findings within organizations' systems.

5.3 Research Methodology – Design Science Research

The following chapter explains in detail the research design, the method used for the collection of data, the analysis technique used to draw the results and conclusions as per the aims and objectives of the study. A detailed description of research participants, research assumptions, sample population, data gathering tools, and the justification for analysis technique has been presented below. The research methodology of any research can be the most important part of the research study which provides the set of techniques to a researcher who intends to use or gather, interpret and analyze the data to reach a conclusion for the predefined research questions or hypothesis of the study. This practice is essential for the authenticity of the research (Cooper & Schindler, 2006). In the process of articulation of research methodology for the study, design science research has been adopted. The reason why I chose the design science research method is that it is a problem-solving approach that has its origins in the engineering disciplines. The design science research combines ideas, practices, technical skills and products (design artifacts) that make the analysis, design, implementation, management and use of information systems more effective and efficient (Hevner, March, Park, & Ram, 2004). This approach fits on my proposed framework which combines the engineering disciplines but also is based on the existing theories and standards applies to information security. So, the design science research method helped me to make possible the development of my Framework prototype based on scientific and practical criteria.

I perform this research method through a mixed strategy, combining qualitative and quantitative approaches. Data gathering methods include the information obtained from the questionnaire, direct interviews, and literature review. My research strategy is considered as strategy that fits the business informatics field and sometimes it is considered as a new discipline. However, unlike existing Anglo-Saxon methodologies about information research, business informatics and information systems prefer a methodology that has a design science-oriented approach. I chose this method in my research because it is precisely the method that is based on engineering discipline combined with science and artifacts. My research thesis touches on the research problems

of architecture and reports on experiences made with design science research in architecture.

Another important issue on the design science methodology is combining the creation and evaluation of the artifacts to solve and organizational problem, which in my case is the need for a semi-automated framework in order to measure the level of information security risk in organizations. The artifact represented in my research is the web-based application framework developed.

I followed the design science research methodology and the process model to present my work as it is shown in Figure 4.

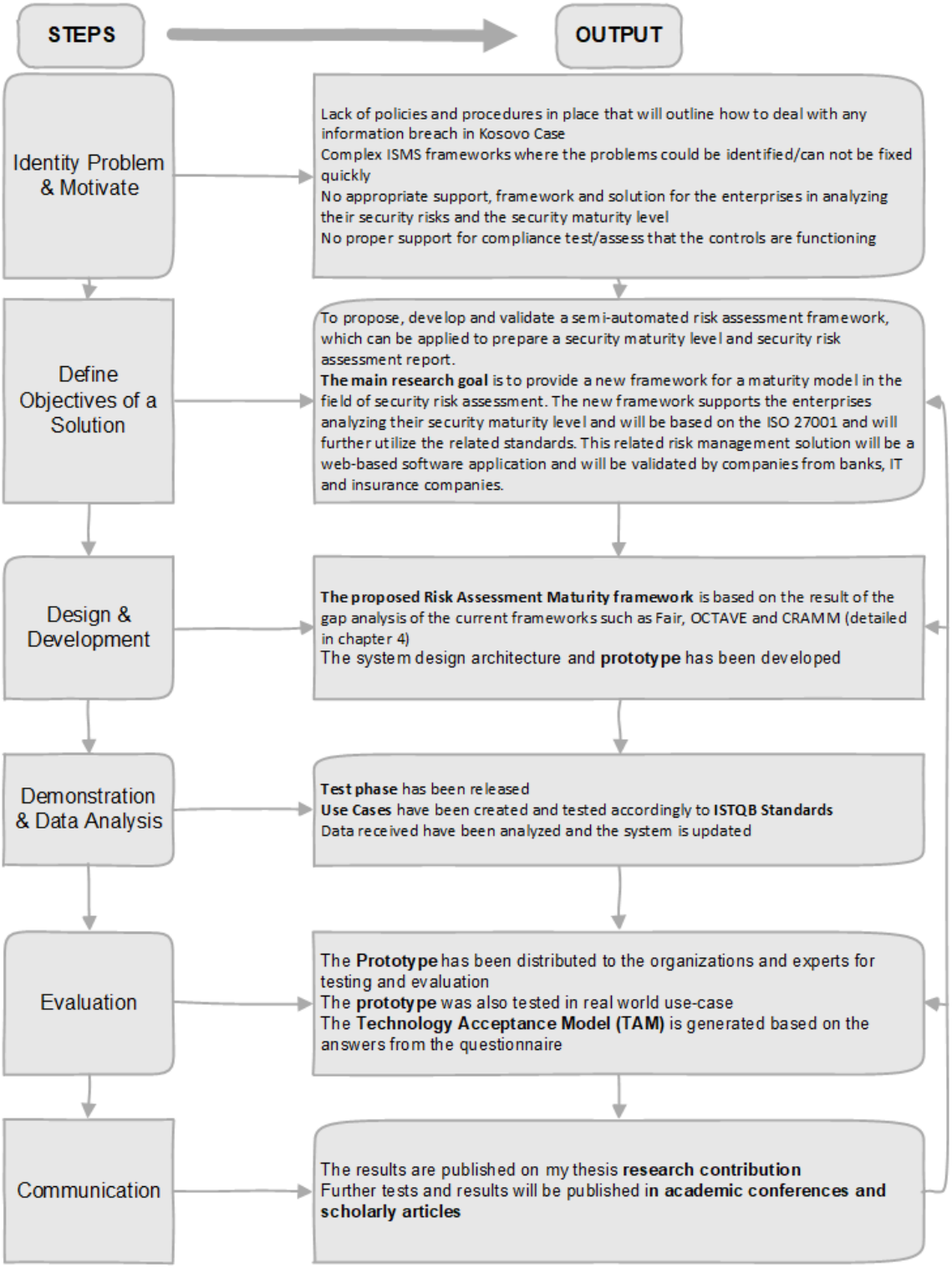


Figure 4 - Design Science Research Methodology process model (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007)

Design Science Research is geared towards practical research, recognizable by the application-oriented demands and objectives, such as the feasibility of the artifact, the development of technology-based solutions, the mentioning of means to be used or the mentioning of the economy as problematic.

The first phase of the current study has adopted the qualitative research design in which the existing literature is analyzed with respect to the current risk assessment methods to make comparisons about the available maturity models. This analysis and identification of the gaps were helpful for the next step of the study to reach the final answer on the main research question and sub questions. There are commonly two research designs termed as quantitative and qualitative. The quantitative research can be termed as the one which deals with the hard data in the form of figures or numbers (Amaratunga, Baldry, Sarshar, & Newton, 2002), whereas; the questions concerning about "why and how" of human behaviors and perceived realities are intended to be answered in the qualitative research (Rajasekar, Philominathan, & Chinnathambi, 2006). In the current study, the available literature has been analyzed for the maturity models to identify the common issues, problems, or factors; which are influencing the effectiveness of risk assessment systems specifically in the domains of IT, banking and insurance.

This research is an exploratory study in which an inductive theoretical approach is adopted to compare the current decisive risk assessment methods such as ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model, ISO 27001. After making the comparisons, the data were collected from the selected organization from the IT, banking and insurance sector to understand the current situation of information security management systems at the ground level and the methods used by the selected sectors for the identification of risks, its assessments and treatment.

5.4 Design and Engineering Cycle

Following the design science research methodology, I chose the design and engineering cycle as the problem-solving process with the structure as I have presented in Figure 5.

As the design and engineering cycle is built on four main pillars such as problem investigation, treatment design, treatment validation and treatment implementation. Each of the pillars consists of specific tasks and questions that must be answered in order to have the complete design and engineering cycle process (Wieringa, 2014).

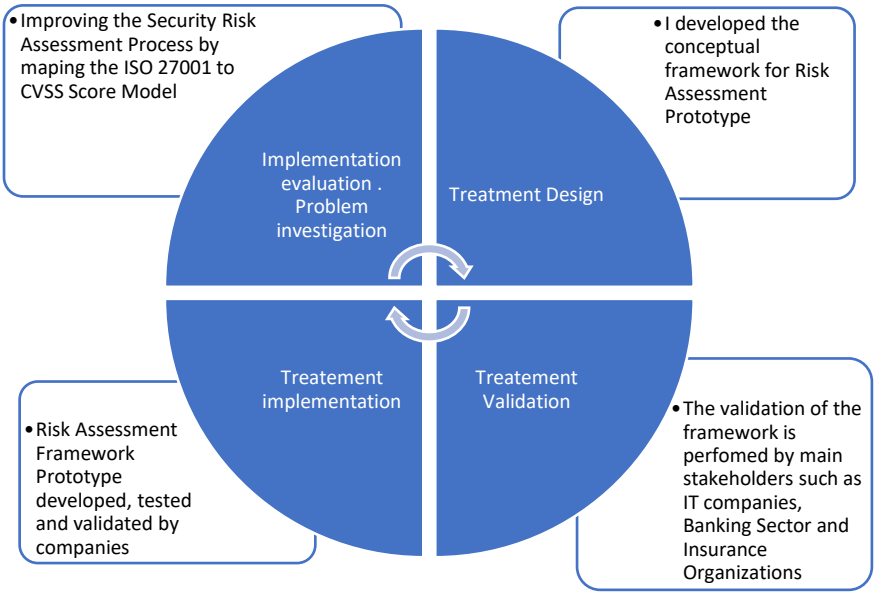


Figure 5 – Research method applying on design science cycle

In Figure 5, it is presented briefly my research and framework prototype lying into the four pillars of the design science. In the following I am going to present a detailed approach of my framework prototype according to the specific tasks and questions that are part of each pillar in the design science cycle.

Problem Investigation

As shown in Figure 5, the first element of the design engineering cycle is Problem Investigation. At this point answering questions like: What should be improved and why? in my research, I want to simplify the risk assessment process in information security through a semi-automated model that links to the ISO 27001 Information Security Objectives and open scoring system CVSS model. Turning to the research I have conducted on identifying the needs of organizations about measuring security level, I have identified a gap between the application of security standards and the way security level is measured.

Treatment Design

I have developed a risk assessment framework concept that is tested and operational. This framework, which is easily accessible and implemented by IT auditors and security experts, will enable you to more quickly generate reports on security levels and a list of recommendations for changes.

Treatment Validation

My framework is validated by organizations stakeholders and experts from the field such as IT Auditors, Information Security Officers and so on. The stakeholders will evaluate and validate the system and after will complete a questionnaire which is part of the After-Scenario Model (ASQ) which is followed by the Technology Acceptance Model for the framework prototype. With the ASQ model my aim is to get the results about the framework prototype based on: framework usefulness, time consuming, interface quality and information quality. The questions are created on the Likert Scale 1 – 5.

Treatment Implementation

In this phase of the engineering cycle, I will finalize and transfer to the practice and deployment of my framework prototype. This implementation can be iterated through the new engineering cycle that can be followed by an evaluation experience.

This approach involves testing theory and hypothesis to establish the artifact which in fact is the framework prototype(Hyde, 2000)[126](Hyde 2000)(Hyde 2000)(Hyde 2000)(Hyde 2000). This approach is concerned with the collection of data and then the formulation of a theory on the basis of analytical findings (Thomas, 2006).

5.4.1 Research Design; Mixed Method Research and Its Justification

To understand the views of the researcher as well as participants, a plan or course of action is identified to solve the problem in the real-life scenario which can be termed as a research design (Kothari, 2004). It can be said that there is no right or only one procedure for the conduction of research because the approach depends upon the number of important and influential factors such as the topic of the study, audience, participants, time, availability as well as the maximum utilization of resources (Greener, 2008). Everyone is engaged in a research process through the search for a solution to a problem. Therefore, research has a relationship with everyday life and activities.

Historically, researchers were forced to choose between a quantitative approach and a qualitative approach. However, now, there is a third approach which is mixed methods research (Kaplan, Duchon, & Study, 1988; Leech & Onwuegbuzie, 2009). The overall research will adopt a mixed method research design by employing both qualitative as well as quantitative data collection methods and techniques. Creswell (Creswell, Klassen, Plano, & Smith, 2011) reported that several authors have recognized the advantages of using mixed methods within a single study and numerous mixed methods studies have been reported for social scientists. Generally, a mixed method begins by investigating and

understanding the social world to collect evidence for the study. The social inquiry is targeted toward the many sources that influence a problem, such as policies, organizations and individuals (Creswell et al., 2011). Mixed methods research involves a mixture of concepts from both qualitative and quantitative research (Johnson, 2011). The integration of both quantitative and qualitative data increases the strengths and decreases the weaknesses of each data type (Creswell et al., 2011). As a result, the mixed methods approach has several benefits, because it uses more than one method, researchers can collect more information on different aspects of the topic being researched (Giddings & Grant, 2006). Using mixed methods may provide greater diversity, and it could lead to better confidence in the research conclusion (Mark Saunders & Thornhill, 2016). Gray (Gray, 2014) stated that qualitative and quantitative methods could be conducted separately, without any particular order; thus, a researcher may carry out the qualitative and quantitative portions either sequentially or concurrently (Caldas, 2009; Giddings & Grant, 2006). According to Saunders (Mark Saunders & Thornhill, 2016), there are two main forms of sequential design (mixed methods complex), sequential exploratory research design and sequential explanatory research design (Creswell & Plano Clark, 2007). The former is when a researcher uses the qualitative techniques of data collection and analysis in the first phase, which is followed by quantitative techniques of data collection and analysis at a second phase. On the other hand, the latter is when a researcher uses the techniques of quantitative data collection and analysis in the first phase, which is followed by qualitative techniques of data collection and analysis in the second phase (Creswell et al., 2011; Giddings & Grant, 2006).

During the first phase of the study, literature describing the digital maturity models in the context of information security is analyzed so that the more appropriate approaches can be listed to be used easily and efficiently within the context of the organization's risk assessment systems. Risk assessment processes and systems adopted by the IT, banking and insurance companies are assessed and analyzed to identify any gaps in the implementation of information security management systems. It is analyzed how the organizations from the sectors of IT, banking and insurance have implemented the information security management systems and how effective these systems are for the information security of the organizations. It will also be identified that what organizational factors are affecting the effective implementation of information security maturity models within the context of the organization.

Using mixed methods may provide greater diversity, and it could lead to better confidence in the research conclusion (Mark Saunders & Thornhill, 2016). Gray (Gray, 2014) stated that qualitative and quantitative methods could be conducted separately, without any particular order; thus, a researcher may carry out the qualitative and quantitative portions either sequentially or concurrently (Caldas, 2009; Giddings & Grant, 2006). According to Saunders (Mark Saunders & Thornhill, 2016), there are two main forms of sequential design (mixed methods complex), sequential exploratory research design and sequential explanatory research design (Creswell et al., 2011). The former is when a researcher uses the qualitative techniques of data collection and analysis in the first phase, which is followed by quantitative techniques of data collection and analysis at a second phase. On the other hand, the latter is when a researcher uses the techniques of quantitative data collection and analysis in the first phase, which is followed by qualitative techniques of data collection and analysis at the second phase (Caldas, 2009; Creswell et al., 2011; Giddings & Grant, 2006).

5.4.2 Population and Sampling of the Study

The population can be referred to as the, the whole set of units which is intended to be observed through systematic and scientific methods in a research study (Lee, 2014). Within a research study, a sample is selected from the whole population which is the selection of a few units or few individuals as the representative of the whole population (Kumar, 1996). Sample can also be said as the sub group of a population which is being observed and investigated by the researcher during a research study so that the predictions can be made for the whole set of population.

The population for the present study is the organization or companies from the IT, banking and insurance sectors in the Republic of Kosovo. In total I have interviewed 72 companies respectively, 37 companies from the IT sector, 15 insurance companies and 20 banks. The technique of purposive sampling is adopted to recruit the sample participants for the collection of the data through questionnaires and interviews. The sample participants were responsible for the information security systems at their respective organizations within the IT, banking and insurance sectors. The participants include; chief information security officer, data protection officer, information security and assurance, and risk management officer, depending upon the structure of the sample company. According to Collis and Hussey (2013), there are several commonly used sources of evidence in research, which come from two main sources: qualitative and

quantitative. The quantitative data for the study is collected through the questionnaire, whereas the qualitative data is collected by the interviews.

I perform this research through the mixed method, combining the information obtained from the questionnaire, direct interviews, and literature review. The questionnaire was distributed to 97 organizations from the banking sector and insurance companies and IT industry and I received 72 of them completed the questionnaire. For this research, it was beneficial to collect the relevant quantitative data through the questionnaire from the selected sample participants to have a significant amount of evidence regarding the currently prevailing information security management systems in the selected organizations to make the comparisons for the information security standards. The review of the literature identified the important and crucial areas and the questionnaire was developed by the researcher in accordance with the research objective of the study. According to Gray (2014), the use of questionnaires has many advantages. First, questionnaires save both money and time, since they can be sent to a large number of respondents at a low cost. Secondly, respondents' feedback and replies are returned within a short amount of time. Thirdly, coding the questions is often a very simple and quick process. Lastly, the respondents can complete questionnaires at times and places that are suitable for them. The research question intended to be answered through the questionnaire is, "How is the risk assessment process in the context of the information security management systems' implementation handled within the organizations (specifically on IT sector, banking sector and insurance companies)?"

One of the most important sources for the collection of data and evidence is the interview which is more concerned about the views, opinions, and perceptions of human beings. An interview is considered as the most significant tool to gather in-depth information regarding the attitudes, behaviors, perceptions, knowledge, and opinions of the individuals who are the social actors in any contemporary situation (Gray, 2014). The interview is of three categories i.e. structured, semi-structured, and unstructured (Gray, 2014; M. Saunders, Lewis, & Thornhill, 2009). Out of these three categories, semi structured in-depth interviews are considered as the most useful and effective tool for the collection of qualitative data which normally have open ended questions, so the participants can express their experiences and behaviors in a more detailed and in-depth manner (Easterby-Smith & Thorpe, 2002). Semi structured interviews are considered as the best option for the exploration and understanding of human behaviors because they

allow the responders to express their thoughts in detail (Gray, 2014). Semi structured interviews provide an opportunity to understand the context in an exploratory manner to make the links between the social situations and attitudes of the social actors (M. Saunders et al., 2009). In a research study where some specific participants are involved, it is important that the participants agree for the semi structured interviews to provide the most relevant information about their experiences (Mark Saunders & Thornhill, 2016). A number of additional themes and relevant information can also be explored with the help of semi structured interviews (Wesely, 2011). The research question intended to be achieved with semi structured interview is "What is the most appropriate information security maturity model for the IT sector, banking sector and insurance companies? What are the maturity models that can be used to treat the finding of the risk assessment process?".

All data collected in this research have been analyzed using the SPSS and Minitab for quantitative data and thematic content analysis for the qualitative data stage with the help of NVivo software. The analysis of the data includes the examination, organization, categorization, and interpretation of the data with the support of qualitative and quantitative evidence to reach out for the analytical findings (Yin, 2014).

5.5 Research Contribution

The current research offers three important contributions for the existing literature such as: 1) maintaining a counter balance and create a semi-automatic framework that would provide facilitation in the risk assessment for the organization by identification of the weaknesses that need to be improved to bring betterment in the internal processes. This implies that, the framework which will evolve through the conduction of the current study will provide recommendation and suggestion in respect of the educational perspective and identification of the steps that may be taken to bring more work in the field. The second (2) contribution that this research will provide is the identification and similarities between the selected four information security models i.e. ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model, ISO 27001. This will also ensure that the developed model from the current research don't repeat any administrative or unnecessary processes. Lastly, the third (3) contribution is that the current research will help in building a model based on the scoreboard combined by ISO 27001 Control Objectives and Common Vulnerability Scoring System in order to offer a

unique solution on measuring information security maturity level and which is validated for functionalization and operations by the most important applications

5.6 Ethical Considerations

The ideology of the behaviors that provide the roadmap for the interaction, and behaviors of the people in forming the relations is known as “Ethical Approval”. Factors of honesty and integrity are the most fundamental elements for performing any research activity. Due to this reason, a line needs to be drawn as a stopping point to safeguard the rights of both parties (Gray, 2014). Gratton and Jones (2010) proposed that the measures for good ethical principles should be methodical and regardless of the research design and other elements of the research, ethical norms should be followed strictly. (Gratton & Jones, 2010). For the purpose of research, Cooper and Schindler (2006) argued that the purpose of research should be clear with respect to the collection of the data and the analysis of data. For the current study, the researcher ensures that all the aspects in relation to the confidentiality and personal space of the participants will be dealt with care. Furthermore, the researcher proposes to abide by the following ethical considerations as established by Gray (2014)

- Societal benchmarks will be dealt with care and the researcher will behave in a responsible manner
- Participants will not be forced to take part in any activity of the research and they will be free to disengage from the research at any time.
- Participants of the research will be free to raise any queries and the researcher will ensure that enough and a satisfactory answer is provided to the participants.
- The ethical code of conduct will be duly cared for.

