Jari-Pekka Peltonen

Roadmap to Information Security

Theoretical study about information security with the views of practitioners

School of Technology and Innovations
Master Thesis in Computer Science
Digital Business Development

Vaasa 2022

VAASAN YLIOPISTO
Akateeminen yksikkö Tekniikan ja innovaatio johtamisen yksikkö
Tekijä: Jari-Pekka Peltonen
Tutkielman nimi: Tiekartta tietoturvaan: Teoreettinen tutkimus tietoturvasta harjoittajien näkemysten kanssa
Tutkinto: Master of Science in Economics and Business Administration
Oppiaine: Digital Business Development
Työn ohjaaja: Ahm Shamsuzzoha
Valmistumisvuosi: 2022 **Sivumäärä:** 115

Tiivistelmä:
Tietoturvallisuus on tänä päivänä ehkäpä yksi kuumimmista aiheista ja saamme lukea ja kuulla mediasta erilaisia tarinoita siitä, kuinka tietoturva on pettänyt joissakin yrityksissä. Siitä on tullut yksi erittäin tärkeä toiminto yrityksissä, vaikka yritys itsessään ei tietoturva alalla toimisikaan. Suomalaisessa teollisuudessa on käynnissä vallankumous, jossa valmistusprosesseissa aletaan hyödyntämään digitalisointia, kuten esimerkiksi asioiden internettiä, aiempaa enemmän. Tämän muutoksen myötä liitettävyys laitteiden välillä kasvaa ja samalla tietoliikenne lisääntyy ja tämä osaltaan luo uusia haasteita tietoturvallisuuteen. Tässä tutkimuksessa luodaan teoreettinen viitekehys tiekartan luomiseksi parempaan tietoturvallisuuteen. Tutkimus pysyttelee käsitteellisellä ja analyyttisella tasolla ja siinä on johtamisen näkökulma. Työssä esitellään käytännönharjoittajien näkökantoja sekä SABSA® malli, joka on vähemmän tunnettu käytännönharjoittajien keskuudessa.

Teoria osuudessa käsitellään tämän työn kannalta tietoturvallisuuden keskeisimpiä käsitteitä. Sen tarkoituksena on luoda teoreettinen viitekehys, jonka pohjalta rakennetaan tiekartta parempaan tietoturvallisuuteen. Keskeisiä tietoturvallisuuden käsitteitä tässä työssä on, klassinen tiedon arvoon perustuva määritelmä, laajennettu tietoturvallisuuden määritelmä, tietoturvallisuuden arkaluontoisuuden luokittelu, tietoturvallisuuden osa-alueiden luokittelu, tietoturvallisuus strategia, tietoturvallisuus politiikka, standardit, menettelyt ja käytännöt, riskienhallinta, tietoturvallisuuden kontrollit, tietoturvallisuuden hallinnointi, tietoturvallisuuden arkkitehtuuri, tietoturvallisuuden johtaminen ja kulttuuri. Teoria osuudessa tehdään katsaus myös projektien eri hallinta menetelmiin tietoturvallisuuden näkökannalta ja siinä lähinnä käydään läpi niitä eroja, joita vesiputous ja ketterillä menetelmillä on. Lisäksi teoria osuudessa tehdään erikseen katsaus tietoturvallisuuden eri standardeihin, viitekehyksiin ja parhaisiin käytänteisiin. Teoria viitekehys muodostettiin kirjallisuus tutkimuksena ja empiirinen osuus koostuu haastattelujen litteroinneista sekä teoriaviitekehyksestä syntyneestä tiekartasta. Haastattelun avulla pyrittiin hakemaan parannuksia ja tarkistamaan muodostettua tiekarttaa ja löytämään niitä haasteita, joita sitä toteuttaessa kohdataan. Aineistona tässä tutkimuksessa on käytetty alan kirjallisuutta ja tieteellisiä artikkeleita sekä haastattelun tuloksia.

Keskeisiä havaintoja tutkimusta tehdessä oli se, että kirjallisuustutkimuksella pystytään muodostamaan tiekartta tietoturvallisuusjärjestelmän toteuttamiseen organisaatioissa. Tietoturvallisuuden johtamiseen ja toteuttamiseen on olemassa standardeja, viitekehyksiä ja parhaita käytänteitä ja juuri nämä ovat niitä olennaisia työkaluja, joita tietoturvallisuuden toteuttamisessa ja ylläpitämisessä tarvitaan. Näillä käsitteellisillä viitekehyksillä, kuten SABSA, ISO 27000, NIST SP8000 ja COBIT on mahdollista toteuttaa kokonaisvaltaisesti organisaation tietoturvallisuus. Projektinhallinnan eri menetelmät ovat niitä menetelmiä, joilla näitä tietoturvallisuuden käsitteellisiä viitekehyksiä, standardeja ja parhaita käytänteitä jalkautetaan organisaatioon.

AVAINSANAT: Tietoturva, Tietoturvastandardit, Tiekartta tietoturvaan

UNIVERSITY OF VAASA
Academic unit School of Technology and Innovation
Author: Jari-Pekka Peltonen
Thesis title: Roadmap to Information Security: Theoretical study about information security with the views of practitioners
Degree: Master of Science in Economics and Business Administration
Subject: Digital Business Development
Supervisor: Ahm Shamsuzzoha
Graduation year: 2022 **Pages:** 115

Abstract:
Information security is one of the hottest topics today, and we get to read and hear various stories in the media about how information security has failed in some companies. It has become an important function in companies. A revolution is underway in Finnish industry, in which digitalization, such as the Internet of Things, is being used increasingly in manufacturing processes. With this change, the connectivity between devices will increase and at the same time the communication will increase, and this will create new challenges into information security. This study provides a theoretical framework for creating a road map for better information security. The research remains at a conceptual and analytical level and has a management perspective. The work presents the views of practitioners and the SABSA® model, which is less well-known among practitioners.

The theory part deals with the key concepts of information security for this work. Its purpose is to create a theoretical framework and road map for better information security. The key concepts of information security in this work are, classical definition based on data value, extended definition of information security, classification of information security sensitivity, classification of information security components, information security strategy, information security policy, standards, procedures and practices, risk management, information security controls, information security management, information security architecture, information security management and culture. The theory section also reviews the different project management methods from an information security perspective and reviews the differences between waterfall and agile methods. In addition, the theory section provides a separate overview of different information security standards, frameworks, and best practices. The theoretical framework was formed as a literature study and the empirical part consists of the transcripts of the main parts of the interviews and the road map generated from the theoretical framework. The aim of the interview was to seek improvements and to review the road map and to identify the challenges it may faces when implementing it.

There are standards, frameworks, and best practices for managing and implementing information security, and these are the essential tools needed to implement and maintain information security. With these conceptual frameworks, such as SABSA, ISO 27000, NIST SP8000, and COBIT, it is possible to implement information security holistically in an organization. The different methods of project management are the methods which are used to implement these conceptual frameworks, standards, and best practices for information security into the organization.