6. Need Identification - Survey about the current level of security in enterprises

I investigated the current level of security in three sectors: ICT Industry, banking sector and insurance companies. I chose the above-mentioned sectors because of the importance of the data that they possess and handle during their work. Besides this, I must take into consideration the ICT sector deals with data from the source code of their applications and the importance of their storage is huge, while the banking and insurance companies mainly deal with personal and financial data which are considered to be very important. This chapter details and discusses my answer for the research sub-question 1. The

questionnaire was created in the format that I can gather reasonable answers from all stakeholders ranging from the managerial level to the experts or professional staff. In order to achieve a general balance of responses, I have received 76 replies from respondents while it is distributed to 98 companies that I involved with 78% of the target audience, however the inclusion and stakeholder character makes convincing responses. According to the sectors, I have managed to get 100% of the banking and insurance companies' responses, while 85% in the ICT sector is the largest volume of companies.

The questionnaire was developed in the period September 2018 - February 2019, while the respondents are listed 5 certification systems, while only a few of them are applied in Kosovo, while there are about 50 different security application procedures listed.

Looking at the results presented by the three sectors analyzed during my research, I see that we are dealing with a significant difference between ICT companies and other sectors such as the banking sector and insurance companies. This implies that the banking sector is well organized in terms of enforcing security standards for data protection by applying all the parameters from the procedural ones such as password change processes, general change procedures in IT to technical issues such as server upgrades or switching and migrating infrastructure. In general, the banking sector is more structured and with policies that are appropriate to the standards applied, while the ICT sector is noted to have a huge gap in the aspect of standards compliance. This implies that ICT companies are constantly investing in hardware equipment and security applications that attempt to create defense mechanisms, but security which is not based on a standard is a threat to the organization as it lacks basic treatment procedures for the particular problem you may face. It is a major challenge for organizations in the ICT sector, where the position of information security officers covers the position of IT in general, and it provides a possibility for manipulation by malicious people.

Table 4 Organizations that implemented an IT Governance Framework such as ITIL or ISO 27001

	No	Yes	All
Banking Sector	5	15	20
Insurance Company	6	9	15
IT Company	30	7	37
All	41	31	72

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	18.872	2	0.000
Likelihood Ratio	19.843	2	0.000

From the result of analysis above, the chi-square (χ^2 (2) =18.872, p<5%), this corresponds to the rejection of the above stated null hypothesis, I can however conclude from the above that there is a significant association between the companies' sectors and organizations that implemented IT Governance frameworks such as ITIL or ISO 27001. To buttress this assertion, of the 72 respondents, 15 of the 31 who affirmed yes are from the banking sector, of those who responded no, 30 of 41 are from the IT company.

The insurance *companies'* sector is relatively well organized, but here I see some gaps, especially in the part of the regular check or scanning of the system from possible vulnerabilities. In one form, lack of regular controls poses challenges to computer systems, given that most of the attacks on data systems occur precisely because of carelessness in updating computer systems. These results also relate to part of Table 4 (Using of IPS/IDS Systems in your organization) in which about 40% of insurance companies do not use detection systems and prevent eventual attacks. Here I can understand that such organizations can potentially have an outdated infrastructure that does not support advanced algorithms for detecting attacks or the other factor may be the financial implication of upgrading the existing technology. For the Banking sector, among the 20 persons, only 1 person said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are not used by their Organization, 12 said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are used by their Organization, while 7 said they don't know.

For the IT company, among the 37 persons, 16 persons said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are not used by their Organization, 11 said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are used by their Organization, while 10 said they don't know while for the Insurance Company, among the 15 persons, 6 persons said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are not used by their Organization, 9 said Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are used by their Organization, while no one said they don't know. These results are also linked to the lack of staff

training in terms of increasing awareness of data security, whereby some 30% of the insurance companies did not train the staff in terms of information security and lack of such information; or even tracking trends in technological change may result in poor infrastructure or potential vulnerabilities.

Table 5 Using of IPS/IDS Systems in your organization

	Don't know	No	Yes	All
Banking Sector	7	1	12	20
Insurance Company	0	6	9	15
IT Company	10	16	11	37
All	17	23	32	72

Cell Contents
Count

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	14.860	4	0.005
Likelihood Ratio	20.652	4	0.000

From the result of analysis above, the chi-square (χ^2 (4) =14.860, p<5%), this corresponds to the rejection of the above stated null hypothesis, I can however conclude from the above that there is a significant association between the companies' sectors and organizations using of IPS/IDS systems in their organization. The majority of the organization using IPS/IDS in their organization are banking, while 16 of the 23 IT companies are non-compliant. The IT companies constitute the majority of those that do not use IPS.

A gap I have observed during the research is that there are organizations that have implemented international security standards such as ISO 27001, COBIT or ITIL, but in practice they have been hampered by the implementation of the procedures or the compatibility of the framework. This *gap* is especially notable for ICT companies. For the Banking sector, among the 20 persons, 5 persons said the organization had not implemented an IT Governance framework such as ITIL or ISO 27001, while 15 said the organization implemented an IT Governance framework such as ITIL or ISO 27001.

For the IT company, among the 37 persons, 30 persons said the organization had not implemented an IT Governance framework such as ITIL or ISO 27001, while just 7 said the organization implemented an IT Governance framework such as ITIL or ISO 27001. For the Insurance Company, among the 15 persons, 6 persons said the organization had not implemented an IT Governance framework such as ITIL or ISO 27001, while 9 said the organization implemented an IT Governance framework such as ITIL or ISO 27001. In general, from table 1 I see that about 43.1% of the respondents agreed that an IT Governance framework such as ITIL or ISO 27001 is implemented in the organization while 56.9% indicated that the organization does not implement an IT Governance framework such as ITIL or ISO 27001.

Table 6 Organizations that have or not security measures in place for data protection

	No	Yes	All
Banking Sector	0	20	20
Insurance Company	7	8	15
IT Company	17	20	37
All	24	48	72

Table 6 shows that insurance companies and ICT companies are more exposed to risks and cyber-attacks in terms of implementing security measures. While companies that have security measures, and the procedures that they follow are such as smart card authentication, access based on needs "least privileged", access control lists and so on. While in the case of more customer data, access policies are regulated within the systems, which means that not all information can be displayed in all job positions. Some of the companies that have implemented advanced standards for data security management, primarily the banking sector, also use various software tools to monitor real-time data transactions. In addition to maintaining data security and continuous monitoring, some organizations have implemented encryption keys so that the client feels as secure as possible through their services. In *general*, there are a lot of gaps in the security companies that seem to have not yet understood the importance of the client's or their client's data protection and that's how I see that around 30% of them interviewed have different problems that you are exposed to certain risks. However, most organizations have restricted access to sensitive data spaces such as those physical spaces that they have

restricted by using lockers, fingerprints, smart cards, face recognition etc. to those *applicative* approaches such as domain controller implementation, access control, two-factor authentication, Firewalls, AES Encryption etc. About 66.7% of the respondents indicated that the organization has security measures in place for data protection while 33.3% of the respondents indicated that the organization does not have security measures in place for data protection.

Table 7 Has the organization verified the back-up and recovery process based on sector

	No	Yes	All
Banking Sector	1	19	20
Insurance Company	6	9	15
IT Company	9	28	37
All	16	56	72

Cell Contents

Count

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	6.270	2	0.044
Likelihood Ratio	7.092	2	0.029

From the result of analysis above, the chi-square (χ^2 (4) =6.27, p<5%), this corresponds to the rejection of the above stated null hypothesis, I can however conclude from the above that there is a significant association between the companies' sectors and organizations who provides answers whether on whether they have verified back-up and recovery process based on sector. 19 of 20 responses from banking sectors can answer the question of whether their organization has verified backup and recovery processes, while the majority (6 out of 9) of those in the insurance company cannot answer the question whether their organization has verified backup and recovery process.

In my research, I have also compared the implemented security systems and identified a gap between organizations that performs system back-up and over 90% of the responses that back-up is performed on a regular basis, but only 22% of organizations verify if the

back-up process was successful. Verifying the backup copy in one of the basic steps of the process and procedures to perform a successful backup. The backup of important information is often the last line of defense in case of an accident or malicious loss or modification of organization information, applications and infrastructure configurations. The purpose of this standard is to set out the baseline requirements for the backup of organizations' information systems and data. Organization information must be backed up on a regular basis, protected from unauthorized access or modification during storage, and available for recovery in a timely manner. As backup media may contain sensitive information in high-volumes (i.e., financial transactions, personal identifiable information etc.), the backup media must be protected during the entire information lifecycle.

Table 8 Organizations that possess a Disaster Recovery Plan or Business Recovery Plan

	No	We have business continuity plan	We have disaster recovery plan	We have disaster recovery plan;	All
Banking Sector	0	4	4	12	20
Insurance Company	0	1	8	6	15
IT Company	7	8	9	13	37
All	7	13	21	31	72

Cell Contents

Count

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	13.784	6	0.032
Likelihood Ratio	16.196	6	0.013

From the result of analysis above, the chi-square (χ^2 (6) =13.784, p<5%) corresponds to the rejection of the above stated null hypothesis, but however I can conclude from the

above that there is a significant association between the companies' sectors and organizations that possess a disaster recovery plan or business recovery plan. Comparatively, the banking and insurance sector seems to have a better recovery plan compared to them from IT companies, whose 7 respondents opined not to have a disaster recovery plan or business recovery plan.

During my research with organizations I have compared organizations that possess a disaster plan and organizations that have a business continuity plan. The results show that the most vulnerable sector in the absence of these plans is the ICT sector who considers that implementing a disaster recovery plan or a business continuity plan is very costly. However, during the discussion with this sector of organizations, I have noticed that a part of the vast majority of the services they use are on cloud platforms that indirectly have a disaster recovery model which is covered by the organizations that offer cloud services. It is interesting that in the banking sector and those of insurance companies consider more seriously the disaster recovery plan compared to the business continuity plan. Only about 43.1% of the interviewers indicated that they have both disaster plan and business continuity plan for data processing facilities, 29.2% disaster recovery plan only, 18.1% business continuity plan only while 9.7% of the respondent indicated that they don't have any of the plans for data processing facilities.

Table 9 Organizations that outsource its data storage (Cloud Platforms)

	No	Yes	All
Banking Sector	14	6	20
Insurance Company	8	7	15
IT Company	7	30	37
All	29	43	72

This is also related to Table 9, from which I see that a considerable number of organizations, mainly in the insurance companies' sector and the banking sector, use outsourced services to store their data. The limit of this research is because I do not know what information can be stored on cloud platforms and endanger the overall data

protection system because, given the important personal information that these organizations have in their possession, this can affect also directly on their trustiness and credibility of the clients. This conclusion is based also on the general calculation where about 59.7% of the respondents indicated that the organizations outsource its data storage (Cloud Platforms) while 40.3% of the respondent indicated that the organization does not outsource its data storage (Cloud Platforms).

Table 10 Organizations that faced an information security breach in the past two to four years

	No	Yes	All
Banking Sector	13	7	20
Insurance Company	15	0	15
IT Company	28	9	37
All	56	16	72

Cell Contents
Count

Chi-Square Test

	Chi-Square	DF	P-Value
Pearson	6.270	2	0.044
Likelihood Ratio	9.325	2	0.009

From the result of analysis above, the chi-square (χ^2 (2) =6.270, p<5%) corresponds to the rejection of the above stated null hypothesis, but however I can conclude from the above that there is a significant association between the companies' sectors and organizations that faced an information security breach in the past two to four years. 56 of the 72 respondents opined that their organizations faced an information security breach in the past two to four years, while 16 respondents opined that their organizations faced. There are 16 organizations that faced an information security breach in the past two to four years, 7 are from the banking sector while 9 are IT companies.

Statistics show that the most targeted organizations by hackers are banking institutions and IT companies. One result of this is understandable also by following of the global trends of the attacks, where the financial aspect and financial institutions are mainly targeted, as far as the attacks on ICT companies are concerned more with industrial espionage or attacks that have no financial aspect, but the flow of information for existing projects, the acquisition of prototypes developed and the illegal acquisition of information

related to the development of new products. About 22.2% of the respondents indicated that the organization had experienced an information security breach in the past two to four years while 77.8% of the respondents indicated that they had not experienced an information security breach in the past two to four years.

My research study focuses on identifying the level of security of information within organizations, the implementation of standards and the challenges of their implementation. One particular focus of this research is the identification of gaps that exist within the interconnection of security policies with their technical implementation and the results show that there is a gap between these two elements.

Following this chapter, I will present graphically and narratively the preliminary findings that I have encountered during my research and provide the answer to my research sub-question 3.

According to my research and interviews with organizations, about only 37.5% are IT Security Officers and only 15.3% are Chief Information Security Officers, the rest of the respondents are System Administrators or IT Technicians as it is shown on the following figure 1 Survey respondents.

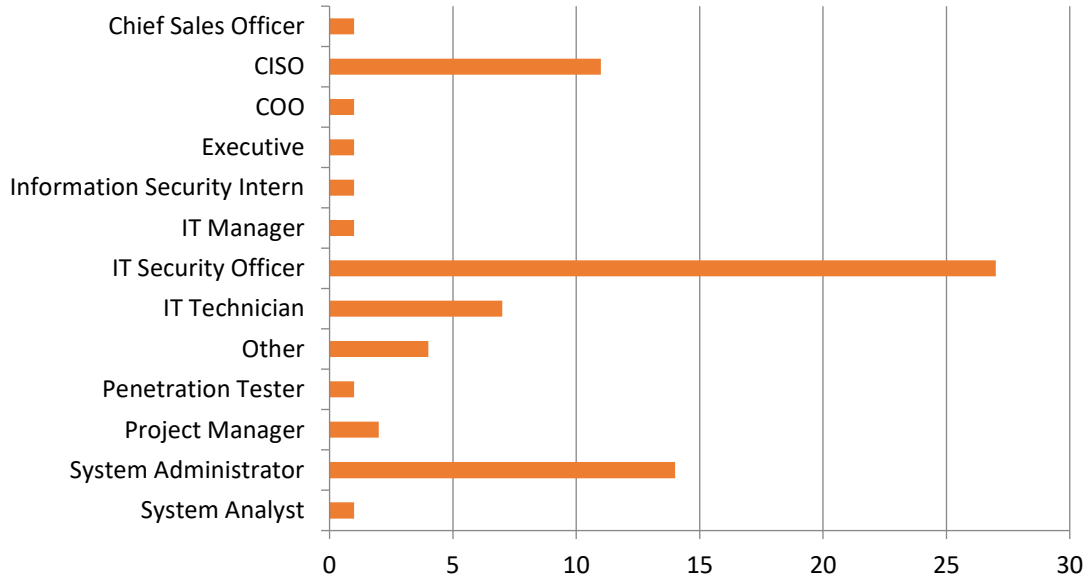


Figure 6 Survey respondents

According to Fig.5 Insurance Companies are most secured, or at least they didn't experience any information security breach on in the past two to four years. Big issues, is the banking sector, because we have around 53% of the banks, have been attacked in the

past, while in the IT industry we have a percentage of breaches around 32%. Therefore, the need to manage this risk with the aim of minimizing or even preventing such risks is a continuous and extremely important process for any organization or institution. Consequently, the fundamental role of information security is to support the mission of the company or organization. In the wake of the challenges that each organization's management faces in the field of technology and information, the role of IT professionals is to understand these ambiguities and challenges, manage them and clarify it before management.

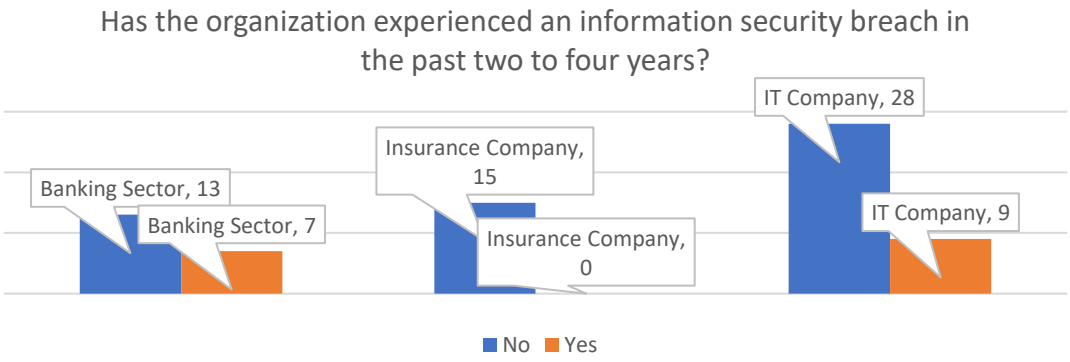


Figure 7 Has the organization experienced an information security breach in the past two to four years?

Usually companies or organizations have limited resources to guarantee the security of information. My research shows that 57% of the interviewed organizations, do not have implemented any IT government framework, or information security standards. They argue, the lack of implementation with a lot of procedures and time-consuming period, in which you have to deal with a lot of documents and paperwork while in the end, the standards mostly help you to define the security on papers rather than on the technical aspect. Organizations do consider that, if there is any semi-automated tool through which organizations can full fill any questionnaire with the more appropriate answers, and then the system would generate them some information on the weakest points of their system which may help them to intervene on specific parts of the system. Organizations are very much interested that beside the documentation those are interested also in technical protection of the system. In my survey I found that 57% of organizations don't have implemented any IT Governance framework such as ITIL or ISO 27001. As shown in Figure 2 below, it is noticed that the banking and insurance companies have implemented

and certified their services based on a specific information security standard, while most IT companies are not certified by information security standards.

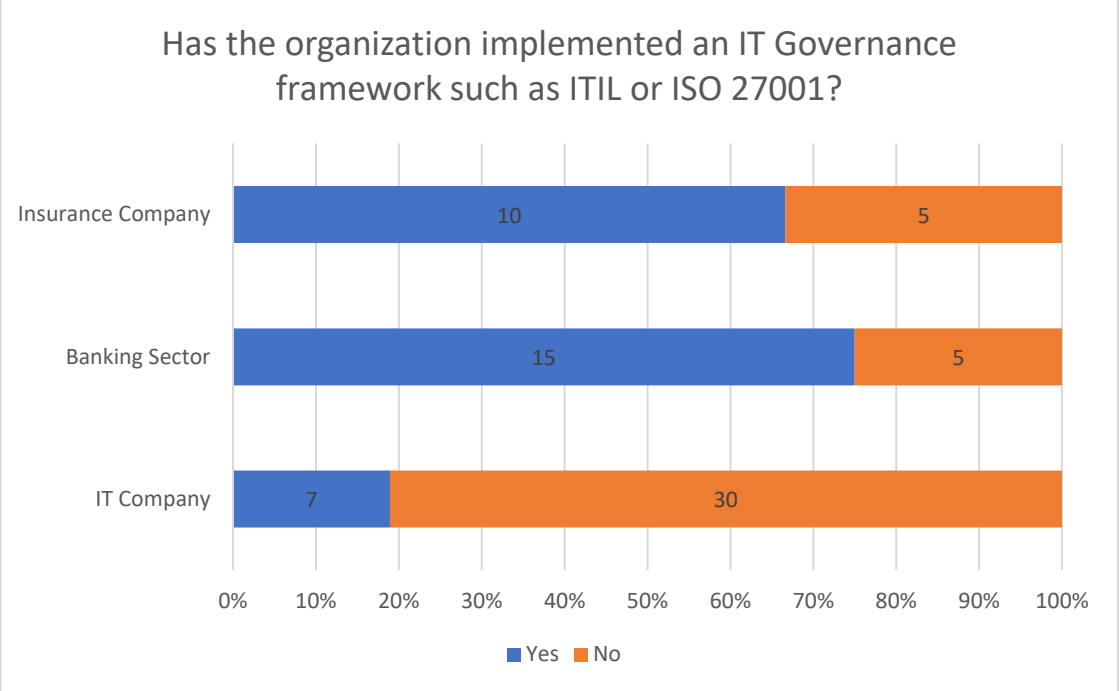


Figure 8 Answers to the question "Has the organization implemented an IT Governance framework such as ITIL or ISO 27001?"

According to the analysis there are organizations that have implemented Information Security Standards, but at the same time they are still technically unprotected, they operate without any firewall or antivirus system installed on the infrastructure. There are organizations that deal with sensitive data such as client's data, and at the same time they do not encrypt their backups or there is not any disaster recovery plan implemented. These gaps must be treated very seriously in the field of information security, because security does not mean only protecting the system on the papers but in practice as well.

In information security management, the role of the human factor, as well as the organization's employees, is also relevant, which may be the cause of changes in terms of protection of data. Workers within organizations can operate in two different forms, respectively they may have a negative role by involving them with or without awareness in breaking the security rules, namely sharing information with unauthorized persons. On the other hand, providing training and raising the awareness of the staff about the importance of security policies, as well as reporting on the consequences that each may

have on the security rules, can have a positive role in information security (Soomro et al., 2016; Vance, Lowry, & Eggett, 2013).

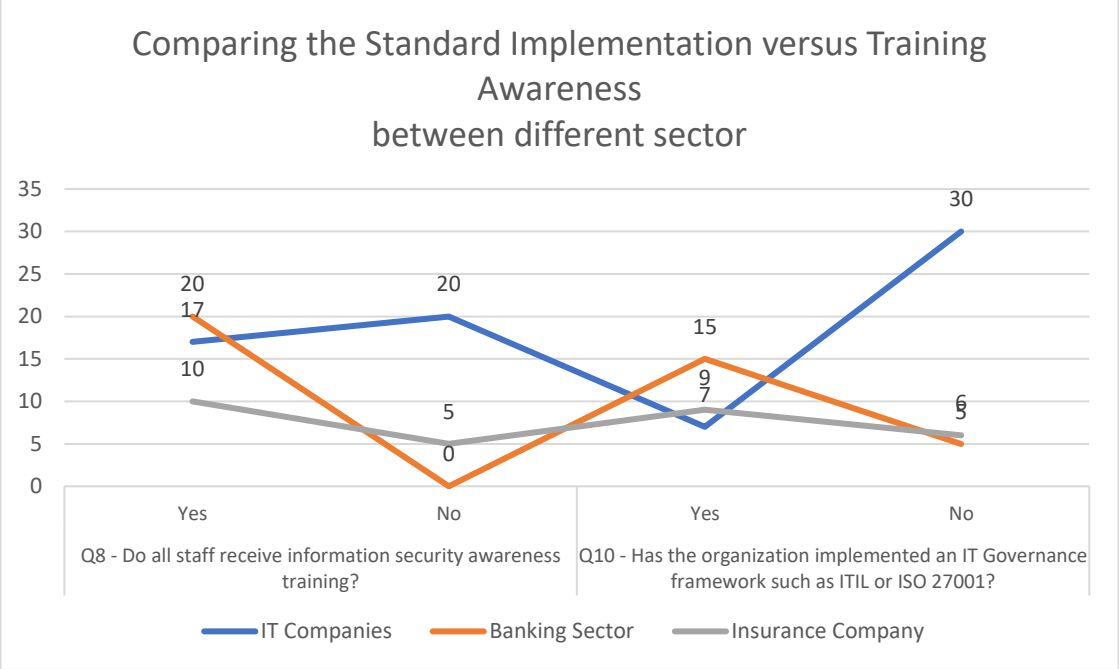


Figure 9 - Standard Implementation vs Training Awareness between sectors

My research shows a gap between sectors, when I talk about the organizations that have implemented an information security standard and organizations that organize training about security awareness. Specifically, there is a big gap between the banking sector and IT companies. According to this I see that the banking sector and insurance companies are more responsible and more aware of the information security while IT companies, do not invest a lot either on standard implementation or information security training awareness. This gap is shown as well in Figure 5 - Standard Implementation Vs Training Awareness between sectors.

The ultimate protection of the last few decades has become one of the most valuable assets of the organization, putting the number one priority on many of them. When I asked organizations if they have any formal change control process for IT changes, 75% of the organizations provided a positive answer while the other 25% confirmed that they do not have any formal process. Comparing the answers given to question “Has the organization implemented an IT Governance framework such as ITIL or ISO 27001” with the answers to the question “Does the organization have a formal change control process for IT changes”, I see and understand that organizations often practice different standards in managing IT services but formally fail to certify any of the standards required , and during

my direct meetings some of the reasons that organizations point out are the high cost of implementation and at the same time the standards sometimes exceed the needs that they have to emphasize the need for a standard that is more polluted and oriented to less formal documents.

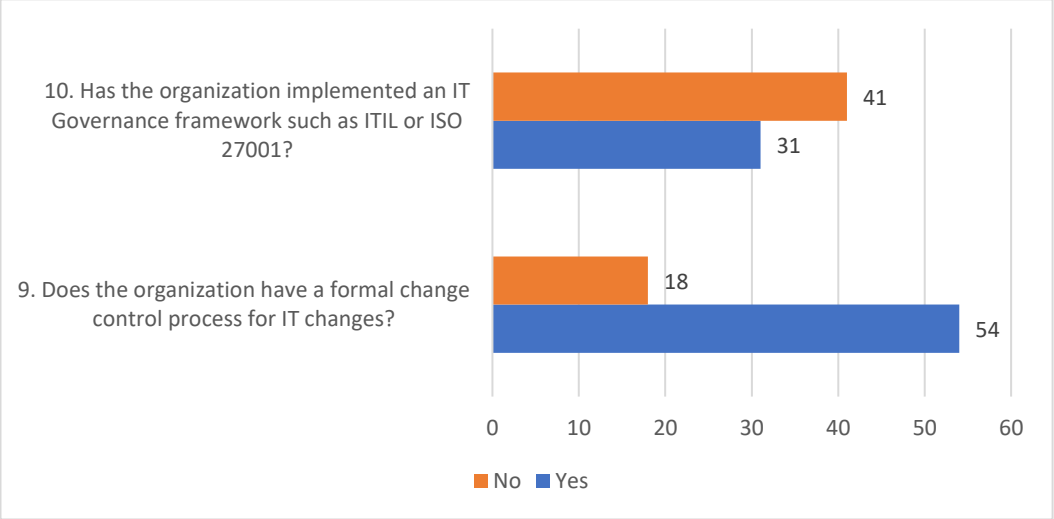


Figure 10 Comparing two questions results

For this reason, (Susanto et al., 2011) elaborates on the need for a set of mechanisms or benchmarking standards that will ensure the adoption of best practices and achieving a level of security.

Based on the assessment and criteria presented by (Montesino & Fenz, 2011b), I will present the framework prototype I created for risk assessment based on ISO 27001 respectively the list of security controls by article. In my research and the interviews with organizations, I have divided the questions into several sections such as by controls: General Security Controls, Networks Security Controls, System Security Controls, Business Continuity, Disaster Recovery and Incident Response. In the following Figure 7 – Comparing the Implementation of Network Security Controls by sector, I have identified the most implemented controls. According to the results I can see that, almost every organization has implemented an Intrusion Detection System and Intrusion Prevention System, followed by the regular network vulnerability scans. Even that organizations do regular network vulnerability scans, most of the organizations do not possess any timing procedure, but usually they act based on IPS/IDS alarms. Regarding the remote access via VPN or BYOD (Bring Your Own Device) I see that organizations have strict procedures, on who can have remote access and when it is allowed. Also, it is

important to mention that most of the organizations have deployed the Bring Your Own Device Policy which specifies to mobile devices such as laptops, Tablets and other smart devices the polices of access to the internal company network (Al-rashdi, Dick, & Storey, 2017). Regarding the Wireless Access most of the organizations have implemented the procedures based on ISMS policies, where they have separated the internal wireless access from the guest access but as well it has been divided also to the technical part through implementation of the Access Control Lists (Alqahtani, 2017). Overall, I can see the maturity of the organizations in relation to network security controls. My research presents several gaps as well that I found in this regard, but those gaps are solvable and may not risk the entire information security system. It is very important for organizations to establish a strong link between information security standards and security controls which then must fit the organization's needs.

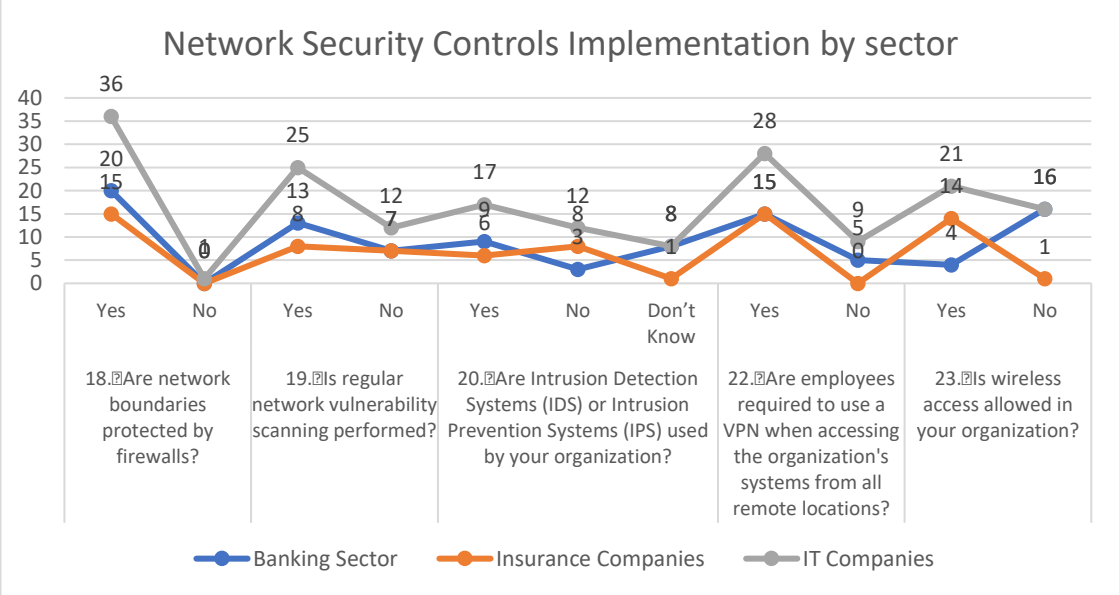
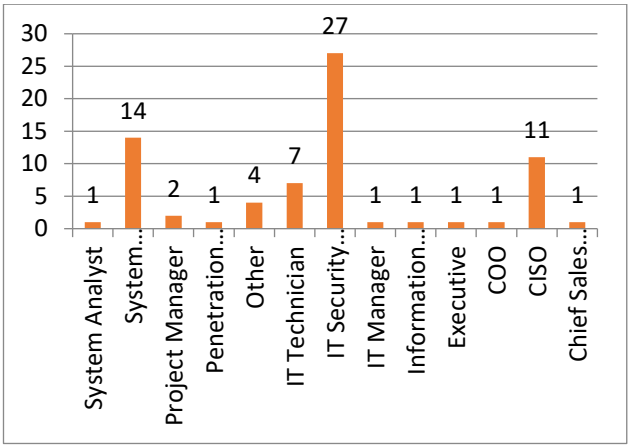


Figure 11 - Comparing the Implementation of Network Security Controls by sectors

It is very important for the organization to perform a risk assessment in their information security system. But to realize it, it is very important for an expert to make the assessment, given that his suggestions may be important and play a major role in the company while defining the development of the information security system. However, the question is that not all companies possess such a person, or not all companies can afford the costs of such a person or organization. According to my research ad interviews with companies only 52.8% of responding organizations pose an Information Security officer or Chief Information Security Officer.



		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	System analyst	1	1.4	1.4	1.4
	System Administrator	14	19.4	19.4	20.8
	Project Manager	2	2.8	2.8	23.6
	Penetration Tester	1	1.4	1.4	25.0
	Other	4	5.6	5.6	30.6
	IT Technician	7	9.7	9.7	40.3
	IT Security Officer	27	37.5	37.5	77.8
	IT Manager	1	1.4	1.4	79.2
	Information Security Intern	1	1.4	1.4	80.6
	Executive	1	1.4	1.4	81.9
	COO	1	1.4	1.4	83.3
	CISO	11	15.3	15.3	98.6
	Chief Sales Officer	1	1.4	1.4	100.0
	Total	72	100.0	100.0	

Figure 12 Number of Information Security Officers at organizations

As a result, a solution is for companies to build an expert system that can help you in determining the level of information security in the system through risk assessment. The use of such systems in risk assessment would help to ease and consistency during the decision-making process (Disterer, 2013; International Organization for Standardization, 2014a). A good system can solve many problems as well as facilitate decision-making but need to have large amounts of data for analysis. To build a risk assessment system, we need to have the knowledge in the field that we want to develop the system's detailed field analysis as well as the opinion of end-users that will use it (Joseph C. Giarratano, 2004). To build a good system, we must first set the general principles for system building by defining the method I will use for implementation. There are 4 methods for system building and those are: forward chaining, backward chaining fuzzy and certainty methods. Given that my system should provide a suggestion, alternative or a response to the questions that are submitted during the completion of the application, the method that suits my system's earnings is the forward chaining method. This method is also known as

the method that is largely implemented in the IT Security Risk Assessment (Seebauer, 2011; Sihwi, Andriyanto, & Anggrainingsih, 2016).

According to the SANS Institute, a good policy is a formalized, short, and high-level statement or plan that incorporates an organization's approaches, goals, objectives and procedures to a specific area. Policies require compliance and disrespect of a policy will result in disciplinary action. In addition to the technical controls, organizations should also implement security policies as a form of administrative control. In fact, these policies should indeed be a starting point in developing an overall security plan. A good information security policy instructs employees to use the company's information resources and provides the company with security if an employee violates a policy. But, in my research it shows that not every sector pays attention to the information security standard implementation besides information security policies. A good example is the IT Companies, who are not very interested in implemented ISMS such as ISO 27001 or any other, but they do have implemented properly written policies related to information security. During my discussions with companies, I understood that the reason why they do not implement any standard is the cost of implementation, time consuming and sometimes those standards are very generic without a customized solution for a specific industry. This is one of the reasons why they do implement only specific security policies that may affect their work. In the following Figure 8, I am showing the comparison of Information Security Standard Implementation and Written Policies between different sectors such as the Banking Sector, Insurance Companies and IT Industry. In my stacked line analysis, it can be seen that there is not a huge gap between the banking sector and insurance companies but there is a big discrepancy between the IT Industry and the other two sectors. This is explained by the fact that banking sector and insurance companies deal more with the private and sensitive data, so their awareness must be higher than others while IT Industry is more focused on the technical aspect of security such as implementing more security hardware equipment, software applications that deals with cybersecurity rather than taking care about the standards and policies.

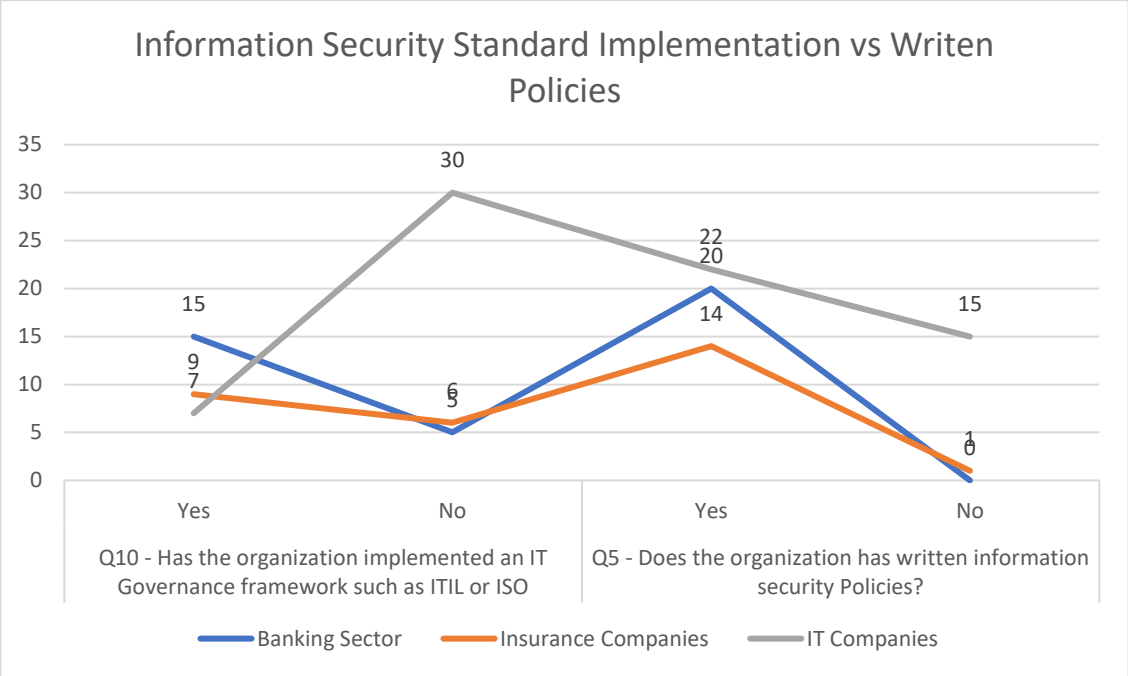


Figure 13 - Standard Implementation versus Written Policies

Comparing three sectors, I found also that not all organizations pose a dedicated staff for information security. Only 20 IT Companies out of 37 interviewed has a dedicated staff member who deals with information security. The Banking Sector and Insurance companies stay better on this issue. However, in all the interviewed organizations I have noticed an uncertainty in relation to the person responsible for security. Not all organizations have a CISO position - Chief Information Security Officer or Chief Information Officer or something. Some organizations cover the position of the Responsibility for Information Security by the IT Department, respectively system administrator, IT technician and others. This issue raises many questions as to whether a person is adequate and whether he is familiar with certain action procedures in case of any technical or procedural problem but according to (Haqaf & Koyuncu, 2018) an information security manager must be familiar not only with the information security issues but also with the network security, application security, malware analysis etc.

Organizations often encounter confusion between IT Policy and Information Security Policy. Information security is more than just IT. Of course, the IT-specific content usually takes the largest amount. However, there is more to it. You want to protect your entire corporate value. It's not just about transmitting, editing or storage being digitally secured. My framework would enable, besides identifying the weaknesses and dangers it

may have, also provide a general assessment of the position of the individual who is responsible for the security and information.

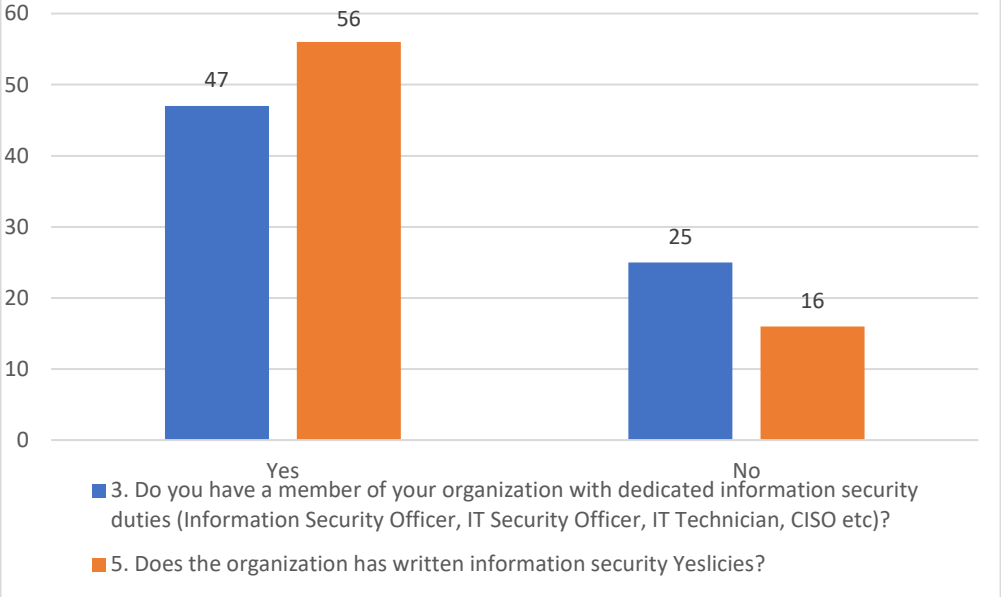


Figure 14 - Comparing organizations that have IS policies and organization that have dedicated staff for information security

The policy does not specify specific technical details but focuses on the desired results. A security policy should be based on the guiding principles of confidentiality, integrity and availability. A good example of a security policy is the policy of using the Internet. Internet usage policy defines the responsibilities of company employees as they use the company's resources to access the Internet.

7. Risk Assessment Maturity Framework Prototype

The proposed Risk Assessment Maturity framework is based on the result of the gap analysis of the current frameworks such as Fair, OCTAVE and CRAMM (detailed in chapter 4). This chapter details and discusses my answer to the main research question.