KEYWORDS: Information security, Information security standards, Road map to information security

Table of Contents

1 Introduction 9

1.1 Background 11

1.2 Research focus 12

1.3 Problem domain and research question 12

1.4 Results 13

1.5 Method and strategy 13

1.6 Structure of thesis 14

2 Literature review 15

2.1 CIA triad 18

2.2 Expanded information security definition 19

2.3 Information sensitivity classification 21

2.4 Security of components in computing 22

2.4.1 Personnel security 24

2.4.2 Activity Security 25

2.4.3 Information security 25

2.4.4 Technology security 26

2.4.5 Network security 27

2.5 Information security strategy 28

2.6 Information security policy, standards and practices 29

2.6.1 Information security standards 34

2.7 Risk management in IS 36

2.8 Information security governance 37

2.9 Information security architecture 41

2.10 Information security controls 48

2.11 Management and culture theory in context of information security 51

3 Project management methodologies and IS standards & best practice methodologies 55

3.1 Review of different project management methodologies 56

3.2 Information security standards & best practices 57

4 Research design and methodology 59

5 Results of the research 63

5.1 Best standards and best practices for implementing and maintaining information security 63

5.1.1 Strategies 63

5.1.2 Policy 66

5.1.3 Standards 67

5.1.4 Practices, Procedures, and guidelines 67

5.2 Project management methods for implementing and maintaining information security? 68

5.3 Biggest challenges implementing and maintaining information security? 73

5.4 Biggest challenges in information security today and future? 75

5.5 Project management methods in information security, their role and importance 79

5.6 What is the role and importance of Risk Management in IS? 81

5.7 What is the role and importance of management in IS? 84

5.8 Role and importance of culture in IS 86

5.9 Lacks and improvement suggestions in IS standards and best practices 90

5.10 Other observations and managerial implications 92

5.11 Suggestion for the road map 95

5.11.1 Challenges of implementation of IS 98

5.11.2 Future research proposals 99

6 Discussion 100

7 References 105

Appendix: Interview questions 114

Figures

Figure 1. Information sensitivity taxonomy (Adapted from Raggad, 2010). 22

Figure 2. Security of an information system (adapted from Raggad, 2010). 23

Figure 3. Layers of strategy (adapted from Baskerville & Dhillon, 2008). 29

Figure 4. Security policy framework for information security (adapted from Rees, et al., 2003). 31

Figure 5. Policies, standards, and practices (adapted from Whitman & Mattord, 2012). 35

Figure 6. Components of Risk Management (adapted from Whitman & Mattord, 2012). 37

Figure 7. Main elements of information security management (adapted from von Solms, 1999). 39

Figure 8. IT security organizational aspects (adapted from von Solms, 1999). 41

Figure 9. SABSA® development process (adapted from Burkett, 2012). 42

Figure 10. The SABSA® Model for Security Architecture Development (Sherwood, et al., 2005). 43

Figure 11. Relationship between policy, risk analyses, and control framework (adapted from Purser, 2004). 51

Figure 12. Development of and IS culture (adapted from Hellriegel, et al., 1998 [da Veiga & Martins, 2017]). 54

Figure 13. Research process (adapted from Vuori, 2022). 60

Figure 14. Security culture. 87

Figure 15. Road map for information security. 97

Tables

Table 1. Cybersecurity threads (Malatras, et al., 2021) 11

Table 2. Personnel security safeguards categories (adapted from Raggad, 2010). 25

Table 3. Organizations features in adoption of ISG (Adapted from Harris, 2006, [Raggad, 2010]). 38

Table 4. Risk management options (von Solms, 1999). 39

Table 5. SABSA® questions in each layer (adapted from Sherwood, et al., 2005). 44

Table 6. The Operational Security Architecture (adapted from Sherwood, et al., 2005). 45

Table 8. SABSA® Matrix for security architecture (adapted from Burkett, 2012). 46

Table 9. The Operational Security Architecture Matrix (adapted from Sherwood, et al., 2005). 47

Table 10. Information security controls (adapted from Tipton & Krause, 2004). 50

Table 11. Summary of the Standards and best practices. 68

Table 12. Challenges when implementing and maintaining subject. 75

Abbreviations

ACE	Access control list
ACL	Access control entry (in an access control list)
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIA	Confidentially, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIS CSC	Center for Internet Security Critical Security Controls
CIS 20	Center for Internet Security 20
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technologies
DevSecOps	Development, Security, and Operations
DNA	Deoxyribonucleic Acid
EA	Enterprise Architecture
EISA	Enterprise Information Security Architecture
EISP	Enterprise Information Security Policy
GDPR	General Data Protection Regulation
GRC	Governance, Risk & Compliance
HR	Human resource
IS	Information Security
ICT	Information Communication and Technology
ID	Identifier
Industry 4.0	Fourth Industrial Revolution
IoT	Internet of Things
IT	Information Technology
ISAE 3000	International Standard on Assurance Engagements 3000
ISF	Information Security Forum
ISFM	Information Security Management Framework
ISG	Information Security Governance
ISO	International Organization for Standardization

ISSP	Issue Specific Security Policy
MOV	Measurable organizational value
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan Do Check Act
PM	Project Management
PMO	Project Management Office
PMP	Project Management Professional
Prince2	Projects in Controlled Environments
SABSA®	Sherwood Applied Business Security Architecture
SCM	Supply Chain Management
SCRUM	Scrum (Software development method)
SecOps	Security Operations
SOC 2	Service Organization Control 2
SysSP	System Specific Policy

1 Introduction

This chapter starts with basic discussion about information security to make its importance to companies clear. Threats that organizations face in digital security can be categorized into three classes. Network attacks, intrusion, and malicious software. Network attacks are done over the network. They can cause millions of dollars in damages by slowing the network performance, degrade online services and email. This can be done without breaching into the organizations IT system. These kinds of attacks can be such as Denial of service or Distributed denial of service. They disable computers by sending an overwhelming number of messages to them and when computers try to respond to these thousands of messages they often crash because their resources are over consumed (Austin & Darby, 2003).

Intrusions are different than network attacks because there the actual penetration to companies' IT systems is done. Intruders can steal usernames and passwords and sometimes it is possible to get those because of the flaws in the software code. After they are in, intruders enjoy the same rights of access and control over the system and resources as does the legitimate users. They can erase or alter data, steal information, damage web sites, or introduce them as company representatives. Intruders can use sniffer software to eavesdrop on conversations on the network and get more passwords. They can that way get other companies' passwords also and get into their IT systems too. One of the most difficult problems that come here, is the question "What precisely was done?" Hackers cover their tracks, and they can make subtle changes in the system and open obscure doors that may allow other hackers to access secretly in the system, or they can slightly alter data that is difficult to detect. They can deposit time bombs that are scheduled to explode in the future. They can also leave software that allows them to use the company's IT system to do other attacks (Austin & Darby, 2003).

The last of these three types of threats are malicious code, they are worms and viruses, there is no precise definition, but viruses need help replicating and propagating, they

rely on naive users to for example open an e-mail attachment. Worms do it automatically. Both types of malicious code move faster than any human hacker does. Their target can be random which makes them impossible to predict where they hit next. They both are often used to launch other strikes which make their potential for destruction enormous. Digital attacks especially when used in combination can cause severe damage to the company (Austin & Darby, 2003).

December 2020 software company called SolarWind became aware that it was attacked by one of its software systems. The malware was added to the signed version of the supplier's software. 18000 private government and private organizations were infiltrated by this malware. The malware was activated when the software was deployed in the target environment (Panetta, 2021). Finnish bank Osuuspankki's web services faced a cyberattack in January 2022. The disruption was caused by a volumetric attack on the application, in which the service was crashed with many application queries. This caused an error on the login pages of OP's website. According to Osuuspankki, personal data or money were never at risk (Iltasanomat, 2022).

European Union Agency for Cybersecurity lists threats in the report "Enisa security landscape." According to Malatras, Lella, Theocharidou, & Tsekmezoglou, (2021) there are eight prime threats, they are listed and explained in table 1. In addition to these eight prime threats ENISA lists the ninth threat, supply chain threats. There is a separate report about it, and it is called "Enisa supply chain threats." According to Garcia, Malatras, Lella, Theocharidou, Tsekmezoglou & Valeros, (2021) supply chain attacks have been increased since 2020, and it has become a greater concern than before. Probably because companies have built robust security systems, and cyber criminals are moving towards their suppliers looking for vulnerabilities. They have been able to cause significant impact in terms of reputation damages, downtime of the system, and monetary loses. SCM attacks has at least two attacks, and it is the combination of these attacks. Supplier is attacked first, and the purpose is to get access to its assets. The actual target can be their final

customer or another supplier. SCM attack is classified as one when both the customer and their supplier are the targets.

Table 1. Cybersecurity threads (Malatras, et al., 2021)

Thread	Description
Ransomware	Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Ransomware has been the prime threat during the reporting period, with several high profile and highly publicized incidents. The significance and impact of the threat of ransomware is also evidenced by a series of related policy initiatives in the European Union (EU) and worldwide.
Malware	Malware is software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The threat of malware has been consistently ranked high for many years, albeit at a decreasing rate during the reporting period of ETL 2021. The use of new attach techniques and some major wins for the law enforcement community have impacted the operations of relevant threat actors.
Cryptojacking	Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. With the proliferation of cryptocurrencies and their ever-increasing uptake by the wider public, an increase in corresponding cybersecurity incidents has been observed.
E-mail related threats	E-mail related attacks are a bundle of threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems. Interestingly and despite the many awareness and education campaigns against these types of attacks, the threat persists to a notable degree. In particular, the compromise of business e-mails and advanced sophisticated techniques in extracting monetary gains are on the rise.
Threats against data	This category encompasses data breaches/leaks. A data breach or data leak is the release of sensitive, confidential or protected data to an untrusted environment. Data breaches can occur as a result of a cyber-attack, an insider job, unintentional loss or exposure of data. The threat continues to be high, since access to data is a prime target for attackers for numerous reasons, e.g., extortion, ransom, defamation, misinformation, etc.
Threats against availability and integrity	Availability and integrity are the target of a plethora of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stand out. Strictly related to web-based attacks, DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages. The treat is consistently ranked high in the ENISA threat landscape, both because of its manifestation in actual incidents and its potential for high impact.
Disinformation – misinformation	Disinformation and misinformation campaigns are on the rise, spurred by the increased use of social media platforms and online media, as well as a result of the increase of people's online presence due to the COVID-19 pandemic. This group of threats is making its first appearance in the ETL; however, its importance in the cyber world is high. Disinformation and misinformation campaigns are frequently used in hybrid attacks to reduce the overall perception of trust, a major proponent of cybersecurity
Non-malicious threats	Threats are commonly considered as voluntary and malicious activities brought by adversaries that have some incentives to attack a specific target. With this category, we cover threats where malicious intent is not apparent. These are mostly based on human errors and system misconfigurations, but they can also refer to physical disasters that target IT infrastructures. Also attributed to their nature, these threats have a constant presence in the annual threat landscape and are a major concern for risk assessments.

1.1 Background

Actors in cybersecurity are getting better and finding more cunning ways to achieve their goals. The overall aim of this research is to make road map for better information/cyber security. This study has more management and strategic approach rather than explaining technical details. At the end purpose of this paper is not to create perfect instructions for information security, but the purpose is more to make journey of exploration into

information security and the actual road map is not the best giveaway in this paper and after all it is a living document. There are quite a lot of literature about information security, still there are need for new perspectives and that way increase awareness of information security.

1.2 Research focus

Existing literature has lot of research closer to tactical level solutions and not so much research about the business and the organizational aspect kind of approach or at least not enough. This study aims to take and emphasize those aspects and, in that way go sort of backwards in this issue. Topic has developed in interaction to the degree program and has been evolving over the time. Study will present various important concepts and conceptual frameworks related to information security. There are also expert interview transcripts in this paper, giving valuable insight from the world of information security. Purpose of this research is to create a theoretical framework from literature and create a road map for better information security and use expert interviews to complement the road map. Clear the role of project management in the context of information security. One goal is to increase the awareness of information security related issues.

1.3 Problem domain and research question

How to create company's information security structures? What are needed to do that? What kind of conceptual frameworks there are? These kinds of questions start to arise when considering company information security. There is no exact research question in this study, but as the name of this study mentions the road map for information security is the end goal of this study and therefore serves as a research question, what is needed and what is important there.

1.4 Results

This study will present key concepts related to information security. It will present some of the most important standards, project management methods, and practitioners' viewpoints of them. According to this research quite often standards and best practices are used parallel. Some frameworks are better when starting from zero and some works better in larger scale operations. Information security is not running by project management methods, information security must be integrated into projects such as quality or work safety issues are integrated into projects, and if there are a separate IS projects, it is recommended to use same methods that are used elsewhere in the company. Road map is a high-level overview of a significant business initiative, it is the glue that links strategy to tactics, it communicates strategy quickly and keeps employees on the same page. In order to keep it productive, it must be working document which is updated regularly. Road map in this study is meant to be like that. There are also main parts of the interview transcriptions in this paper. The reason they are included into this is that they provide valuable and interesting insights about information security and to most of the people such point of views is difficult to access.

1.5 Method and strategy

Research is qualitative and it is done as literature research by going through academical journals conference papers and books, literature review part is formed using search words such as "information security", "information security management", and "information security standards", and then collecting important concepts and aspects from search results into it. Based on the literature review the interview questions were made, they purpose is to complement and support theoretical framework and revise road map, and finding more practitioners view of IS, information security standards, challenges in IS, role of the project management, the risk management, the management, and the culture, in the context of IS. Lacks in the IS standards and the best practices. This

approach was chosen to bring practitioners viewpoint of these important aspects of the information security, which are often lacking from scientific literature.

1.6 Structure of thesis

There are seven chapters in this study. First chapter is the introduction chapter. Second chapter is the presentation of the information security management. Third chapter introduces the project management methodologies, and there is review about the different information security standards. Fourth chapter is about the research design. Fifth chapter is the result chapter where there are transcripts of the main parts of the eight interviews of the company security officers and suggestion for the road map and finally there is the sixth chapter which is the discussion chapter. Seventh chapter is for the references.