The unique feature of the proposed framework is, that it combines ISO 27001 controls and control objectives with the Common Vulnerability Scoring System. In the framework development, I analyzed each of the control objectives and compared them to the relevant CVSS Scoring Model.

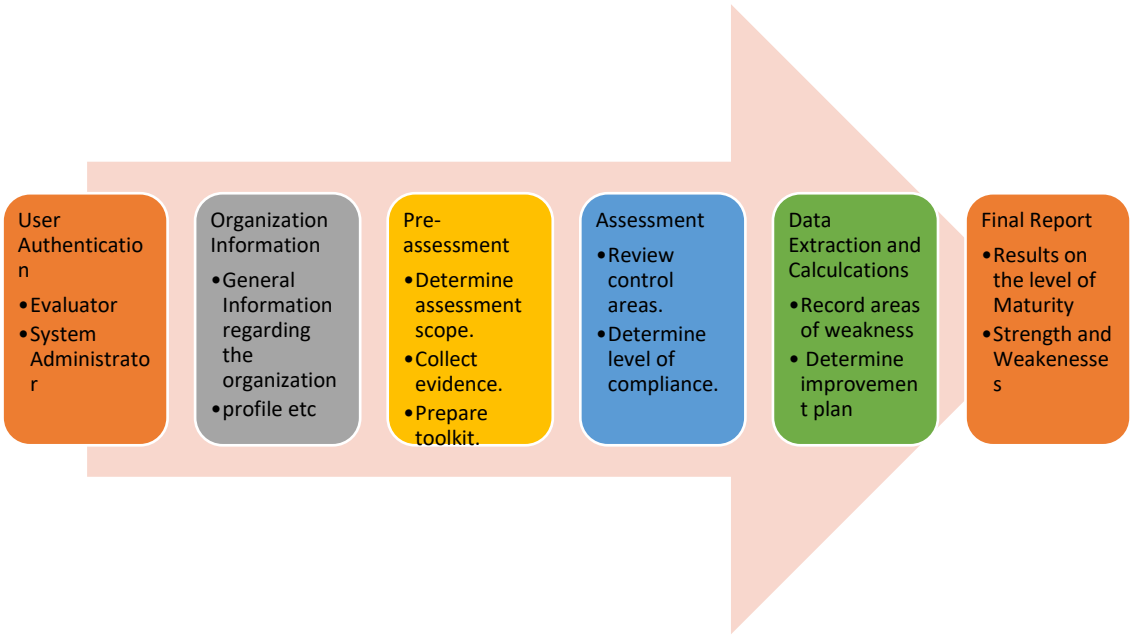


Figure 15 - Risk Assessment Framework - Functional Design

With the help of quantitative and qualitative data analysis and through the identification of gaps in the literature, a software application was developed which will apply a semi-automated information security risk assessment method after the compilation of recommendations from analytical findings. The development of the software application prototype is the achievement of the main research question which states, "How can we develop the semi-automatic risk assessment system? How risk assessment systems can be extended to provide a list of recommendations by identifying the list of areas with a lack of suitable security measures through an automated risk or semi-automated assessment solution? The system prototype is developed on the basis of the literary findings, comparison of maturity models, and analytical findings from the quantitative and qualitative data collected from sample participants from companies of IT, banking and insurance sectors. The proposed framework prototype is the result of comparisons made among the existing models in service sector practices as well as academic researches.

7.1 Conceptual Model

In this section of Chapter 7 I will detail my answer for sub-question 2. The framework prototype is a web-based application developed on PHP programming language and the database is based on MySQL. The web-based application is optimized for use on every device ranging from personal computers to smartphones with the technology of auto responsive content. This means that depending upon the resolution and the screen of the device, the software is automatically optimized. The framework prototype is user friendly

and easy to navigate but the issue of less memory and internet consumption has been solved by implementing the backend-oriented layout using the HTML5 and CSS3 mostly for design and very few images. On completion of the questions from the companies and organization, this system has the opportunity to export the report generated with the recommendations. The prototype is tested and validated based on the developed test scenarios. The framework prototype also had a period as a beta version during which any possible bugs or improvements have been identified.

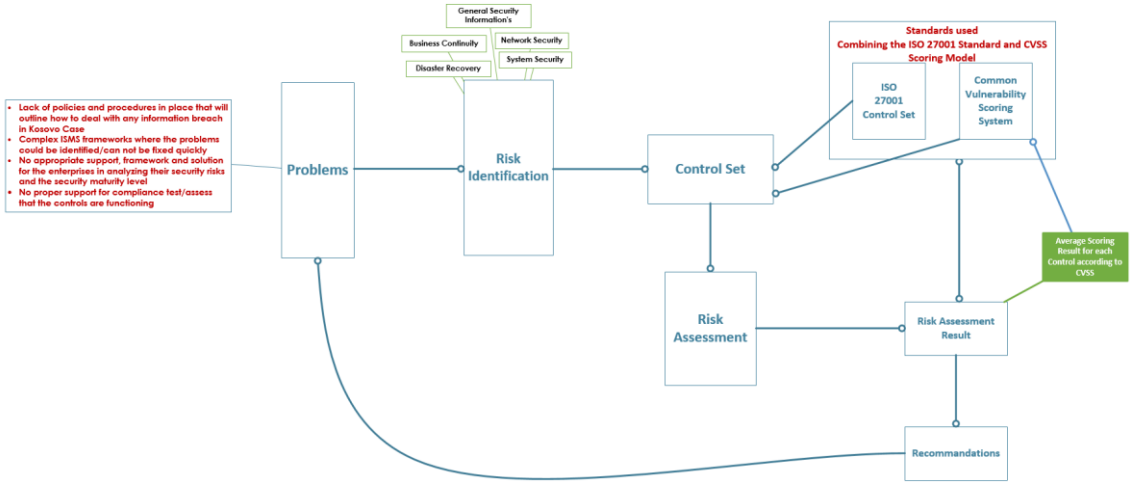


Figure 16 - Conceptual Model

7.2 Framework Architecture

The current proposal forwards a framework that is more user-friendly easy to be used and adaptable to develop any risk assessment questionnaire. The application is made up of several blocks that represent the respective functions as well as are interconnected with other parts of the system. This is an incremental and iterative development that is implemented as a new concept and is in line with the idea of the on-the-job development (Cockburn, 2008; Tsai, Stobart, Parrington, & Thompson, 1997). Characteristics of the framework are defined on two levels. The overall level definition establishes the foundation and framework; it indicates particularities and critical issues that need special attention. The detailed level specification defines requirements with full particulars. These documents are prepared simultaneously for the present one. Specifically, the database design will seek to:

- Minimize data redundancy meaning information is not duplicated in several places making it hard to maintain

- Provide easy access to the data including the ability to handle ad-hoc queries
- Provide security for the data
- Allow constraints that ensure data integrity;

The framework database uses a relational model because of its wide acceptance and ease of use.

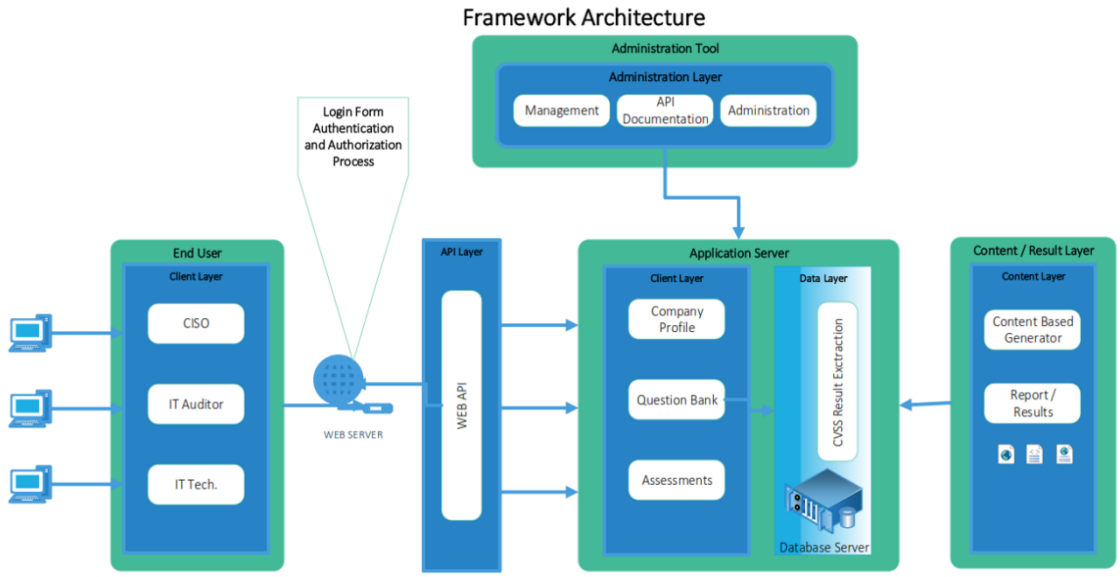


Figure 17 - Framework Architecture

The framework links information security control of ISO 27001 with CVSS metrics then using the scoring model provided by CVSS to evaluate it on a qualitative rating scale. I have analyzed all ISO 27001 Information Security Controls to see their relevance and what are their common points that may have the same scoring pattern. Their analysis is based on case studies and technical papers presented by various companies dealing with information security. Here I have realized that some of the Information Security can be merged in order to eliminate repeat queries and results. On the other hand, I have also analyzed all of the CVSS Metric and Scoring Model to see the purpose of each of them.

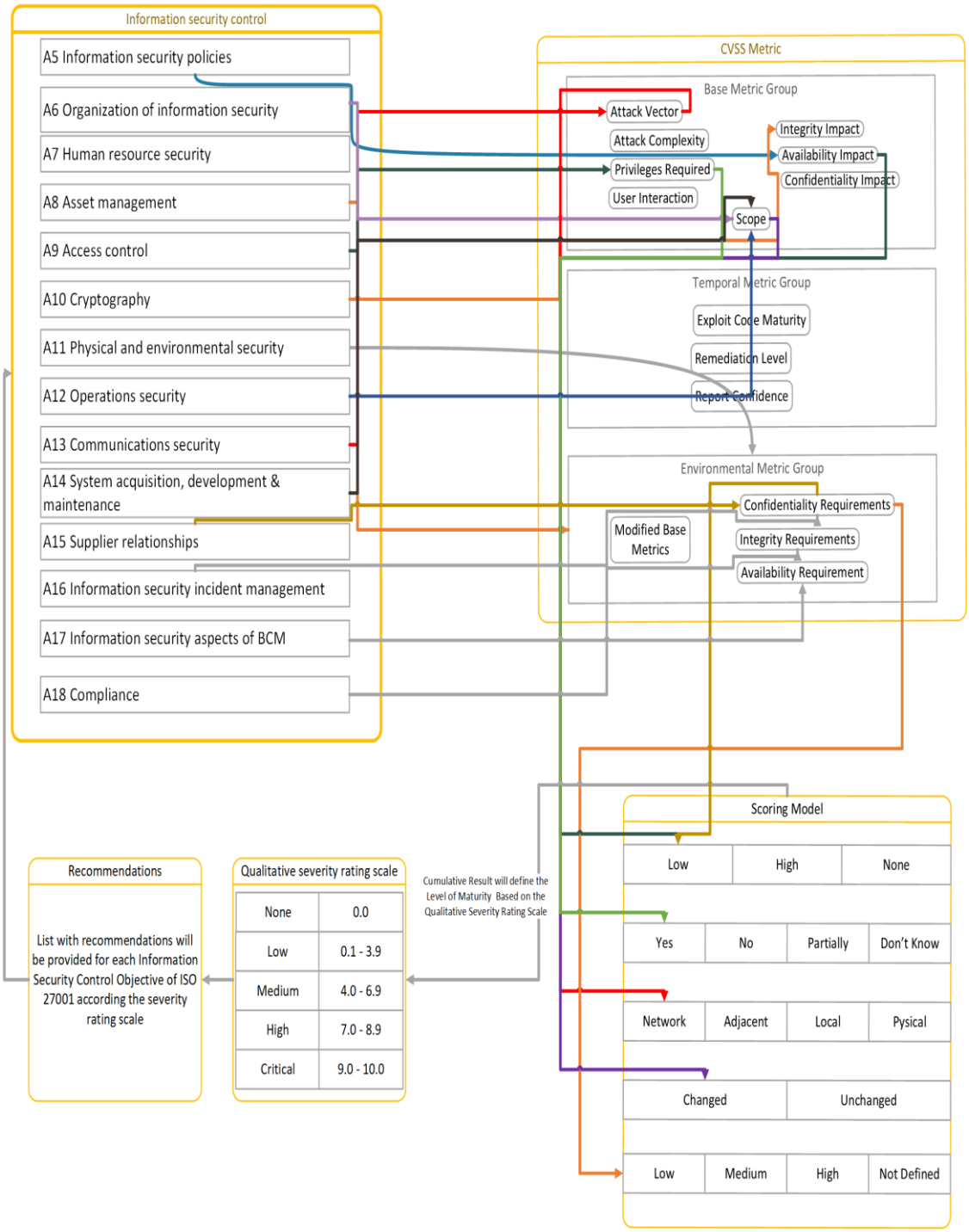


Figure 18 ISO 27001 Information Security controls and CVSS Metrics

In the following table (Table 10) I am presenting the mapping between ISO 27001 Information Security Controls and CVSS Metrics.

Table 11 - Mapping between ISO 27001 IS Controls and CVSS metrics

ISO 27001 – Information Security Controls	Explanation	CVSS Metric	Scoring Model
A.5 Information security policies	I mapped the A.5 Control to the Availability Impact metric from the Base Metric Group because the organizations that are assessed are supposed to have Information Security Policies in place, but measuring the level of implementation is important. This level can be measured from Low | High | None.	Base Metric Group / Availability Impact	Low | High | None
A.6 Organization of information security	Controls on how responsibilities are assigned also include controls on mobile devices and teleworking. In this regard I mapped the A.6 to the Scope metric of the Basic Metric Group with a scoring model on Low | High | None because the Scope metric captures whether a vulnerability impacts beyond its security.	Base Metric Group / Scope	Low | High | None
A.7 Human resource security	Checks before, during and after employment. I mapped the A.7 controls to the availability impact. This can be measured with 4 levels of the CVSS scoring system.	Base Metric Group / Availability Impact	Yes | No | Partially | Don't Know

	The organization can follow the procedures of employment, don't follow or there is also an option partially, which sometime defines only some of the main procedures that organizations take care of.		
A.8 Asset management	This control is mapped to the Environmental Metric and Integrity Requirement metric, because there are controls related to the asset's directory and acceptable use, as well as for information classification and media handling.	Environmental Metric Group / Integrity Requirement	Low | Medium | High | Not Defined
A.9 Access control	I mapped to the CVSS Privileges Required Metric with a three-level scoring. I chose Privileges Required metric because it included privileges and controls for the access control policy, user access management, system and application access control, and user responsibilities	Base Metric Group / Privileges Required	Low | High | None
A.10 Cryptography	This control is related to the integrity and authenticity of stored or transmitted sensitive or critical information. On my prototype framework it is mapped to the Integrity	Base Metric Group / Integrity Impact	Yes | No | Partially | Don't Know

	Impact metric which controls related to encryption and key management.		
A.11 Physical and environmental security	This control is mapped to the Environmental Metric Group with a modified base metric because this control defines security areas, access controls, protection against threats, device security, safe disposal, clear desk and clear screen policy.	Environmental Metric Group / Modified Base Metric	Yes | No | Partially
A.12 Operations security	At the operations security control a lot of controls are related to managing IT production such as: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities.	Base Metric Group / Scope	Low | High
A.13 Communications security	The A.13 controls related to network security, segregation, network services, information transfer, messaging. In this case, I mapped to the Attack Vector metric with three possible options.	Base Metric Group / Attack Vector	Low | Medium | High
A.14 System acquisition, development and maintenance	Since the control defines security requirements and security in development and support processes, I mapped it to the Modified Base Metric with three possible options.	Base Metric Group / Modified Base Metric	Low | Medium | High

A.15 Supplier relationships	I mapped to the Confidentiality Requirement controls what is to be included in agreements and how the suppliers are to be monitored.	Environmental Metric Group / Confidentiality Requirement	Low | Medium | High
A.16 Information security incident management	Incidents occur in every company. A.16 aims to ensure a consistent and effective approach to handling information security incidents, including notification of security events and vulnerabilities. Therefore, the first step is to define the responsibilities and procedures. Many companies already have a ticketing system. This can ideally be expanded with the information security incidents type. As we know that any incident can be categorized by Low, High, Medium and Critical, I mapped the A 1 to the Environmental Metric Group with the Scoring Model of Low | Medium | High	Environmental Metric Group / Confidentiality Requirement	Low | Medium | High
A.17 Information security aspects of business continuity management	The A.17 control requires the planning of business continuity, procedures, verification and	Environmental Metric Group / Availability Requirement	Yes | Partially | No

	review, as well as IT redundancy. For this reason, I mapped it to the Availability Requirements.		
A.18 Compliance	Confidentiality Requirement Metric is mapped to the A.18 control that requires identification of applicable laws and regulations, protection of intellectual property, protection of personal data and verification of information security	Environmental Metric Group / Confidentiality Requirement	Yes | Partially | No

The system is based on question-answers with the Likert scale options according to the CVSS model. The questions are strictly linked only to the corresponding controls and control objectives of ISO 27001. Since CVSS consists of three measurement groups such as Base Metric Group, Temporal Metric Group and Environmental Metric Group, and each has its own evaluation measures depending on the evaluation object, I have applied the most appropriate measures in each ISO 27001 Information Security Control. Using the framework, the company will get a security assessment report (recommendation part) describing its level of security on each IS control. The system automatically generates a report with presents the gaps and suggestions for improvements as a recommendation. The proposed framework model makes possible the implementation of information security risk assessment questionnaires, which are programmed for generating results automatically by doing specific mathematical calculations in the backend of the framework. The model distinguishes and stores all the changes or removed records and makes them accessible, e.g. assessment number or username logs. A high-level integration of graphical and textual data is provided by the model since it assigns an integrant data model segment to the graphical data. The results are easily readable or visually understandable.

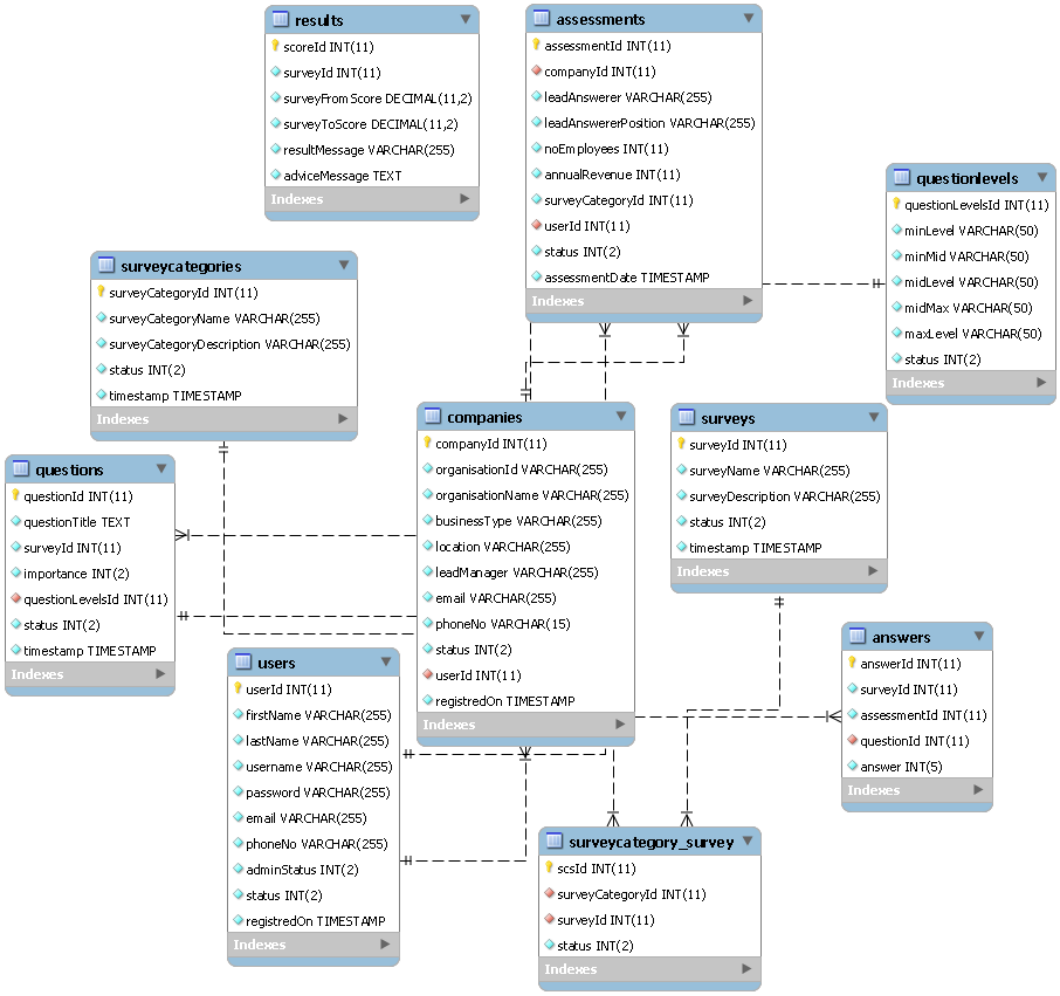


Figure 19 - ER Diagram

The framework database design is the process of producing a detailed data model for the database. This logical data model will contain all the requested logical and physical features and physical storage parameters needed to generate the framework database. The framework data model contains detailed attributes for each entity.

The database design has several abstraction levels, which are usually the steps of the database development. These levels are supported by different IT development tools and

management techniques. The following diagram indicates the adobe-mentioned described schema.

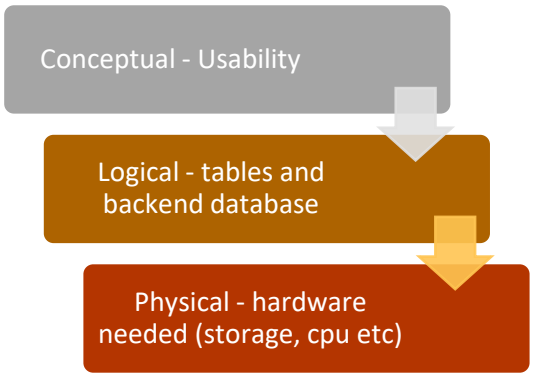


Figure 20 - Structural Layered Schema

The logical segmentation not necessarily impacts the physical representation of the model to databases. Due to certain technical, managerial and organizational constraints, and optimize requirements, the "managing data in one single database" approach cannot be implemented. However, the database design makes an effort to define databases with the same borders as the modules or sub-systems have (Lu, 2017).

In the dashboard of the system, statistics showing, the number of companies that have carried out the risk assessment, the number of questions, how many questionnaires have been conducted and how many questions have been answered are displayed. Further statistics are visualized on the dashboard, such as the most frequent answers, the most prevalent security issues from all questionnaires and so on.

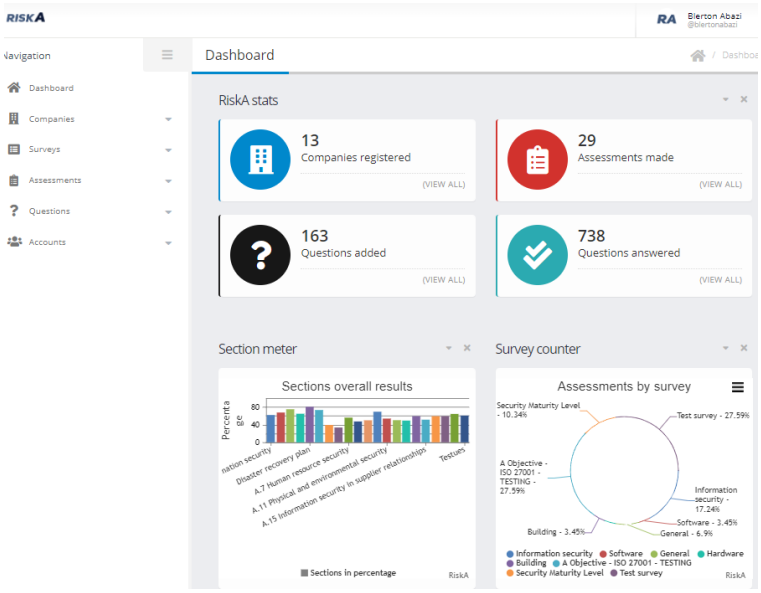


Figure 21 The system dashboard

The application also has a navigation menu on the left that helps us to overall manage the system.

In the navigation menu, six sections are outlined:

1. Dashboard - which presents visualizes general data and statistics
2. Companies – This section helps us to obtain general data for companies that are subject to the questionnaire. In this section, I developed two subsections, respectively the option to register a new company and the current list of the companies that are already on the system
3. Surveys – This is the main part of the application because through this section you manage with questionnaires. In this section, you can add new questions from the database, categorize questions, or even change the type of questions.
4. Assessment - In this section, you can see the list of assessments you have accomplished so far. Particularly in this section is that you can make a comparison between some assessments. For example, if Company X has conducted the Assessment in 2017 and 2018, then through the Compare Assessment option you can see the progress that the company has made in certain sections.
5. Questions – through this section, you can add new questions, modify the existing ones, or even change the form of the question.
6. Accounts - is the ultimate part that enables us to administer the system or create new users by setting the level of use. For the moment you have two types of users, respectively administrator and user simple.

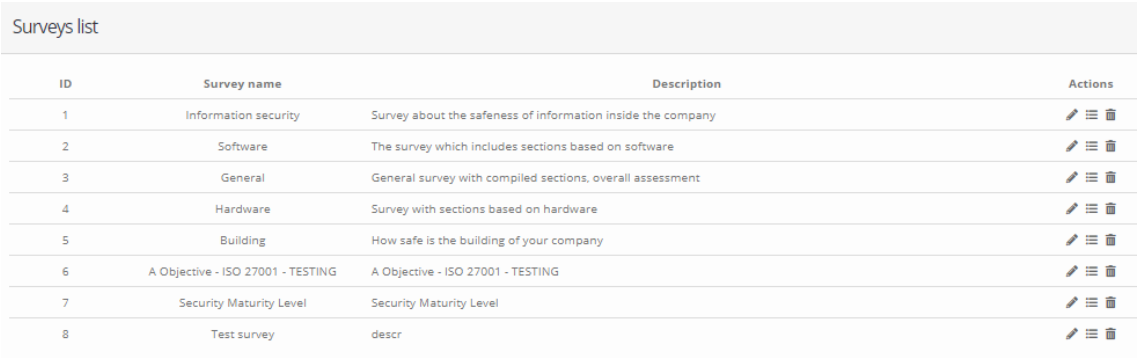


Figure 22 Dashboard of Assessments

Looking at different models of software applications that make a risk assessment, based on different techniques and methods, I have found it reasonable to create my model as well. To build this application I used the questionnaire technique.

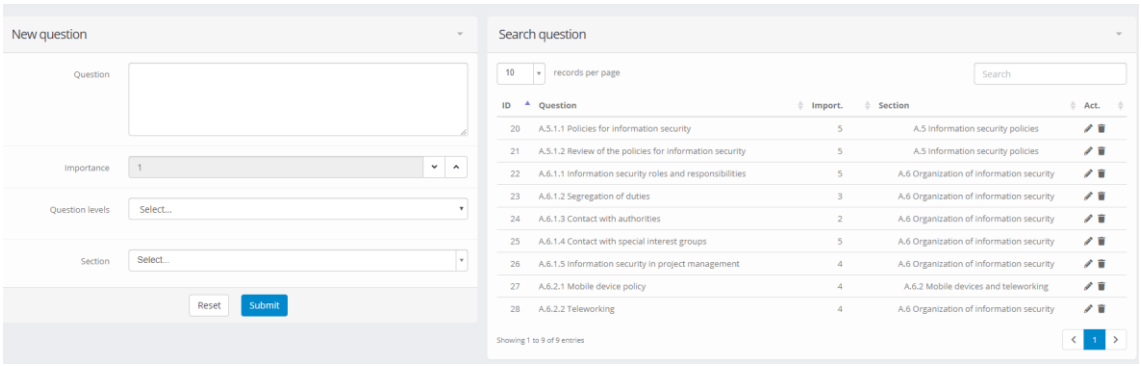


Figure 23 Managing Questions Section

This tool is designed to assist a skilled and experienced professional in ensuring that the relevant control areas of ISO / IEC 27001:2013 have been addressed.

This tool does not constitute a valid assessment, and the use of this tool does not confer ISO/IEC 27001:2013 certification. The findings here must be confirmed as part of a formal audit/assessment visit.

The application is built on web technology, as it provides easy and fast access from various devices and wherever there is Internet access. The technology used for the user-interacting look is developed with HTML, designed and stylized with CSS and Bootstrap, animations and JavaScript behaviors. To have dynamic content, to display the questionnaire etc., in the background for data manipulation is used PHP and data storage is used by the MySQL database

The software is structured in such a way that only authorized persons with specific privileges can access the system, and every use and manipulation of the system is recorded on a log sheet behind the system. Once one of these people accesses the system, he/she can create different types of questionnaires based on the assessment that he/she wants to make.

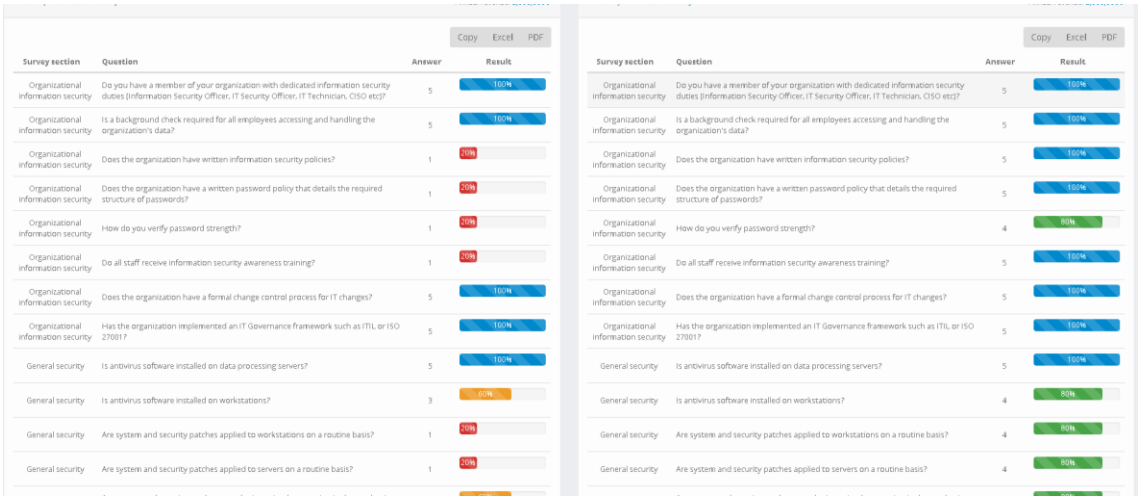


Figure 24 Comparing results between two different assessments

Therefore, any questionnaire can be created, and each questionnaire contains sections or subcategories. Sections should contain questions related to a particular topic. Questions can have up to 5 responses to be predetermined, and each question has its own value. Once completed with data, it is possible to create different versions of the questionnaires and provide manipulation with sections belonging to questionnaires, as a section may be in a different questionnaire. A questionnaire may have many sections. If the creation of questionnaires has been completed, registration of companies that are subject to the risk assessment process can be continued. Only simple, informative information about the company is required, to continue with the next steps.

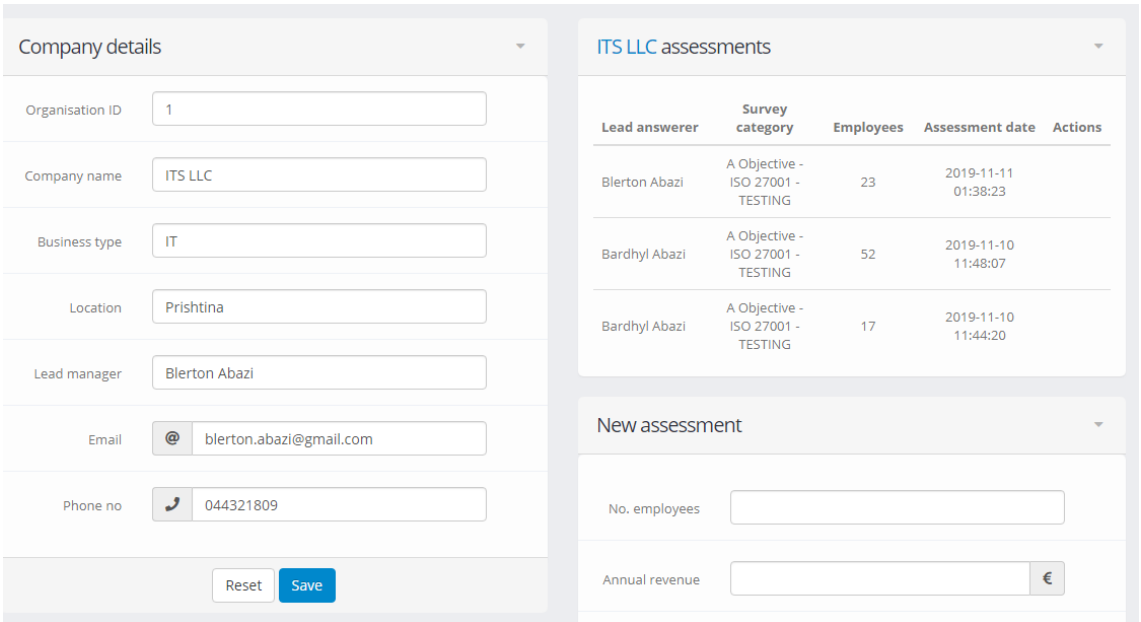


Figure 25 Company Details

Each question may have different types of responses tailored to each case, as there is a possibility to change five response levels as needed. Whenever a new question is added and the desired option is not available, a new set of options can be added and used in the new question. A set contains more than five options, all with the option of adjusting as needed.

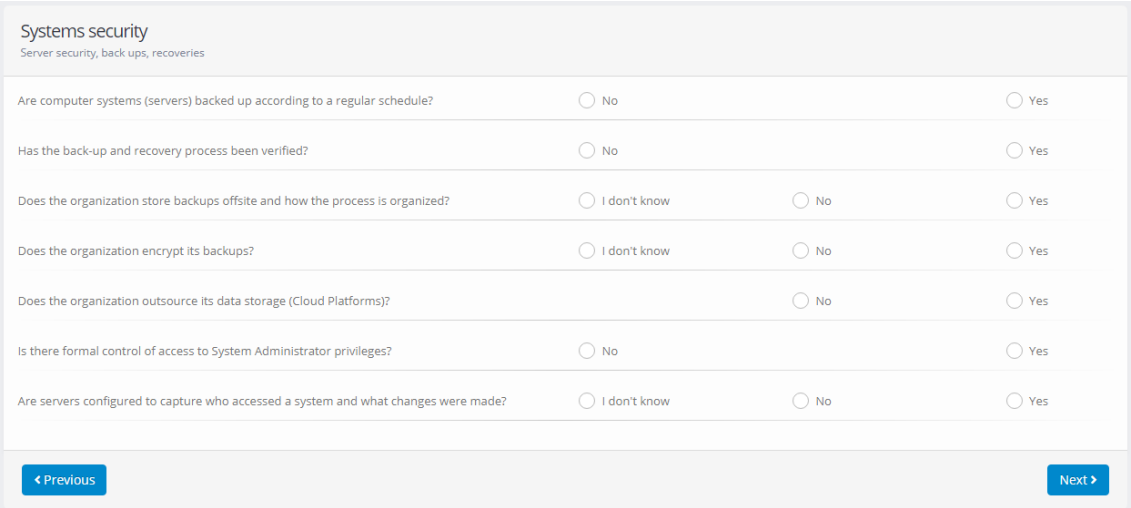
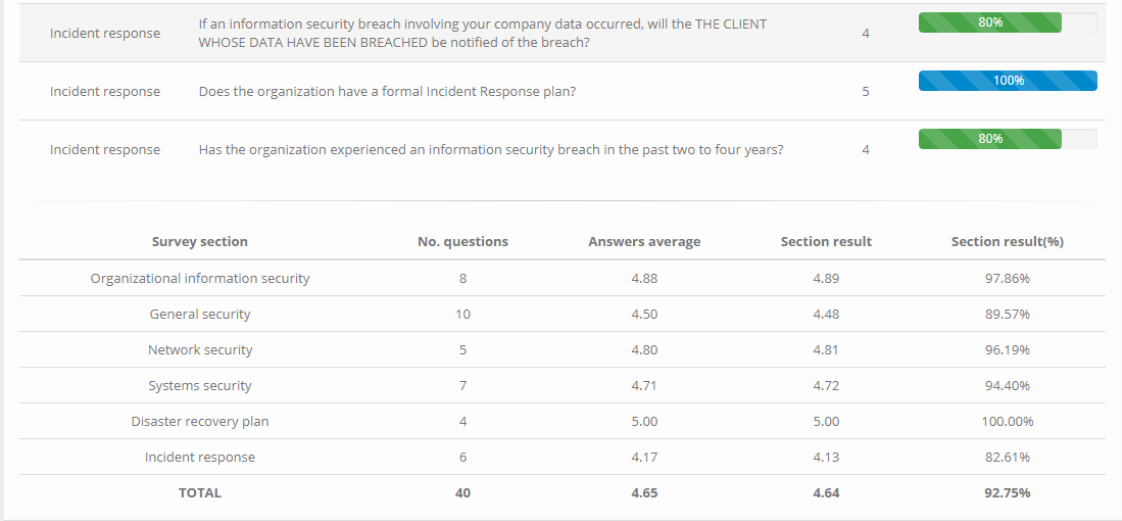


Figure 26 Part of the Assessment Processes

Although the answers to the questions are presented with a rating of 5 options ranging from 1 to 5 points, this does not mean that the analysis is quantitative. In the application there is the possibility that numbers can easily be replaced by word or sign and have the same meaning. These answers may represent frequency, method, concrete response to Yes and NO, etc.

After answering all questions in all sections, it is possible to progress to the next page, so all the answers are stored based on the data. From the answers provided, the result is calculated separately for each question, and it will show as a result, an average response per section and a general average. For each section a result and a recommendation based on the level of responses are produced.



Incident response	If an information security breach involving your company data occurred, will the THE CLIENT WHOSE DATA HAVE BEEN BREACHED be notified of the breach?	4	80%
Incident response	Does the organization have a formal Incident Response plan?	5	100%
Incident response	Has the organization experienced an information security breach in the past two to four years?	4	80%

Survey section	No. questions	Answers average	Section result	Section result(%)
Organizational information security	8	4.88	4.89	97.86%
General security	10	4.50	4.48	89.57%
Network security	5	4.80	4.81	96.19%
Systems security	7	4.71	4.72	94.40%
Disaster recovery plan	4	5.00	5.00	100.00%
Incident response	6	4.17	4.13	82.61%
TOTAL	**40**	**4.65**	**4.64**	**92.75%**

Figure 27 Presenting the results

8. Framework Prototype Validation Method

After I have finalized the framework prototype, I have followed with the process of validation in order to make it more accurate and functional. The framework prototype has been validated by companies, IT auditors and IS officers. The process of validation included the key points of the system that are related to the following 5 key elements:

1. System usefulness
2. Time consuming on completion of the assessment
3. Support Information (description of the tools)
4. Information / Report quality
5. Interface Quality (System Navigation)

The aforementioned elements have been part of the validation through the test scenarios that I have developed and distributed to the stakeholders involved in the process to test the framework prototype. Each of the 5 elements has been teste with a specific scenario, in a total of 5 use case scenarios. After completing the test scenarios, the validation process has been followed by the ASQ (After-Scenario Questionnaire) model in which system users will evaluate the 5 key elements by answering 5 questions created on the Likert scale model with points 1 to 5 where 1 meaning strongly disagree and 5 means strongly agree. After the user has completed the ASQ, the ASQ score is calculated by taking the average (arithmetic mean) of the 5 questions (Lewis, 1995).

The ASQ method is a method developed to measure the satisfaction of using technology through questionnaires (Lewis, 1995). I determined this method based on the number of respondents I have received and the simplicity of generating results that directly corresponds to my framework development model.

The following test scenarios with steps are distributed to the stakeholders:

Table 12 - Use Case Scenario - System Usefulness

Test Scenario name: **System Usefulness**
Scenario: Successful login into the system. Access to the list of companies that have been assessed from the framework. Access to the questionnaire management system. Sign Out
Steps: 1. The user can access the system with a username and password. 2. The user has entered the dashboard where he/she can see all the brief report on the current situation of the assessments and reports for each survey. 3. User click at the Companies Navigation Menu 4. It shows two sub-menus – Companies List and New Company 5. User clicks on the Companies List and it shows the complete list of the companies that have been assessed 6. User clicks on the Questions Navigation Menu 7. After it, shows two sub-menus – Manage Questions and Manage Question Leve 8. Users click on the Manage Questions and the windows show two options on the screen such as: New questions and Search Questions 9. The user searches for a question and it shows the result. 10. The user clicks the Logout button which is at the top right corner after the username. 11. User logs out successfully

Table 13 - Use Case Scenario - Time consuming on completion of the assessment

Test Scenario name: **Time consuming on completion of the assessment**
Scenario: Successful login into the system.