2 Literature review

Information security is a necessary factor when considering organizational success because organizations need to protect their information assets. Organizations public and private sector must struggle with the exploitation of their information security vulnerabilities, the internal and external threats live continuous evolution (Burkett, 2012). Companies have become increasingly dependent of their information and communication technologies. This is not just for their key operational purpose's companies are also gaining strategic advantages with ICT. Another thing is that organizations have increasingly become location independent as in the past they were just concentrating to one geographical area. ICT have changed their whole business models. Information technology development have changed the boundaries of the companies and because of that, it has increased the importance of the data and information. Information helps organizations to reach their aims and it helps managers to take better decisions (Dhillon, 2001).

In old business model information is usually processed in central location and this made it easier to protect, in other words to ensure the confidentiality. Also, the content and form of the information did not usually change, so it was easier to keep the integrity, and ensure the accessibility for authorized personnel. Maintaining CIA was mainly the information security management. The difference in nature of the organization and scope of information processing today has changed the information security, it is not just keeping confidentiality, integrity, and availability. Emphasis should be more in setting up responsibility, integrity of people, trustworthiness, and ethicality (Dhillon, 2001).

According to research of Fenz, Heurix, Neubauer, & Pechstein (2014) there are six challenges in IS risk management. Challenge 1 is asset and countermeasure inventory. According to Fenz, et al. [2014] it is suggested by Vose (2008) that everything connected to any component of information technology is asset, despite is it tangible or intangible. According to Fenz, et al. (2014) challenge 2 is assigning asset values, this has proven to be difficult. Also assessing value of small items such as email is virtually impossible.

Assessing values that are not monetary such as the system downtime losses are difficult to assess. Losses are not just monetary there are reputation and image losses also and those can be hard to assess and recover. Challenge 3 is failed predictions of the risk. Nature of the risk changes and that makes it in practice impossible to predict which assets are interest of an attacker. Some less important and ignored assets today may in future be interesting for the attacker. In addition defining risk might be problem. Risk can be defined as uncertainty of outcome (positive or negative), it can be also be defined as frequency and magnitude of the loss. Challenge 4 is the overconfidence. According to Fenz, et al. [2014] it is suggested by Rhee, Ryu, & Kim (2012) managers estimations tend to be far too optimistic. Combined with the time limits and the stress that decision makers are facing this overconfidence effect leads to the attitude where formalism is dismissed. Biases of the risks caused by the overconfidence effect goes to probabilities, threat and impact assessments.

Challenge 5 is the knowledge sharing. Accoring to Fenz, et al. [2014] it is suggested by Fang, Liang, & Jia (2011) that the knowledge sharing between organizations reduces cost of knowledge acquisition, it enhance synergy between them, innovation ability improves, and promoting overall competitiveness. According to Fenz, et al. (2014) in IS domain it is desirable to exhange information to reduce overlappings when developing information security and achieve higher quality when further developing existing approaches instead of inventing the wheel again. Challenge 6 is risk vs. cost trade-offs. According to Fenz, et al. [2014] it is suggested by Lee, Fan, Miller, Stolfo, & Zadok (2002) that usually risk management drives countermeasures and technical effectiveness is enforced to protect organization’s assets and minimize risks. Countermeasures costs should not exeed the cost of expected losses. This is often neglected. According to Fenz, et al. [2014] it is suggested by Cavusoglu, Mishra, & Raghunathan (2004) that cost of attacks are difficult to define, because they are not just financial there are also losses in trust, image and similar nonphysical organizational values. According to Fenz, et al. [2014] it is suggested by Jansen (2010) that management decisions must be bases on solid data and knowledge of and experience in security mechanism handling. Many managers lack

this knowledge, then either external consultant needs to be hired or security status needs data model must be so simple that inexperienced person is able to interpret it. This data can be provided by using security metrics it can be help in various aspects of IS, such as security controls effectiviness or efficiency of operations.

Information security is a business enabler which is bounded strictly to trust of the stakeholder, by creating value for an enterprise for example bringing competitive advantage or by addressing business risk. Today significance of information and technologies related to it is increasing in business and public life. There is growing need for mitigating information risk. This means protecting information and IT from threats that are constantly changing. Regulation in business landscape is increasing and this adds boards of directors' awareness of the criticality of information's and IT-related assets security (ISACA, 2012).

Information is subject that must be protected, like other important business subjects, it is especially important for the organizations business and that for it must be protected properly. This is especially important in constantly networking business environment. Because this increasing integration information is exposed now to increasingly and different kind of threats and vulnerabilities. Information can occur in different forms. It can be printed or written in paper, electronically stored, mail, or electronically transmitted, seen or heard in movies or spoken in conversation. Whatever form information is or how it is stored or transmitted, it should always be protected properly (Suomen Standardoimisliitto SFS ry, 2012).

Information security means protection of information from different kind of threats where the purpose is to ensure continuity of the business, minimize business risks and maximize profit from investments and business opportunities. Information security is achieved through implementation of proper safety mechanism system, which can form from procedures, processes, and software- and equipment operations. These safety mechanisms must be created and take into use, and they must be review and if necessary,

improve, so that organizations definitions for the security- and the business goals would be achieved. This should be done with the other business management processes (Suomen Standardoimisliitto SFS ry, 2012).

2.1 CIA triad

In the literature, and most of the companies it is accepted that goals of the security are what matters. Security goals that they have mainly adopted is called the CIA triad, which comes from confidentiality, integrity, and availability (Raggad, 2010). This definition is also sometimes called traditional value of information-based definition. The confidentially means that information systems information is only available to those who are authorized to use it (Hakala, Vainio, & Vuorinen, 2006). The aim of confidentially is to prevent unauthorized personnel to access information that is classified to be confidential (Raggad, 2010). This is important especially when the information concerned is for example sensitive information in a government context, an intellectual property, or a personal information (Richot, 2013).

Maintaining the confidentially includes protecting the information systems equipment and the data repositories, using passwords and user identification. Different kind of encryption methods are also suitable for securing the sensitive or especially valuable information (Hakala, Vainio, & Vuorinen, 2006). The integrity is widely understood as meaning that the information containing in the information system is accurate and it does not have any intentional or unintended errors (Hakala, Vainio, & Vuorinen, 2006). The integrity of the data aims to prevent corruption of information. The agent in this can be system, virus, or person. For example, student who want to access in the files to change course grade. Virus can corrupt information by modifying or deleting the files or the records (Raggad, 2010).

Integrity means that there is no corruption in data, or it can mean its overall consistency. If the integrity of data is compromised, it will create lack of trust if the data have been manipulated, changed, or deleted (Richot, 2013). Integrity is pursued mainly with the software programming solutions. Different kind of input restrictions, or input verifications are programmed into the applications, saving and data transfer operations are included check sums or hash values. In the equipment level the aim is to prevent errors by using for example error corrective memories or bus systems. In the telecommunication solutions error recognition and fault rectification mechanisms equipped protocols and equipment's are favored. Most of the encryption methods and products are suitable also for the maintaining integrity (Hakala, Vainio, & Vuorinen, 2006).