Registering a new company for assessment Creating a new assessment Starting the assessment Completing the assessment Generation, the Results Sign Out
Steps: 1. The user can access the system with a username and password. 2. The user creates a new company for assessment from the Companies Navigation Menu 3. The user creates New Assessment for the company from the Assessment Menu 4. User starts to answer all the questions on the assessment/questionnaire 5. The questionnaire is composed of 8 pages 6. In the end the user clicks the finish button 7. After the use click the finish button it shows the results from the answers and the list of recommendations 8. The user clicks the Logout button which is at the top right corner after the username. 9. User logs out successfully

Table 14 - Use Case Scenario - Support Information

Test Scenario name: **Support Information**
Scenario: Successful login into the system. Registering a new company for assessment The user enters invalid data Starting the assessment User leaves several questions incomplete Sign Out
Steps: 1. The user can access the system with a username and password. 2. The user creates a new company for assessment from the Companies Navigation Menu 3. The user types letters at the phone number text box.

4. The system does not allow letters at the phone number box (it is mandatory to write only numerical values) 3. The user creates New Assessment for the company from the Assessment Menu 4. User starts to answer all the questions on the assessment and in the end left some of the questions without answers 5. The system will not allow finishing the assessment without completing all the questions (The error box is shown which explain that it is mandatory to complete all the questions) 6. In the end the user clicks the finish button 8. The user clicks the Logout button which is at the top right corner after the username. 9. User logs out successfully

Table 15 - Use Case Scenario - Information / Report Quality

Test Scenario name: **Information / Report Quality**
Scenario: Successful login into the system. User enter the Assessment List The user wants to see the reports from previous assessments The user compares two different assessments from the same company Sign Out
Steps: 1. The user can access the system with a username and password. 2. The user clicks the Assessment Navigation Manu 3. The user views the previous assessment for a specific company 4. The user checks the results and compares them to the answers he gave 5. After it, the user clicks the small checkbox on the right side of assessment and then clicks the compare assessment button in the bottom of the page 6. In the windows there are shown two different assessments that the user chose to compare the results 7. The user clicks the Logout button which is at the top right corner after the username. 8. User logs out successfully

Table 16 - Use Case Scenario - Interface Quality (System Navigation)

Test Scenario name: **Interface Quality (System Navigation)**
Scenario: Successful login into the system. The user navigates on different parts of the system freely Sign Out
Steps: 1. This scenario is open to the user to navigate through the system and in the end to present his/her general opinion about the Interface Quality on the system navigation.

Below I present the statistical analysis regarding the responses received. This framework has been distributed to companies with the aim to measure the performance and actual use of the system using the Technology Acceptance model. 50 responses were collected from the respondents ranging on their satisfaction with the amount of time to complete a task, satisfaction with support information, report generation and ease of navigation. All results and analysis of the responses were conducted in SPSS environment.

Table 17 - Pattern and distribution of respondents' satisfaction with the actual system use.

Variable	Label	Frequency	Percentage (%)
Satisfied with ease of completing tasks	Neutral	2	4.0
	Agree	14	28.0
	Strongly Agree	34	68.0
Satisfied with the amount of time to complete tasks	Neutral	4	8.0
	Agree	21	42.0
	Strongly Agree	25	50.0
Satisfied with the support information	Neutral	5	10.0
	Agree	17	34.0
	Strongly Agree	28	56.0
Satisfied with report generation and results	Neutral	3	6.0
	Agree	18	36.0
	Strongly Agree	29	58.0
Satisfied with easy navigation on the system	Neutral	2	4.0
	Agree	18	36.0
	Strongly Agree	30	60.0

The result of the analysis presented in Table 17 showed that for any of the instrumental variables used to access the overall satisfaction and use of the systems, the respondents were satisfied at least 90% of the time.

I present first the result of the factor analysis here below; the first point of call is the Kaiser-Meyer-Oklin (KMO) test of sampling adequacy. This test measures how suited a data is for factor analysis by measuring the sampling adequacy of each variable and the proportion of variance among variables that might be common variance.

Table 18 - Correlation matrix of the important variables

Correlation Matrix

	Satisfied with ease of completing tasks	Satisfied with the amount of time to complete tasks	Satisfied with the support information	Satisfied with report generation and results	Satisfied with easy navigation on the system
Satisfied with ease of completing tasks	1.000	-.251	.069	-.274	.131
Satisfied with the amount of time to complete tasks		1.000	-.125	-.048	.013
Satisfied with the support information			1.000	-.195	.372
Satisfied with report generation and results				1.000	-.378
Satisfied with easy navigation on the system					1.000

a. Determinant = .613

The result of the correlation matrix shows the different bivariate relationships between all pairs of variables, there exists a relatively weak relationship between all the variable pairs in the questions sampled.

Table 19 - KMO AND Bartlett test

Communalities

	Initial	Extraction
Satisfied with ease of completing tasks	**1.000**	**.591**
Satisfied with the amount of time to complete tasks	**1.000**	**.721**
Satisfied with the support information	**1.000**	**.412**
Satisfied with report generation and results	**1.000**	**.536**
Satisfied with easy navigation on the system	**1.000**	.669

Extraction Method: Principal Component Analysis.

From the result above, the extraction communalities are estimates of the variance in each variable accounted for by the components. The communalities in this table are all high, which indicates that the extracted components represent the variables well. From the above, satisfied with the amount of time to complete tasks ranks tops while Satisfied with the support information ranks least amongst the 5 variables.

In this section, I present the variation explained by the contributing variables, my aim here is to determine the optimal number of components that would predict the actual satisfaction with tested using the acceptance model, by doing this gives us the ideas as to the number of reduced components which can thereafter be selected on the communality table using the strength of the variables.

Table 20 - Proportion of variation explained by the selected components

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.758	35.151	35.151	1.758	35.151	35.151	1.676	33.524	33.524
2	1.173	23.453	58.603	1.173	23.453	58.603	1.254	25.079	58.603
3	.950	19.001	77.604						
4	.574	11.483	89.087						
5	.546	10.913	100.000						

Extraction Method: Principal Component Analysis.

From the above result (Table 21), only 2 of the 5 components are significant in predicting and understanding the actual satisfaction with tested using the acceptance model, the

variables are obtained by extracting the significant contributors using Eigen value of 1. My result showed that, the 2 components predict about 59% of the variation in the overall satisfaction of usage, meaning that the remaining variables account for the 41% unexplained.

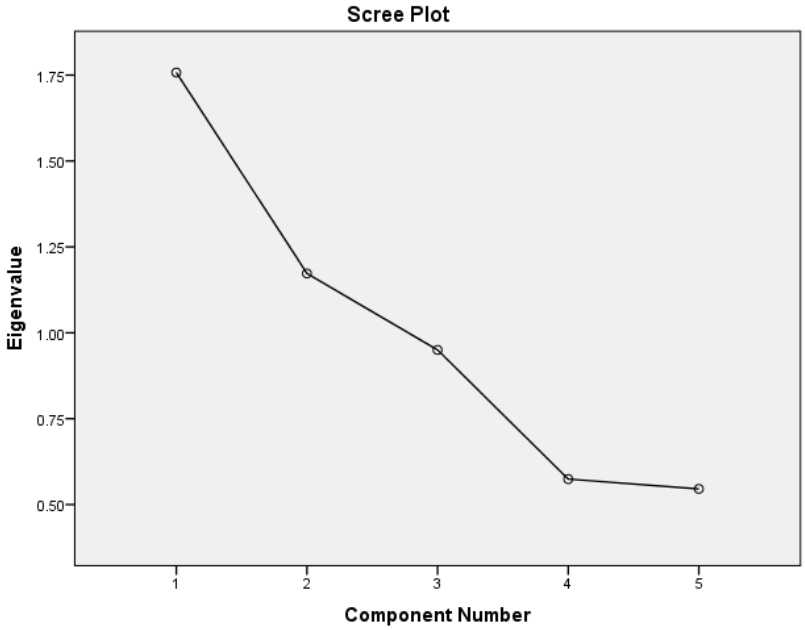


Figure 28 - Scree plot extraction of the significant component using the Eigen value of 1

The result of the scree plot corroborates the result of table 21 that only 2 of the components rank above the Eigen value of 1.

Finally, I tried to explore whether there is a linear association between the overall satisfaction with completing a task using the acceptance model and the other satisfaction indicator. The result of the analysis is presented below; hypothesis testing and decision making in this case would be inferred from the results of the chi-square testing.

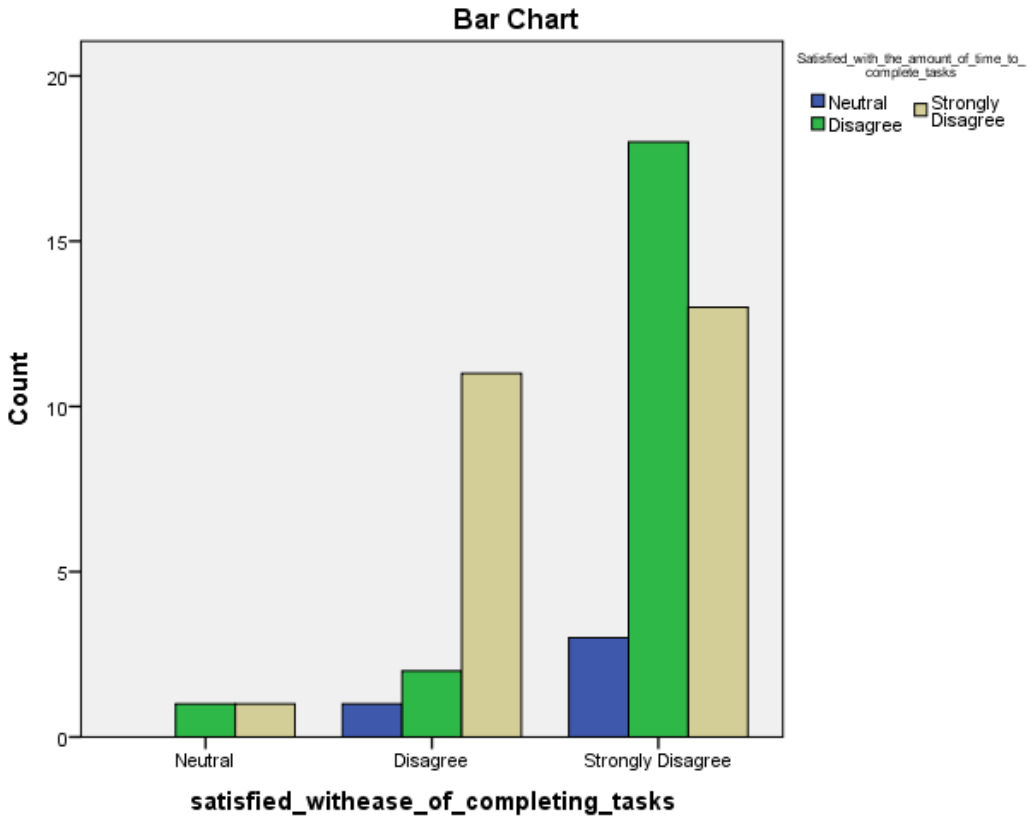
Null Hypothesis 1: There is no significant Association between respondent's satisfaction with the ease of completing the task and the amount of time to complete tasks

Crosstab

Count

		Satisfied_with_the_amount_of_time_to_complete_tasks			
		Neutral	Agree	Strongly Agree	Total
satisfied_withease_of_completing_tasks	Neutral	0	1	1	2
	Agree	1	2	11	14

	Strongly Agree	3	18	13	34
Total		4	21	25	50



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.988[a]	4	.137
Likelihood Ratio	7.700	4	.103
Linear-by-Linear Association	3.084	1	.079
N of Valid Cases	50		

a. 5 cells (55.6%) have expected count less than 5. The minimum expected count is .16.

From the result of analysis above, the chi-square ($\chi^2(2) = 6.988,\ p > 5\%$) and this corresponds to the non-rejection of the above stated null hypothesis, I can however conclude from the above that there is no significant Association between respondent's satisfaction with the ease of completing the task and the amount of time to complete tasks

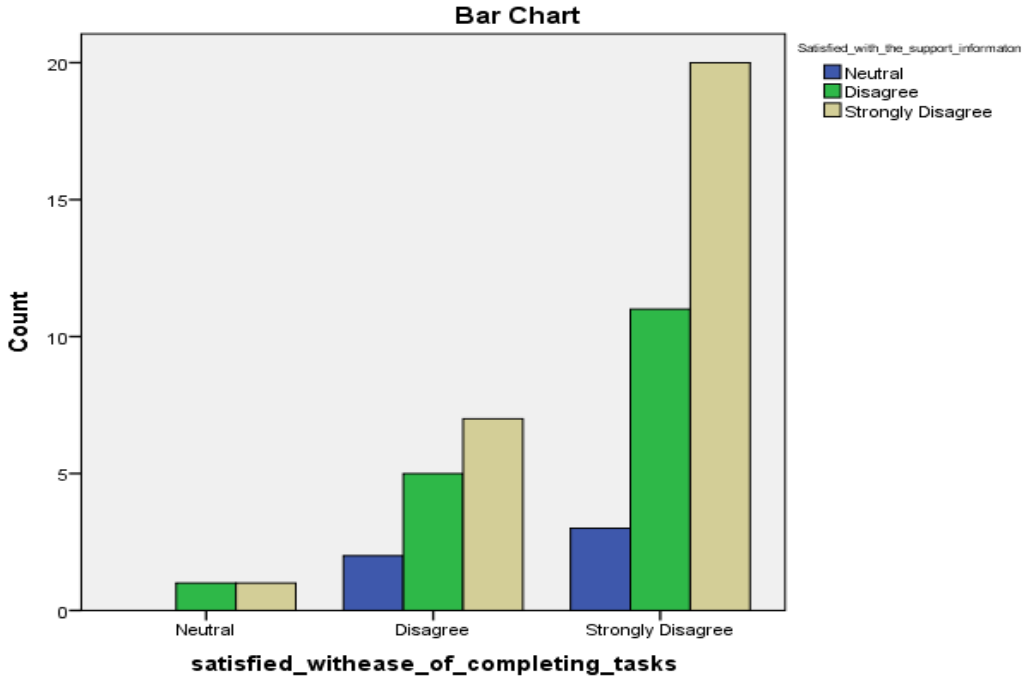
Null Hypothesis 2: There is no significant Association between respondent's satisfaction with the ease of completing the task and the support information

Crosstab

Count

	Satisfied_with_the_support_informaton	Total

		Neutral	Agree	Strongly Agree	
satisfied_withease_of_co mpleting_tasks	Neutral	0	1	1	2
	Agree	2	5	7	14
	Strongly Agree	3	11	20	34
Total		5	17	28	50



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.845[a]	4	.932
Likelihood Ratio	1.001	4	.910
Linear-by-Linear Association	.231	1	.631
N of Valid Cases	50		

a. 6 cells (66.7%) have expected count less than 5. The minimum expected count is .20.

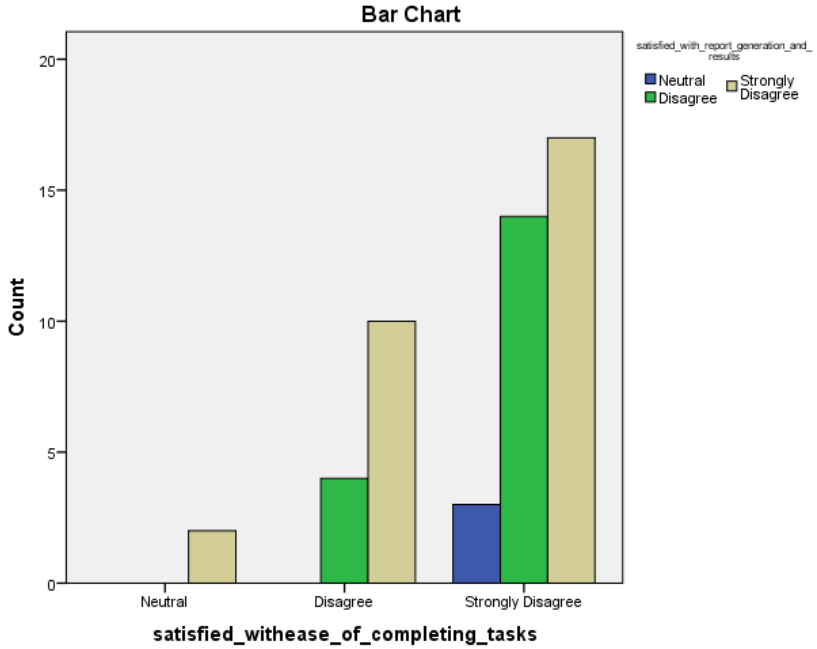
From the result of analysis above, the chi-square ($\chi^2(2) = 0.845$, $p > 5\%$), this corresponds to the non-rejection of the above stated null hypothesis, I can however conclude from the above that there is no significant Association between respondent's satisfaction with the ease of completing the task and the support information

Null Hypothesis 3: There is no significant Association between respondent's satisfaction with the ease of completing the task and the report generation

Crosstab

Count

		satisfied_with_report_generation_and_results			
		Neutral	Agree	Strongly Agree	Total
satisfied_withease_of_completing_tasks	Neutral	0	0	2	2
	Agree	0	4	10	14
	Strongly Agree	3	14	17	34
Total		3	18	29	50



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4.018[a]	4	.404
Likelihood Ratio	5.525	4	.238
Linear-by-Linear Association	3.678	1	.055
N of Valid Cases	50		

a. 5 cells (55.6%) have expected count less than 5. The minimum expected count is .12.

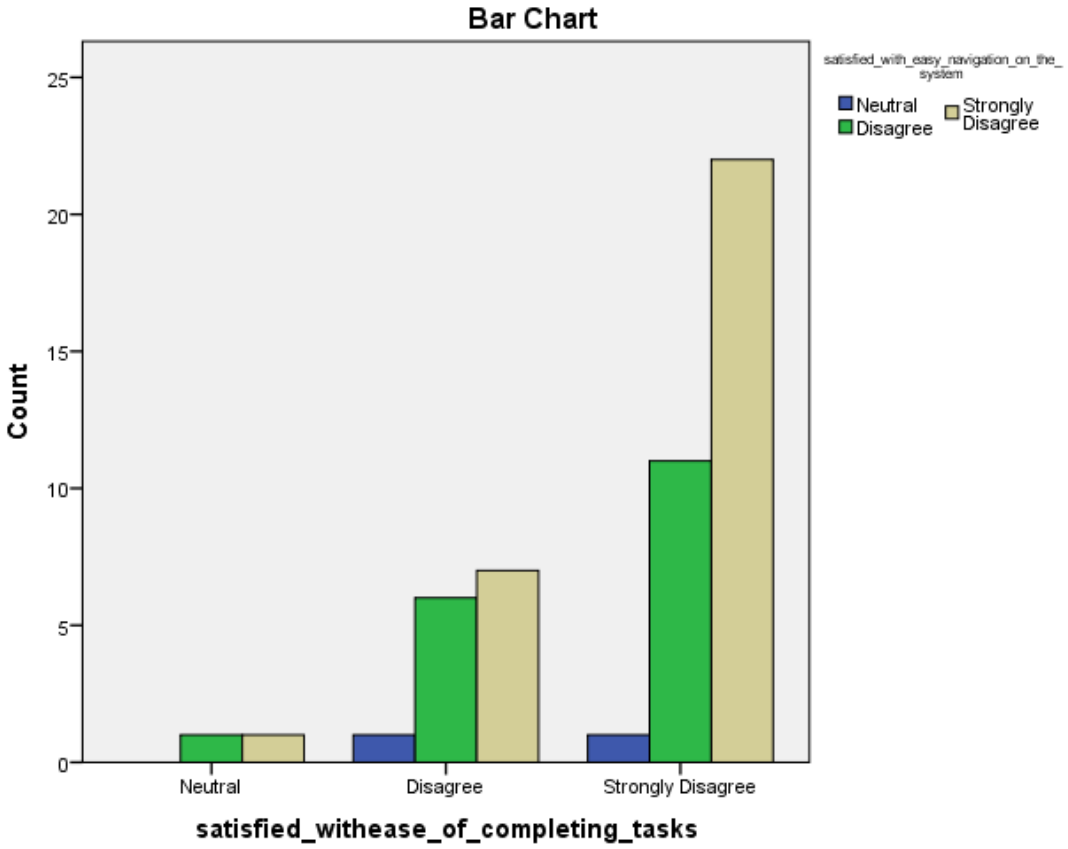
From the result of analysis above, the chi-square ($\chi^2(2) = 4.018$, $p > 5\%$), this corresponds to the non-rejection of the above stated null hypothesis, I can however conclude from the above that there is no significant Association between respondent's satisfaction with the ease of completing the task and the report generation

Null Hypothesis 4: There is no significant Association between respondent's satisfaction with the ease of completing the task and the easy navigation on the system

Crosstab

Count

		satisfied_with_easy_navigation_on_the_system			
		Neutral	Agree	Strongly Agree	Total
satisfied_withease_of_completing_tasks	Neutral	0	1	1	2
	Agree	1	6	7	14
	Strongly Agree	1	11	22	34
Total		2	18	30	50



Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.331[a]	4	.856
Likelihood Ratio	1.349	4	.853
Linear-by-Linear Association	.837	1	.360
N of Valid Cases	50		

a. 5 cells (55.6%) have expected count less than 5. The minimum expected count is .08.