The availability means that the information on the information system is accessible and in correct format (Hakala, Vainio, & Vuorinen, 2006). Information must be made to be available to users as said in security policy and from where it resides (Raggad, 2010). The authorized information must be accessible when it is needed. If information is affected, it is then not accessible and authorized when needed, and availability has then been compromised (Richot, 2013). The availability is kept by taking care of that information and communications systems and equipment are sufficiently efficient and that used software are suitable as possible to processing date that is stored to them. Aim there is also automate the refining of the information as far as possible. User should be able to retrieve the information they want in proper format, as ready-made reports, or summaries (Hakala, Vainio, & Vuorinen, 2006).

2.2 Expanded information security definition

The classical information definition or CIA triad is insufficient because it does not consider enough owners or producers of the information, and it does not consider equipment's or information and communication systems value (Hakala, Vainio, & Vuorinen, 2006). CIA triad is suffering at least from two drawbacks. Firstly confidentially, integrity

and availability are not enough, there must be more goals added in information security. Secondly if the security management is not incorporated into the security model even with all the security goals added, this risk-driven model based on the extended CIA triad is not sufficient (Raggad, 2010).

Most common definition for the expanded definition concepts consists of five factors. First three confidentially, integrity and availability are from CIA triad and two additional factors are the authentication and the non-reputation (Raggad, 2010). The access control (authentication) refers to the methods that are used to restrict use of the information processing infrastructure. The actual restriction of the access to the information is part of the confidentially. It is important to the organization to prevent the access from the outsiders or the own personnel to use its equipment's or telecommunications systems for their own purposes. Unauthorized users overload the equipment and the telecommunication networks and so weaken their usability. Unauthorized use may also expose organizations information systems to the malware spreading, which leads to integrity and confidentially problems (Hakala, Vainio, & Vuorinen, 2006).

The authentication mechanism is verifying the identity of an agent, which can be human, or system, before it is granting access. Effective security management requires authentication. This can be implemented using user ID and password, biometrics, public key infrastructure, or smart card (Raggad, 2010). Non-reputation in legal terms refers party's intention to fulfill obligations that are accepted. In the information security this means that when transmission is done, both ends of cannot deny their involvement in there. This means that sender of sent information cannot deny sending of it and receiver of that information cannot deny receiving it, if from the beginning it is in fact received (Raggad, 2010).

The non-repudiation means the information systems capability to identify and store reliably system user's identification information. There are mainly two reasons to aim for the non-reputation. First reason is to ensure the origin of the information and the second

is to identify unauthorized use of existing information in cases where information system owner must consider legal actions against the system user. The non-reputation is usually conducted by using identification mechanisms that utilizes the cryptographic methods or using the biometric identifications. Most common methods for the cryptography-based user identification are exploiting smart cards or other small portable device where user identification and validity time of the certification is saved. Fingerprints and fundus of the eye identification are biometric identifications (Hakala, Vainio, & Vuorinen, 2006).

2.3 Information sensitivity classification

The ISO/IEC 27002 standard provides taxonomy for the information sensitivity. There are five classes of information they are: top secret, highly confidential, proprietary, internal use, and public. The top-secret data is extremely sensitive data and if any of this kind of data is divulged to an unauthorized person its consequences can be catastrophically to its owner. This level is highest level of sensitivity. The highly confidential information is not top secret, but it is extremely critical information. This kind of information is critical to organizations ongoing operations and if divulged to an unauthorized person it can harm organizations capability of the business continuity. The information that can be top secret are such as accounting information, new products, new business plans, and innovative technology (Raggad, 2010).

The proprietary information is something that is produced by in-house resources they can be hardware, method, or software. This kind of information can be such as design specifications, processes, and operational information. The internal use only information is confidential information, but it is not public information. If this kind of information gets public it can be nuisance for organizations management, there is no financial losses, or they are negligible. This kind of information can be such as announcements and minutes, internal correspondence, and periodic activity reports. The public information is public, and it does not bring any harm or undesirable consequences if

published. This kind of information can be such as web site information, ads, annual reports, and commercials. In figure 1 this taxonomy is shown (Raggad, 2010).

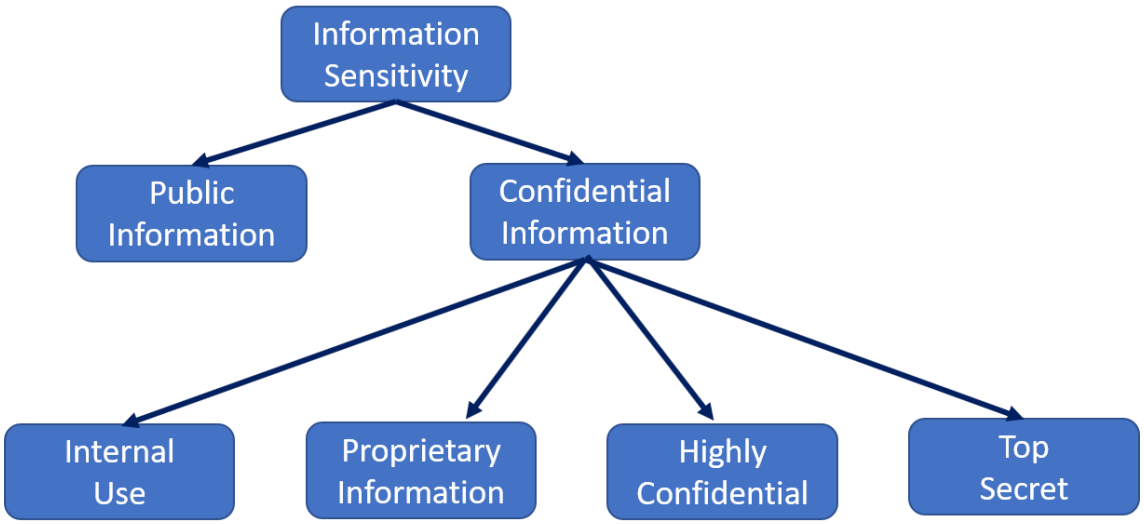

Figure 1. Information sensitivity taxonomy (Adapted from Raggad, 2010).

2.4 Security of components in computing

Security is quite often discussed without defining secured resources. Definition of security varies if security resources are not defined. This is because the definition of the information security is not necessarily the same as the definition of the network security or the personnel security. Resources that must be protected in computing environment can be defined to five main resources, they are: people, activities, data, technology, and network. Securing computing environment leads to secured enterprise. An information system is a defined computing environment, there the information is generated for user's needs. If we want to protect information, we must protect the information system components, they are forming together the information (Raggad, 2010).

So, if we want to protect information, computing environment, or information systems, we must protect networks, technology, data resources, system activities, and people. In the figure 2 there is information system illustrated with its five components: people, activities, technology, data, and network. Information security components must be secured to secure the information system itself, and with these terms information system security should be understood. Security of an information system is: 1. security of its people, 2. security of its activities, 3. security of its technology, 4. security of its data, 5. security of its network (Raggad, 2010).