8.1 Proposed TAM model

In terms of the variation explained by the instrumental variables related to perception and satisfaction usage (**see Table 22 – Model Results)**, only 15% of variation in the satisfaction with use is explained by the instrument available, similarly, the regression

analysis of variance suggested that the proposed model is not a good fit, owning to the (F (4,45) =1.934, p >5%).

In terms of the individual parameter, only the ease of navigation tends to affect the satisfaction of use positively.

Table 21 - Model Results

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.38300
R Square	0.14668
Adjusted R Square	0.07084
Standard Error	0.54249
Observations	50

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	4	2.276625909	0.569156477	1.93395137	0.121178892
Residual	45	13.24337409	0.294297202		
Total	49	15.52			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	6.773277133	1.284487945	5.27313406	3.68618E-06	4.186185 61	9.360368657
Ease completing Task	-0.235922799	0.122163711	-1.93120196	0.059771669	-0.481973144	0.010127546
Support Information	-0.028943 9	0.12497637	-0.231594981	0.817902516	-0.280659 23	0.222771 43
Report Generation	-0.254368337	0.136772846	-1.859786818	0.069460105	-0.529842 99	0.021106317

Ease Navigation	0.04130 1823	0.153717477	0.268686578	0.789398 893	-0.26 8301 069	0.3509 04715

The proposed model is given by

$$Satisfaction\ with\ Use = 6.77 - 0.236\ Ease\ completing\ Task - 0.029\ Support\ Information - 0.254\ Report\ Generation + 0.041\ Ease\ Navigation\ support$$

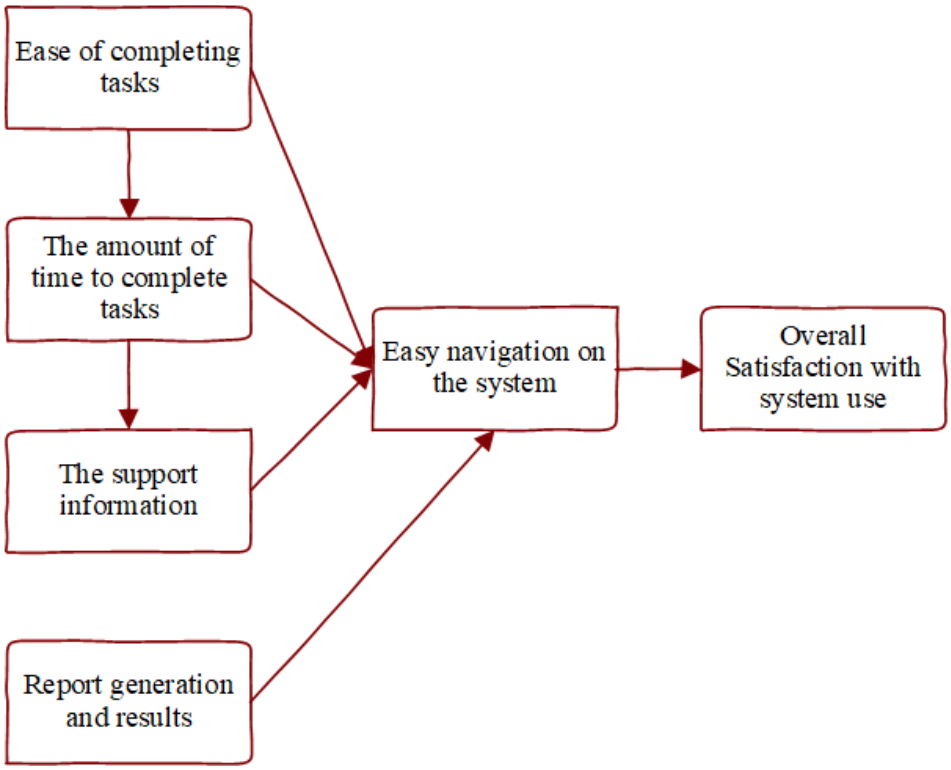


Figure 29 - Proposed TAM model for evaluation

This model **(Figure 29)** helps us measure the overall ease of use (overall satisfaction of use of the system), and I expect that the factors and determinants of this use to be impacted upon by some fluctuations called (attitude) for more realistically behavioral intention which is measured through data and response collated on the system usage.

The model suggests that I can measure two main factors namely:

I identified within my system variables that link to the TAM model structure below, and how it helps us feed into the overall ease of use (system overall satisfaction).

Perceived ease of Use - Ease of completing tasks and the amount of time to complete tasks

Perceived usefulness - The support information

From the results of the analysis presented above, I can conclude with the following;

- The descriptive statistics showed that the respondents opined strong agreement with the satisfactory parameters.
- The result of the factor analysis however showed that 2 of the 5 components carried about 59% of the weight in the satisfaction indicators. Satisfied with the amount of time to complete tasks ranks tops while Satisfied with the support information ranks least.
- It is hard to identify a linear association between the overall satisfaction with completing a task using the acceptance model and the other satisfaction indicators, the reason being that all the respondents answered the questions in a similar pattern of agreement.

Statisticians generally estimate models to explain different and underlying relationships that ensured or present between several phenomena. In this case, I measured the satisfaction with the use of my TAM model verified whether or not the proposed predictors are essentially contributing to the overall system use. The predictors to measure the satisfaction with use range from the ease of completing the task to the ease of use which had earlier been explained in the TAM framework. The result of the analysis showed that the predictors measuring the efficiency of the TAM framework could only explain the satisfaction of the use of the model. The positive side is the additional result which suggests that, if we achieve a substantial model improvement the ease of navigation is likely to be the positive driver of the satisfaction of use with the TAM framework, meaning that the ease of completing task, support information and report generation are somehow important parts to improve the model result using this framework.

9. Summary and discussion

In the dissertation I presented an approach, model and solution for the information security risk assessment especially for the banking sector, insurance companies and IT industry. Through this approach, I've explored some of the biggest gaps that organizations have in implementing security. I identified the points in which most organizations encounter problems with the use of the questionnaire, while my application helps in solving these problems. In this part I did a summary of my work so far and will present the possible future work.

While the dependence of people on different platforms is on the rise, the risk this data will be exposed is likely to increase. Thus, research data reflects an interesting, current state of information protection. A growing number of companies continue to feel

threatened by cyberattacks, and the media frequently report attacks on data being made for larger companies such as Facebook and Google as well.

In addition to the above-mentioned risks of data destruction, companies need to consider the reality that such attacks can happen. It is imperative that every company with an online presence considers the need to protect their data, whether due to the protection of the business or its users

In Kosovo, businesses and organizations need to take the issue of data attacks seriously, put measures in place and make new investments for their customers' security. They need to ensure their measures are appropriate, they have to report cases of security breaches to increase trust in the handling of personal information.

There is no doubt, the risk of data attacks has risen over the years. To prevent data attacks, businesses and organizations should undertake several safeguards as a minimum to ensure safekeeping, and the measure would guide companies:

1. Make regular assessments of security risks in the data;
2. Update security software;
3. Maintain an internal encryption policy;
4. Encrypt data and maintain proper data in case of cyber-attack;
5. Prepare/train staff concerning data security;
6. Ensure partners companies have high standards of data protection; and
7. Employ third parties to conduct security assessments within the company.

These recommendations, if considered, will, without doubt, have a positive impact on data retention within any organization, and will also have positive results regarding the economic aspect, reputation, and ultimately user experience.

Estimation of the risk of data attacks varies depending on the company. Some of the suggestions made in the current research are measures already undertaken by some companies, and some are not.

Information Security (IS) is more than IT security due to its complexity. In addition to the technical aspects, many other questions from the areas of "people" and "processes" must be considered. However, the goal of continuously improving IS adapted to current changes can only be achieved by building a process to manage the IS. Another critical

success factor is the acceptance of the measures. It must be ensured that these are appropriate and geared to the organization's "business operations".

Regarding the above mentioned challenges, I've dealt with the following research questions:

Main Research Question: How can we develop the semi-automatic risk assessment system? How risk assessment systems can be extended to provide a list of recommendations by identifying the list of areas with a lack of suitable security measures through an automated risk or semi-automated assessment solution?

I have answered the main research question by developing a framework prototype that applies a semi-automated information security risk assessment method and provides a list of recommendations. The framework prototype development followed the software development life cycle method, where in the beginning I set the conceptual model followed by the data model and functional description. The development of the framework prototype has been validated by the ASQ model with 5 test scenarios. Details of the answer to the **main research question** are provided in c**hapter 7**.

Sub-question 1 (followed by Main Research Question): How is the risk assessment process in the context of the information security management systems' implementation handled within the organizations (specifically on the IT sector, banking sector and insurance companies)? What are the key elements of the maturity framework in the field of risk assessment, how can it be described conceptually?

I answered the sub-question through the need identification survey, which I performed with organizations from the IT Industry, banking sector and insurance companies. The questionnaire format supported gathering reasonable answers from all stakeholders ranging from the managerial level to the experts and professional staff. The survey helped to identify the significant difference between the IT industry and other sectors such as the banking sector and insurance companies in the risk assessment practice. Through my survey with organizations I noted a huge gap in the aspect of standard compliance to the IT sector and the realistic applicability of the standard. Another issue that I found is that information security risk assessment is a major challenge for organizations in the IT sector, because the position of information security officers is covered by the position of an IT technician. I identified that insurance companies are relatively well organized, but there are still some gaps especially on the regular check or scanning of the systems from

possible vulnerabilities. Lack of regular controls poses challenges to computer systems, given that most of the attacks on data systems occur precisely because of carelessness in updating computer systems. A huge number (around 40%) of insurance companies do not use any system to prevent eventual attacks, and such organizations can potentially have an outdated infrastructure that does not support advanced algorithms for detecting attacks or the other factor may be the financial implication of upgrading the existing technology. A detailed result from the survey, can be found in **Chapter 6 – Need Identification - Survey about the current level of security in enterprises.**

Sub-question 2 (followed by Main Research Question): How can we map the findings of the risk assessment process for the information security maturity models?

To answered this question, I developed a **conceptual model** which is based on the answers that I received during my need identification survey and a proposed framework prototype. The framework links information security control of ISO 27001 with CVSS metrics then using the scoring model provided by CVSS to evaluate it on a qualitative rating scale. I have analyzed all ISO 27001 Information Security Controls to see their relevance and what are their common points that may have the same scoring pattern. Their analysis is based on case studies and technical papers presented by various companies dealing with information security (Almeida, Lourinho, Da Silva, & Pereira, 2018; Beckers, Hofbauer, Quirchmayr, & Wills, 2013; Sheikhpour & Modiri, 2012). Based on the conceptual model I developed my proposed framework prototype, which is a web-based application. Details of the answer to sub-question 2 can be found in **Chapter 7.**

Sub-question 3 (followed by Main Research Question): Is it possible to measure the maturity of the risk management practices within a company through a semi-automated risk assessment system according to the literature?

I answered this question through the literature review on analyzing and describing the digital maturity models in the context of information security. I noticed that in most cases semi-automated risk assessment frameworks processes had been used mainly by the audit firms.

The following areas are considered the main issues to be taken into while measuring the maturity of the risk assessment:

1. Information security management systems

2. Security measures and monitoring
3. Evaluation of IT security
4. Cryptographic and IT security procedures
5. Physical security

I answered this sub-question in detail in **Chapter 3** and **Chapter 6.**

9.1 Main Contributions

The main contributions of this work are summarized as follow:

1. The state of the art analysis of the information security risk assessment maturity models as well as the use of risk assessment processes within organizations.
2. A process mapping between the ISMS Standard (ISO 27001) and CVSS, which is a valuable foundation for future research in the area of information security.
3. The presented conceptual model which combines the process of risk identification, ISO 27001 control objectives and CVSS.
4. The proposed framework prototype, which is a reduction of complexity of risk identification and through the recommendation lists provides you the opportunity for a quick fix.
5. A solution and a framework for enterprises in analyzing their information security risks and the security maturity level.
6. The method of validation and verification of the framework. This method also demonstrates the relevance of the topics of this thesis in the industry.
7. The evaluation of the framework in a real-world scenario is proof of the applicability and adaptability of the framework.

Finally, management support plays an essential role in the success of IS. To follow a risk-based decision making can be successful in the long-term. However, this is not a quick and easy process and requires the involvement of all employees and above all the proactive support of the management. The current study has demonstrated information security in Kosovo, specifically in the banking sector, IT Industry and insurance field, businesses and organizations face severe risks from a range of threat types. The current research set out to determine information security awareness and practices in my country. The analysis was used to understand the information security level in the above-mentioned sectors and, applied to design an appropriate information security risk assessment model that considers the cultural impact as well.

My proposed framework has a modular structure which is a good starting point for further development and compliance with other standards as well. As future work, I suggest that after the use of the framework from several organizations and industries, when the database is populated with data, it may be important to integrate models of Big Data Analytics which may help IT Auditors and CIO with activities which may be predicted by the system.

According to the wide opportunities that the framework offers and based on the state-of-the-art research in specific areas, I consider the following activities are important for future research:

1. Piloting the framework in different industries (except. IT, banking and insurance) with different sizes of organizations. This will be a good point for further optimization of the framework.
2. There is a need for more study to reach full compliance regarding the ISO 27001 control objectives and the CVSS process elements **(see Chapter 7.2).**
3. Research related to the integration of process in information security management frameworks, data protection management and state of the art process framework.
4. There is still a lack of information about the actual usage of maturity level models within ISMS, and this must be investigated by further research.
5. Analyzing the organizational effect of the usage of the current method and framework.

References

Aceituno, V. (2007). Information Security Management Maturity Model. Retrieved from www.ism3.com

Al-rashdi, Z., Dick, M., & Storey, I. (2017). Literature-based analysis of the influences of the new forces on ISMS : A conceptual framework, 116–124. https://doi.org/10.4225/75/5a84e4dc95b42

Ali, M., Kurnia, S., & Johnston, R. B. (2011). Understanding the Progressive Nature of Inter-Organizational Systems (IOS) Adoption.

Almeida, R., Lourinho, R., Da Silva, M. M., & Pereira, R. (2018). A model for assessing COBIT 5 and ISO 27001 simultaneously. In *Proceeding - 2018 20th IEEE International Conference on Business Informatics, CBI 2018*. https://doi.org/10.1109/CBI.2018.00016

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, *124*, 691–697. https://doi.org/10.1016/j.procs.2017.12.206

Amaratunga, D., Baldry, D., Sarshar, M., & Newton, R. (2002). Quantitative and qualitative research in the built environment: application of "mixed" research approach. *Work Study*. https://doi.org/10.1108/00438020210415488

Amberg, M., Markov, R., & Okujava, S. (2005). A Framework for Valuing the Economic Profitability of E-Government. In *International Conference on E-Government (ICEG)*. Ottawa, Canada: Proceedings of the International Conference on E-Government (ICEG).

Bazaz, T., & Khalique, A. (2016). A Review on Single Sign on Enabling Technologies and Protocols. *International Journal of Computer Applications*, *151*(11), 975–8887. Retrieved from http://www.ijcaonline.org/archives/volume151/number11/bazaz-2016-ijca-911938.pdf

Beckers, K., Faßbender, S., Heisel, M., Küster, J.-C., & Schmidt, H. (2012).

Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches, (256980), 14–21. https://doi.org/10.1007/978-3-642-28166-2_2

Beckers, K., Hofbauer, S., Quirchmayr, G., & Wills, C. C. (2013). A method for re-using existing ITIL processes for creating an ISO 27001 ISMS process applied to a high availability video conferencing cloud scenario. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-40511-2_16

Brackney, R., & Anderson, R. (2004). *Understanding the Insider Threat - Proceedings of a March 2004 Workshop*. *Proceedings of the March 2004 Workshop*. https://doi.org/QA 76.9 .A25 B73 2004

Brown, A. (2005). IS Evaluation in Practice. *Electronic Journal of Information Systems Evaluation*, *8*(3).

Bruin, T. De, & Rosemann, M. (2005). Towards a Business Process Management Maturity Model. In D. Bartmann, F. Rajola, J. Kallinikos, D. Avison, R. Winter, P. Ein-Dor, … C. Weinhardt (Eds.), *ECIS 2005 Proceedings of the Thirteenth European Conference on Information Systems* (pp. 1–12). Germany, Regensburg: Verlag and the London School of Economics. Retrieved from https://eprints.qut.edu.au/25194/

Burgeois, D. T. (2014). *Information Systems for Business and Beyond*. Retrieved from saylor.org

Business, V. (2018). 2018 Data breach investigations report. *Trends*, 1–62. Retrieved from http://rp_data-breach-investigations-report-2013_en_xg.pdf

Businge, J., Serebrenik, A., & van den Brand, M. (2010). An Empirical Study of the Evolution of Eclipse Third-party Plug-ins. In *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE)* (pp. 63–72). New York, NY, USA: ACM. https://doi.org/10.1145/1862372.1862389

Caldas, M. P. (2009). Research design: qualitative, quantitative, and mixed methods approaches. *Revista de Administração Contemporânea*. https://doi.org/10.1590/s1415-65552003000100015

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Carnegie Mellon University*. https://doi.org/S0140-6736(85)90167-9 [pii]

Chapin, D. a., & Akridge, S. (2005). How Can Security Be Measured? *Information Systems Control Journal*, *2*, 43–47. Retrieved from http://m.isaca.org/Journal/Past-Issues/2005/Volume-2/Documents/jpdf052-how-can-security.pdf

Cockburn, A. (2008). Using both incremental and iterative development, *21*, 27–30.

Collis, J., & Hussey, R. (2013). *Business Research A Practical Guide for Undergraduate and Postgraduate Students 3rd edition*. *palgrave*. https://doi.org/10.1038/142410a0

Cooper, D. R., & Schindler, P. S. (2006). *Business research methods* (9th ed). Boston : McGraw-Hill Irwin.

Creswell, J., Klassen, A. C., Plano, V., & Smith, K. C. (2011). Best Practices for Mixed Methods Research in the Health Sciences. *Methods*. https://doi.org/10.1002/cdq.12009.

Creswell, J., & Plano Clark. (2007). Designing and Conducting Mixed Methods Research. *Australian and New Zealand Journal of Public Health*. https://doi.org/10.1111/j.1753-6405.2007.00096.x

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Diver, S. (2007). Information Security Policy - A Development Guide for Large

and Small Companies. *Information Security, SANS Institute*.

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology*, *14*(1), 23–57. https://doi.org/10.1108/13287261211221128

Easterby-Smith, M. T., & Thorpe, R. (2002). R. and Lowe, A.(2002). *Management Research: An Introduction*.

Elky, S. (2019). An Introduction to Information System Risk Management.

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud and Security*, *2011*(1), 5–7. https://doi.org/10.1016/S1361-3723(11)70005-7

Ezingeard, J. N., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*. https://doi.org/10.1177/030630700703200404

Falk, M., & Falk, M. (2012). Ableitung des Control-Frameworks für IT-Compliance. In *IT-Compliance in der Corporate Governance*. https://doi.org/10.1007/978-3-8349-3988-3_5

Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach* (1st ed.). Newton, MA, USA: Butterworth-Heinemann.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, *60*(2), 151—157. https://doi.org/10.1016/s1386-5056(00)00115-5

Ge, X. Y., Yuan, Y. Q., & Lu, L. L. (2011). An information security maturity evaluation mode. *Procedia Engineering*, *24*, 335–339. https://doi.org/10.1016/j.proeng.2011.11.2652

Giddings, L. S., & Grant, B. M. (2006). Mixed methods research for the novice researcher. *Contemporary Nurse : A Journal for the Australian Nursing Profession*. https://doi.org/10.5172/conu.2006.23.1.3

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). The 2005 CSI/FBI Computer Crime and Security Survey. *Computer Security Journal*. https://doi.org/10.12957/reuerj.2016.11637

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75–81. https://doi.org/10.1016/j.giq.2008.03.003

Gray, D. E. (2014). *Doing Research in the Real World (3rd ed.)*. *SAGE*.