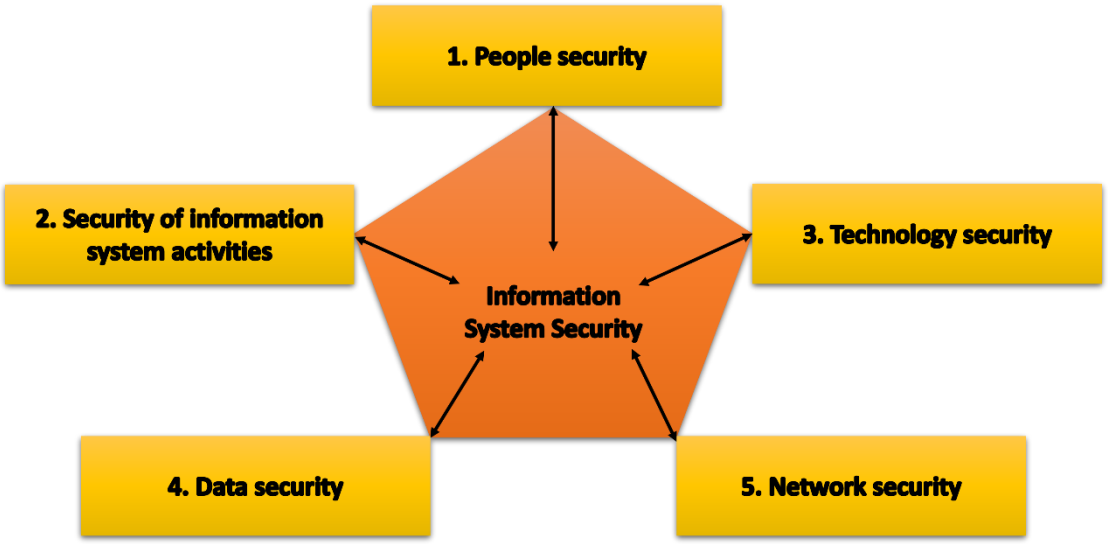

Figure 2. Security of an information system (adapted from Raggad, 2010).

Information security is often discussed meaning information system security or security of one of its components. Also, information security is discussed in terms of CIA components, information confidentiality, information integrity, and information availability. They are the most used terms for information security components in the literature. For example, purpose of implementing the policy and the procedures is to explain it to people and define to computers how interaction with other components must be done in the computer environment, so that the security aims are achieved (Raggad, 2010).

In the literature terms information assurance, computer security, information system security, and information security are used interchangeably. These can mean different

things, but there is no harm using them interchangeably if they are used to provide protection for confidentiality, integrity, and availability to the information in the given computer environment (Raggad, 2010).

Information is protected from unauthorized interactions and that is called as information security. Security policy defines unauthorized interactions of enterprises information resources. Information interactions are access to the information and use of it, destruction, modification, disruption, or disclosure. Security policies for the information systems are defined individually by each organization. Organizations transmit, process, and store vast amounts of confidential information, such as information about their partners, employees, customers, financial reports, and research and development (Raggad, 2010).

2.4.1 Personnel security

There will not be any security if prescribed activities are performed unsuccessfully to achieve planned security or wrong security mechanism is employed by a staff member. Information security is resulted from the work of people, processes, and activities. Planned security is not in place if tasks are performed by a staff member who is not trained for it. Insecurity can come from employees. Employee can unintentionally harm the system when making mistakes or employees may maliciously compromise the system. Therefore, we need personnel security; it is for preventing security problems such as mentioned. The personnel security refers to practices and tools which are used to ensure personnel safeguards usage by the human resources unit (Raggad, 2010). Safeguards for the personnel security can be classified in to five categories, they are presented in the table 2.

Table 2. Personnel security safeguards categories (adapted from Raggad, 2010).

Qualification assurance	Hiring is done only when person matches specifications and security clearance of the job in question. Qualification is easy to verified from candidates work experience and with technical testing. Security clearance is very difficult process.
Screening assurance	Throughly backround and screening checks are necessary to ensure that candidates with poor behavior cannot infiltrate in to the system. Security clearance stringency with association to sensitivity/condidentially of information accessibility of the position in question.
Authorizing of processes	When employee is hired, transferred, or duties are terminated, there has to be formal and auditable process for granting, modifiying, or revoking his or hers physical or system access.
Security training	Employees have access to security training programs in accordance with security requirements of the position they are holding.
Nondisclosure agreements	Nondisclosure agreements have to be assigned by employees who are involved in security matters and with appropriateness to their position in organization. Employees who need access to sensitive or confidential information have to sign nondisclosure agreement.

2.4.2 Activity Security

Interactions between components of the information system and between these components and its environment are governed with procedures, regulations, policies, standards, and protocols, these are called activities. Weaknesses in these activities can produce an undesired event which could lead in situation where security of the information system is compromised. Corruption in activities may damage the information system in a way that are unpredictable (Raggad, 2010).

2.4.3 Information security

To understand data, means that all the facts must be processed to information. On the other hand, information is the interpretation and meanings that user associates with those facts. That how the information is interpreted and applied to make the decisions is how good is the organizations capability to generate business value. The model for business success must define more accurately the business value generation. Organizations should incorporate novel approach for identifying and redefining the information

assets it has and whom without its planned business model would not work. With this innovative approach it should be possible to define all the conceptual resources into information which is possible to transform into value which then brings the business value (Raggad, 2010).

The conceptual resources are part of the computing environment, and they must be secured adequately. Raggard's taxonomy defines those conceptual resources as to be activities, data, the software part of the technology, physical resources which means people, network, and the hardware part of the technology. To prevent unauthorized disclosure or modification of the conceptual resources content and destruction of the information technology resources, they must be physically secured. Buildings, office space housing technology resources and the equipment that is used for the conceptual resources processing must meet the physical security requirements of the organization. Each of the facility's information technology equipment are protected, maintained and that way ensuring their continued availability by applying the security safeguards (Raggad, 2010).

Protecting information resources from the unauthorized access is information security. Information, data, and programs are conceptual resources, and they can be secured by using passwords and digital certificates, but password for example proves that right code is entered but not by whom. The digital certificates and the biometrics can be utilized to control access to the information resources. Still security can be compromised because of the other violations as eavesdropping can take place. It is also possible that persons who have been admitted to the system and has authentication commits unauthorized actions and compromise security by performing malicious actions (Raggad, 2010).

2.4.4 Technology security

Technologies are used to supports enterprises operations and security. Technology can be software or hardware, and if either one of these are compromised, their functions

will be compromised also. Enterprise's security will be compromised, and their operations is weakened. If the detection system for intrusion fails and software of hardware do not perform as it is intended. The result is that security administrator does not receive any information from real-time alert system and there is no actionable visibility to provide actionable information about intrusion. Consequences of this kind of situation might be dangerous (Raggad, 2010).

2.4.5 Network security

Any resources that are interconnected are called as a network and computer network is a system of interconnected computers. Network security aims to protect company's network from unauthorized modification, destruction, or disclosure. Its purpose is to provide assurance for performance of the security-related functions and ensure that the network security is not compromised. Any host-based security should not be taken granted, all aspects of the enterprise's networks must be secured. Every host-based security attribute must be reviewed and understand the effect of the network environment to them (Raggad, 2010).

Servers connected into the network might hold information on how to access the internal resources. Workstations connected into the network might be used attack other computers or they might contain malicious data. Any other network equipment such as routers, switches, bridges, hubs, etc. can be used as an access point into network. Intruders may exploit the network wiring and the media to access into network. They may use wireless access point to get into the internal network. Laptops taken outside of the company must be reviewed for malicious content (Raggad, 2010).

2.5 Information security strategy

Sometimes words strategy and policy are conflated. The definition of these two are similar (Baskerville & Dhillon, 2008). According to Baskerville & Dhillon [2008] Merriam-Webster (2001) defines strategy to be a “careful plan or method: the art of devising or employing plans or schemes towards a goal.” Policy is defined in similar way as to be: “a high level overall plan embracing the general goals and acceptable procedures.” Policy in more detail is defined to be “a definite course of actions selected from among alternatives and in light of given conditions to guide and determine decisions.” When they are defined like this, it is no surprise that these terms are sometimes entangled. To clarify term strategy we can use it at least in two ways, firstly when we are creating security polices, we can have strategy for that, and secondly for implementation of those policies we can have different strategy. In other words organizational strategy is used to determine security policies, and these policies will be carried out with the strategy how carrying out the security policies. Organizational-level strategies that are used to create the security policies are higher-level information security strategies (Baskerville & Dhillon, 2008). This is illustrated in figure 3.

According to Baskerville & Dhillon [2008] it is argued by Mintzberg, Ahlstrand & Lampel (1998) that plans made for attaining organizational missions and goals, which are called intended strategies are very rarely actually achieved as real strategies. Because of this there are two kind of ways how strategy is seen by strategy theorists. Strategy can be deliberate plan that is carried forward starting from intended strategy and which comes out as a realized strategy. The other way of seeing strategy is an emergent pattern which forms and continuously reforms it selfs in learning process, as organization is adapting into its environment.

These two different views of strategy quite often result very similar process in practice when strategy process is formulated. People who see strategy as a prescriptive design and planning process are seeing strategy process as a project where the goal is to deliver

organizational strategic plans. These groups of people focuses mainly one-shot process of strategy formulation. For these strategy framework is guide to strategy settings. They who see this as a prescriptive learning process, will think that this is changing experience where the goal of all this is to nurture and grow the organization. These people expect to repeat continuously the process and that it will change in every cycle. Strategy framework is example of how living strategy-settings process could be formulated or adapted (Baskerville & Dhillon, 2008).

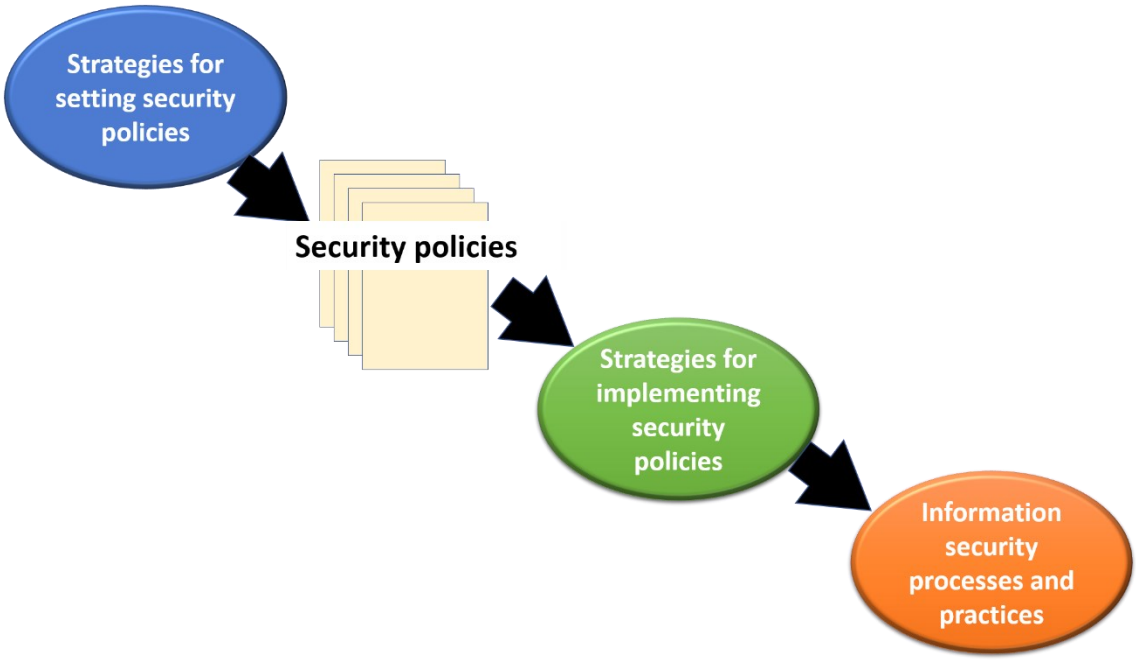

Figure 3. Layers of strategy (adapted from Baskerville & Dhillon, 2008).

2.6 Information security policy, standards and practices

Barman (2002) defines security policies to be a high-level plans where procedure goals are described. Policies are different than the guidelines or the standards, same goes for the procedure and the controls. In the policies security is described in general terms, not in specific way. They are the blueprints of the overall security program, it could be

compared same as product specifications are for the new product. According to Whitman & Mattord (2012) policies comment how technologies should be used and how issues should be addressed. Equipment, software or proper operation are not specified in the policies, information of these should be in the standards, in the procedures, and in the systems documentations and in the user manuals. “Policies should never contradict with law.” Policies can be significant liability to enterprises. Policies should also stand up in court if necessary. They should be administrated properly using dissemination and with the documented acceptance.

In the figure 4 there is a illustration of the policy framework. There are four main phases in the policy life cycle: Assess, Plan, Deliver, and Operate. This process is iterative and that is why there is a feedback loop in every stage back-forward. It ensures that requirements are satisfied in the previous steps. Policy assessment is either initiated after initial policy creation or for changing existing policy. When assessing the policy, existing policy, standards, guidelines, and procedures are also reviewed (Rees, Bandyopadhyay, & Spafford, 2003).

Process change is either strategical or tactical. Risk assessment phase is where organizations protected business asset are identified. Potential threats to those assets are also identified. In planning phase there are policy development and requirements definitions to be created or updated. Policy development must be in line with the existing business strategy and the policy. Requirements phase is where the security policy is analyzed so that requirements could be defined. In the deliver phase there are two steps. First step is to define the controls, they are practices, procedures or mechanisms which are used to reduce the security risks. In this step needs how to satisfy security policy requirements are defined. In the second step there is the implementation of the controls that are selected in previous step. Final security infrastructure is build, tested and implemented (Rees, et al., 2003).