Greiner, L. (2018). Capabilit Maturity Model Integration (CMMI) Definition and Solutions, (Cmmi), 1–10. Retrieved from https://www.cio.com/article/2437864/process-improvement/capability-maturity-model-integration--cmmi--definition-and-solutions.html#Where did it come from

Groot, J. De. (2019). The History of Data Breaches. Retrieved from https://digitalguardian.com/blog/history-data-breaches

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*(March), 165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013

Häring, I. (2015). Risk Analysis and Management: Engineering Resilience. https://doi.org/10.1007/978-981-10-0015-7

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). ISMS Core Processes: A Study. *Procedia Computer Science*, *100*(1877), 339–346. https://doi.org/10.1016/j.procs.2016.09.167

Heilmann, H., & Kneuper, R. (2003). CMM(I) - Capability Maturity Model (Integration). Ein Rahmen zur Gestaltung von Softwareentwicklungsprozessen. *HMD -- Praxis Wirtschaftsinformatik*.

Heschl, J. (2006). *COBIT Mapping - Overview of International IT Guidance*. Retrieved from http://infosec.unige.ch/secu/method et droit/Cobit-compared.pdf

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*. https://doi.org/10.2307/25148625

Hewlett, P. (2007). The HP Business Intelligence Maturity Model. Retrieved from http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA1-5467ENW&cc=us&lc=en

Holland, C. P., & Light, B. (2001). A Stage Maturity Model for Enterprise Resource Planning Systems Use. *SIGMIS Database*, *32*(2), 34–45. https://doi.org/10.1145/506732.506737

Hu, Q., Hart, P., & Cooke, D. (2007). The Role of External and Internal Influences on Information Systems Security - a Neo-institutional Perspective. *J. Strateg. Inf. Syst.*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Hyde, K. F. (2000). Recognising deductive processes in qualitative research. *Qualitative Market Research: An International Journal*. https://doi.org/10.1108/13522750010322089

Institute, P. (2018). *2018 Cost of Data Breach Study, Global Overview*. *IBM Security*.

International Organization for Standardization. (2014a). ISO. 2013. ISO/IEC 27001 – Information security management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Organization for Standardization. (2014b). ISO 27000 Directory. Retrieved from http://www.27000.org/background.htm

ISACA. (2006). *CISA review manual 2007*.

ISACA. (2007). CoBIT 4.1. *IT Governance Institute*, 1–29. https://doi.org/10.1016/S0167-4048(97)84675-5

ISACA. (2013). *COBIT: A Business Framework for the Governance and Management of Enterprise IT*. *COBIT*.

Islamia, J. M., & Delhi, N. (2018). Comparative Study of Big Ten Information Security Management System Standards, *5*(2), 5–14.

ISO/IEC 27001:2013. (2013). Information Technology — Security Techniques — Information Security Management Systems — Requirements. *International Organization for Standardization*. https://doi.org/10.1109/IEEESTD.2005.339589

Johnson, A. (2011). Guide for Security-Focused Configuration Management of Information Systems. *Nist*, (August), 1–88. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-128

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*. https://doi.org/10.1145/1435417.1435446

Jones, J. A. (2005). An Introduction to Factor Analysis of Information Risk. *Risk Management Insight*. https://doi.org/10.1037/h0038787

Joseph C. Giarratano, G. D. R. (2004). *Expert Systems: Principles and Programming, Fourth Edition 4th Edition*.

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2017). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information and Management*, (January), 0–1. https://doi.org/10.1016/j.im.2017.09.003

Kadam, A. (2012). The Evolution of COBIT. *CSI Communications*, 21–22.

Kaplan, B., Duchon, D., & Study, A. C. (1988). Combining Qualitative and Quantitative Information Systems, *12*(4), 571–586.

Kent Crawford, J. (2006). The project management maturity model. *Information Systems Management*, *23*(4), 50–58. https://doi.org/10.1201/1078.10580530/46352.23.4.20060901/95113.7

Khaiata, M., & Zualkernan, I. A. (2009). A simple instrument to measure IT-Business alignment maturity. *Information Systems Management*, *26*(2), 138–

152. https://doi.org/10.1080/10580530902797524

Kneuper, R. (2017). Sixty years of software development life cycle models. *IEEE Annals of the History of Computing*. https://doi.org/10.1109/MAHC.2017.3481346

Kothari, C. (2004). *Research Methodology: Methods and Techniques*. *Vasa*. https://doi.org/http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf

Lapke, M., & Dhillon, G. (2006). A semantic analysis of security policy formulation and implementation: A case study. In *Association for Information Systems - 12th Americas Conference On Information Systems, AMCIS 2006*.

Lee, M. (2014). Information Security Risk Analysis Methods and Research Trends : AHP and Fuzzy Comprehensive Method. *International Journal of Computer Science & Information Technology (IJCSIT)*, *6*(February), 29–45. https://doi.org/10.5121/ijcsit.2014.6103

Leech, N. L., & Onwuegbuzie, A. J. (2009). A typology of mixed methods research designs. *Quality and Quantity*. https://doi.org/10.1007/s11135-007-9105-3

Lewis, J. R. (1995). IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use. *International Journal of Human-Computer Interaction*. https://doi.org/10.1080/10447319509526110

Littlewort, G., Whitehill, J., Wu, T. F., Butko, N., Ruvolo, P., Movellan, J., & Bartlett, M. (2011). The motion in emotion A CERT based approach to the FERA emotion challenge. In *2011 IEEE International Conference on Automatic Face and Gesture Recognition and Workshops, FG 2011*. https://doi.org/10.1109/FG.2011.5771370

Lloyd, V., & Rudd, C. (2011). 2 ITIL V3 SERVICE DESING (SD. *The Office of Government Commerce*. https://doi.org/10.1016/j.im.2003.02.002

Lu, J. (2017). Multi-model Data Management : What ’ s New and What ’ s Next ?, 4–7.

Luftman, J. N. (2003). Assessing Strategic Alignment Maturity. In *Competing in the Information Age: Align in the Sand: Second Edition*. https://doi.org/10.1093/0195159535.003.0002

Macedo, F. N. R. (2009). Models for Assessing Information Security Risk, 1–64.

Maiwald, E., Osborne, M., Brownlow, J., Acker, E., Wald, L., Mueller, M., … Weeks, J. (2002). *Security Planning & Disaster Recovery*. *Security Management*.

Mattord, H. J. (2008). Rethinking risk-based information security. https://doi.org/10.1145/1409908.1409921

Maule-Ffinch, B. (2015). Key trends in information security. *Network Security*, *2015*(11), 18–20. https://doi.org/10.1016/S1353-4858(15)30102-1

Mcafee.com. (2018). Top cybersecurity threats.

McAfee. (2017). 2017 Threats Predictions, (November 2016), 39.

McCumber, J. (2004). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology* (1st ed.). Boston, MA, USA: Auerbach Publications.

McKinsey. (2014). From Bottom to Top: Turning Around the Top Team. *McKinsey Quarterly*, (November 2014), 9.

Mettler, T. (2009). *A Design Science Research Perspective on Maturity Models in Information Systems*. St. Gallen: Institute of Information Management, Universtiy of St. Gallen. Retrieved from https://www.alexandria.unisg.ch/214531/

Montesino, R., & Fenz, S. (2011a). Automation possibilities in information security management. *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011*, 259–262.

https://doi.org/10.1109/EISIC.2011.39

Montesino, R., & Fenz, S. (2011b). Information Security Automation: How Far Can We Go? (pp. 280–285). https://doi.org/10.1109/ARES.2011.48

Morin, B., Thomas, Y., & Debar, H. (2006). Improving security management through passive network observation. In *Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006*. https://doi.org/10.1109/ARES.2006.74

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information and Management*, *52*(1), 123–134. https://doi.org/10.1016/j.im.2014.10.009

Ngwum, N. I. (2016). Information Security Maturity Model (ISMM) Information Security Maturity Model A dissertation submitted to The University of Manchester, (February), 1–136. https://doi.org/10.13140/RG.2.1.2432.8729

Nieles, M., & Dempsey, K. (n.d.). An Introduction to Information Security An Introduction to Information Security.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology*, 1–41. https://doi.org/10.1109/JPROC.2011.2165269

Open Group. (2011). Open Group Standard Open Information Security Management Maturity Model. *ISM3 Consortium*. Van Haren Publishing.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*. https://doi.org/10.2753/MIS0742-1222240302

Petr Komarevtsev. (2018). *FINANCIAL CYBERTHREATS IN 2017 Introduction and Key Findings*.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity Models

in Information Systems Research: Literature Search and Analysis. *Communications of the Association for Information Systems*, *29*(1), 506–532.

Radack, S., & Kuhn, D. (2011). Managing Security: The Security Content Automation Protocol. *IT Professional*, *13*, 9–11. https://doi.org/10.1109/MITP.2011.11

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2006). All You Need to Know About Research Methodology.

Rigon, E. A., & Westphall, C. M. (2013). Information Security Maturity Assessment Model. *Revista Eletrônica de Sistemas de Informação*, *12*(01), 3. https://doi.org/10.5329/RESI.2013.1201003

SANS. (2008). Information Security Resources. Retrieved from https://www.sans.org/information-security/

Sarah Beals, Carol Fox, S. M. (n.d.). Why a mature ERM effort is woth the investement. *Executive Report*, 5.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students Fifth edition. In *Research Methods for Business Students Fifth edition*. https://doi.org/10.1017/CBO9781107415324.004

Saunders, Mark, & Thornhill, A. (2016). *3rd Research Methods for Business Students*. *Research Methods for Business Students*.

Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World* (1st ed.). New York, NY, USA: John Wiley & Sons, Inc.

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked World*. *Wiley*. https://doi.org/10.1109/MSPEC.2000.873914

Seebauer, M. (2011). Expert system for optimization of food consumption in Intelligent Home. https://doi.org/10.1109/SAMI.2011.5738885

SEI. (2010). *CMMI for Development, Version 1.3*. *Carnegie Mellon University*,

Software Engineering Institute.

Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, *18*(1), 45–52. https://doi.org/10.1016/j.jisa.2013.07.002

Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. *International Journal of Security and Its Applications*.

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the effectiveness of ISO 27001:2013 based on annex A. *9th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2014)*, (Fares), 259–264. https://doi.org/10.1109/ARES.2014.41

Sihwi, S. W., Andriyanto, F., & Anggrainingsih, R. (2016). An expert system for risk assessment of information system security based on ISO 27002. *2016 IEEE International Conference on Knowledge Engineering and Applications, ICKEA 2016*, (September), 56–61. https://doi.org/10.1109/ICKEA.2016.7802992

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M. (2002). Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria. *Information Management & Computer Security*, *10*(5), 210–224. https://doi.org/10.1108/09685220210446560

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006

Solomon, M. G., & Chapple, M. (2005). *Information Security Illuminated*. USA: Jones and Bartlett Publishers, Inc.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sophia Wright. (2014). How Can Risk Maturity Model Benefit Your Risk Management. Retrieved from https://www.riskmethods.net/en/blog/How-Can-Risk-Maturity-Model-Benefit-Your-Risk-Management/112

Standardization, I. O. for. (2009). ISO 31000:2009 Risk Management Standard - Principles and Guidelines.

Stantchev, V., & Stantcheva, L. (2012). Extending Traditional IT-Governance Knowledge Towards SOA and Cloud Governance. *International Journal of Knowledge Society Research (IJKSR)*, *3*(2), 30–43. https://doi.org/10.4018/jksr.2012040103

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/https://doi.org/10.1016/j.cose.2004.07.001

Stevanovi, B. (2011). Maturity Models in Information Security. *International Journal of Information and Communication Technology Research*, *1*(2), 44–47.

Stine, K., Barker, W. C., & Gulick, J. (2008). Volume I : Guide for Mapping

Types of Information and Information Systems to Security Categories, *I*(August).

Stoll, M. (2014). An information security model for implementing the new ISO 27001, 216–238. https://doi.org/10.4018/978-1-4666-7381-6.ch011

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2010.07.006

Sun Microsystems. (2005). Information lifecycle management maturity model, (April), 1–8. Retrieved from http://dynamicsystemsinc.com/Downloads/Sun_ILM_Maturity_Model_2005.pdf

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards : A Comparative Study of the Big Five, (October).

Talabis, M., & Martin, J. (2012). *Information Security Risk Assessment: Risk Assessment*. *Information Security Risk Assessment Toolkit*. https://doi.org/http://dx.doi.org/10.1016/B978-1-59-749735-0.00005-1

Tapia, R. S., Daneva, M., Van Eck, P., & Wieringa, R. (2008). Towards a business-IT aligned maturity model for collaborative networked organizations. *Enterprise Distributed Object Computing Conference Workshops*, *12*, 276–287. https://doi.org/10.1109/EDOCW.2008.59

The University of Adelaide. (2009). Risk Management Handbook. *Annals of Physics*, *54*(2009), 258. Retrieved from http://www.adelaide.edu.au/legalandrisk/docs/resources/Risk_Management_Handbook.pdf%0Ahttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title+Avail#0

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*.

https://doi.org/10.1177/1098214005283748

Top 5 Cybersecurity Threats to Watch Out for in 2017 - An Infographic. (2018). Retrieved from https://www.slideshare.net/an.raja/top-5-cybersecurity-threats-to-watch-out-for-in-2017-an-inapp-infographic

Tsai, B.-Y., Stobart, S., Parrington, N., & Thompson, B. (1997). Iterative design and testing within the software development life cycle. *Software Quality Journal*, *6*(4), 295–310. https://doi.org/10.1023/A:1018528506161

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, Processes and Relational Mechanisms for IT Governance. *IGI Global*, 1–36. https://doi.org/10.4018/978-1-59140-140-7.ch001

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems*, *29*(4), 263–290. https://doi.org/10.2753/MIS0742-1222290410

Vancouver Coastal Health (VCH). (2016). Information security. *Computer Law & Security Review*, *11*(5), 292. https://doi.org/10.1016/S0267-3649(00)80072-2

von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security*, *19*(7), 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

Von Solms, B., & Von Solms, R. (2005). From information security to...business security? *Computers and Security*, *24*(4), 271–273. https://doi.org/10.1016/j.cose.2005.04.004

Wangen, G. (2017). Information Security Risk Assessment: A Method Comparison. *Computer*. https://doi.org/10.1109/MC.2017.107

Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, 1–19. https://doi.org/10.1007/s10207-017-0382-0

Webster, M. (2014). No Title. Retrieved from http://www.merriam-webster.com/.

Wei, Y. C., Wu, W. C., & Chu, Y. C. (2017). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing*, *279*, 48–53. https://doi.org/10.1016/j.neucom.2017.05.106

WESELY, P. M. (2011). Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences by TEDDLIE, CHARLES, & ABBAS TASHAKKORI. *The Modern Language Journal*, *95*(1), 152–153. https://doi.org/10.1111/j.1540-4781.2011.01158.x

Whitman, M. E., & Mattord, H. J. (2012). Legal, Ethical, and Professional Issues in Information Security. *Priciples of Information Security*. https://doi.org/10.1016/j.jpeds.2008.05.010

Wieringa, R. J. (2014). *Design science methodology: For information systems and software engineering*. *Design Science Methodology: For Information Systems and Software Engineering*. https://doi.org/10.1007/978-3-662-43839-8

Wiesmann, a, Stock, a Van Der, Curphey, M., & Stirbei, R. (2005). A guide to building secure web applications and web services. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Guide+to+Building+Secure+Web+Applications+and+Web+Services#2

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *28*(3), 1846–1852. https://doi.org/10.1016/j.ifacol.2015.06.355

Woodhouse, S. (2008). An ISMS (Im)-Maturity Capability Model. In *2008 IEEE 8th International Conference on Computer and Information Technology Workshops* (pp. 242–247). https://doi.org/10.1109/CIT.2008.Workshops.46

Wright, S. (2006). Measuring the Effectiveness of Security using ISO 27001.

Information Warfare Site, 1–15.

Yadav, N. (2019). ISO 27001 vs. COBIT: A comparison. Retrieved from https://advisera.com/27001academy/blog/2019/05/06/cobit-vs-iso-27001-how-much-do-they-differ/

Yazar, Z. (2002). *A Qualitative Risk Analysis and Management Tool - CRAMM*. *SANS Reading Room*. https://doi.org/10.4271/2018-01-1164.Abstract

Yin, R. K. (2014). *Case study research: Design and methods (5th ed.). Thousand Oaks, CA: SAGE Publications*.

Publications of the candidate

B Abazi, A Kő (2019)
Semi-automated information security risk assessment framework for analyzing enterprises security maturity level. CONFENIS 2019 International Conference on Research and Practical Issues of Enterprise Information Systems, **Lecture Notes in Business Information Processing**

A Luma, B Abazi (2019)
The Importance of Integration of Information Security Management Systemes (ISMS) to the Organization's Enterprise Information System. 42nd International Convention on Information and Communication Technology – **IEEE Conference**

Blerton Abazi, Besnik Qehaja, Edmond Hajrizi (2019)
Application of biometric models of authentication in mobile equipment 19th IFAC Conference on Technology, Culture and International Stability TECIS 2019

Besnik Qehaja, Blerton Abazi, Edmond Hajrizi (2019)
Enterprise Technology Architecture solution for eHealth System and implementation Strategy
19th IFAC Conference on Technology, Culture and International Stability TECIS 2019

B Abazi, E Hajrizi (2018)
Research on the importance of training and professional certification in the field of ICT Case Study in Kosovo. IFAC-PapersOnLine 51 (30), 336-339

A Luma, B Selimi, B Abazi (2018)
Registration and Authentication Cryptosystem Using the Pentor and UltraPentor Operators. International Conference on Engineering Technologies, 97-101

A Luma, B Abazi, B Selimi, M Hamiti (2018)
Comparison of Maturity Model frameworks in Information Security and their implementation. International Conference on Engineering Technologies, 102-104

B Abazi (2018)
An approach to Information Security for SMEs based on the Resource-Based View theory International Journal of Business and Technology 6 (3), 1-5

Abazi, B. (2016)
An approach to the impact of transformation from the traditional use of ICT to the Internet of Things: How smart solutions can transform SMEs. IFAC-PapersOnLine, 49(29), 148-151.

B Abazi (2016)
The adoption of Free/Open Source CRM software to SME-s An approach to low cost oriented solutions. 5th International Conference on Information Systems and Security

B Abazi (2016)
The implications of Information security to the Internet of Things. JOURNAL OF NATURAL SCIENCES AND MATHEMATICS OF UT (JNSM) 3 (2), 86-90

Acronyms

The following is a collection of acronyms with explanation used throughout the dissertation:

IT	Information Technology
ICT	Information and communication Technologies
ISO	International Standardization Organization
SSO	Single Sign-On
ISMS	Information Security Management Systems
SANS	SysAdmin, Audit, Network, and Security
DoS	Denial of Services
CIA	Confidentiality, Integrity, Availability
ATM	Automated Teller Machine
COBIT	Control Objectives for Information and Related Technologies
SSE	CMM - System Security Engineering Capability Maturity Model
ISM3	Information Security Management Maturity Model
NIST	National Institute of Standards and Technology
CMMI	Capability Maturity Model Integration
ISRA	Information Security Risk Assessment
SOA	Service-Oriented Architecture
ITIL	Information Technology Infrastructure Library
FAIR	Factor Analysis of Information Risk
OCTAVE	Operationally Critical **Threat**, Asset and Vulnerability **Evaluation**
CURF	Core Unified **Risk** Framework
CRAMM	CCTA **Risk** Analysis and Management Method
FAIR	Factor Analysis of Information Risk
CVSS	Common Vulnerability Scoring System
DSRM	Design Science Research Methodology
ASQ	After-Scenario Model
TAM	Technology Acceptance Model
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
AES	Advanced Encryption Standard
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
CISO	Chief Information Security Officer
HTML	Hypertext Markup Language
PHP	General-purpose programming language
MySQL	Open-source relational database management system (RDBMS)