Two steps of the operations phase are operations monitoring and trend reviewing and event managing. Purpose of monitoring operations is to define daily activities. They are done throughout the whole organization. This is because it must be ensured that security policy is enforced over the whole security infrastructure. There is no value of the security policy if it is not reviewed and updated constantly. In this activity events or trends which signal the need for re-evaluate security policy are identified. Events in the manage events step means situations which are outside from normal activity. This could be situation where some individual is looking for sports scores from web during business hours and is so violating acceptable use policy. All these steps have also sub-steps (Rees, et al., 2003).

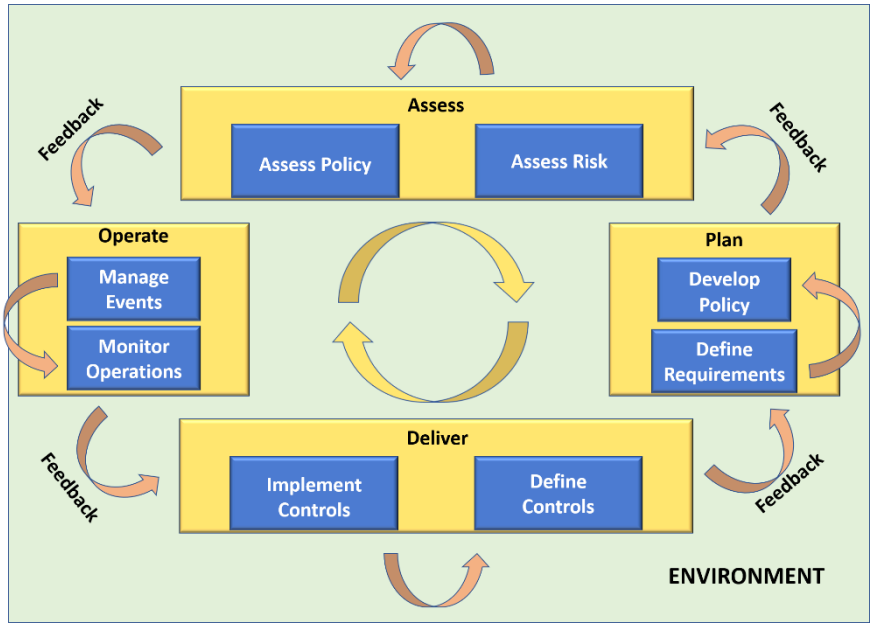

Figure 4. Security policy framework for information security (adapted from Rees, et al., 2003).

According to Whitman & Mattord (2012) Information security is not a technical problem, it is a management problem. It is a tool for management and it obligates personnel to function in a way that they protect information assets security. Security policy is most difficult to implement properly, but on the other hand it is cheapest to control. Its creation and dissemination requires management teams time and effort. Security controls are much more expensive to implement. Barman (2002) argues that policies do

not comment how to properly define what is protected or tell how to assure implementation of proper controls. Policies are telling what is to be protected and what kind of restrictions controls should have.

According to Whitman & Mattord (2012) policies are course of action or a plan whit whom organization's senior management conveys instructions to people who are making the decisions, taking actions, and performing other duties. In policies acceptable and unacceptable behavior within the organization is dictated, they are sort of organizations laws which are telling what is right and what is wrong, penalties for violation of policy, and process for appealing.

According to Whitman & Mattord [2012] it is suggested by National Institute of Standards and Technology (1996) there are three types of security policies that must be defined by the management:

1. Enterprise information security policies
2. Issue-specific policies
3. System-specific security policies

General security policy, organizational security policy, or IT security policy are also known as an enterprise information security policy (EISP). It is based on the mission, vision, and direction of the organization and it also supports it. EISP sets strategic direction, scope, and tone for all security efforts. EISP specific to organization and in its content varies depending the organization, but following documents should be in it:

- "An overview of corporate philosophy on security"
- "Information on the structure of the information security organization and individuals who fulfill the information security role"
- "Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)"
- security that are unique to each role within the organization" (Whitman & Mattord, 2012).

Issue-specific security policy (ISSP) is giving instructions to employees to use properly the technologies and processes which the organization is using to implement its operations. ISSP in generally firstly addresses specific technology areas, such as e-mail, use of internet, minimum configurations of computers against viruses and worms. ISSP can be created and managed with many different way within an organization. Most common three ways are:

- Independent, each ISSP document tailored to specific issue
- A single ISSP document, covering comprehensively all issues
- A modular document, ISSP has specific issue's requirements and it unifies policy creation and administration (Whitman & Mattord, 2012).

Systems-specific Policy (SysSP) looks often different than issue-specific policy, which are formalized as written document and is identifiable as policy, SysSP often work as a procedure or standard used when maintaining or configuring the system. SysSP can for example describe networks firewalls configuration and operation. In the document there can be statement of managerial intent, such as guidance for how to engineering networks, like firewalls selection, configuration, and operation. System-specific policy can be defined as two separate groups, technical specification and managerial guidance (Whitman & Mattord, 2012).

Managerial guidance in the system-specific policy is document created to guide technology implementation and configuration. It also addresses behavior of the people in way that it is supporting the security of information. For example implementing firewall needs a method which on the other hand falls into technical specification SysSP, but guidelines set by the management must be followed in the configuration. If management does not want employees to have access to internet from organizations network, it must be configured accordingly. Every system that affects on confidentiality, integrity, and availability of the information must be evaluated for trade-offs between restrictions and security (Whitman & Mattord, 2012).

To implement managerial guidance SysSP may require a policy, it is called technical specification SysSP. Each type of equipment will require own set of policies to translate management intent for technical control and then into an enforceable technical approach. ISSP for example can require that user passwords are changed at certain intervals. This can be done by implementing technical control and with application that enforces this policy (Whitman & Mattord, 2012).

2.6.1 Information security standards

Surprisingly the primary purpose of standards is to standardize something. We can name here three reasons why they are advantageous, first they reduce complexity, second when there is choice to be made standards document a preference, and thirdly standards help interoperability ensuring (Purser, 2004). In standards there are more detailed statements about what to do that policy is complied. Requirements for the compliance of standards is the same as policies. Standards can de facto standards, which are part of the organizational culture or they can be de jure standards which are formal and which group has published, scrutinized, and ratified (Whitman & Mattord, 2012).

According to Smallwood (2014) de jure standards are not formal, they are just thought to be. De jure standards comes from recognized standard-setting bodies such as American National Standards Institute (ANSI) or International Organization for Standardization (ISO). Organization can create standard for example for inappropriate-use. Where all inappropriate content will be blocked and including definitions for inappropriate content (for example pornography). It is in later in this process where actual technical controls and associated procedures are established. It is in practices, procedures, and guidelines where it is elaborated how employees must comply the policy (Whitman & Mattord, 2008). In figure 5 these relationships are illustrated.

Practices, procedures, and guidelines are described to be detailed steps which are needed to achieve requirements of standards. Procedures are instructions written down

for carrying out tasks. If person without authorization gets access to organization's procedures, then there is threat to information's integrity. For example, security weaknesses can be taken advantage by using its weaknesses such as authentication. Bank consultant whose procedures were available, one employee learned how to use procedure of wiring funds and wired millions of dollars to unauthorized account using computer centers procedures. If there is lax security, it can cause losses of tens of millions before it is corrected (Whitman & Mattord, 2012).

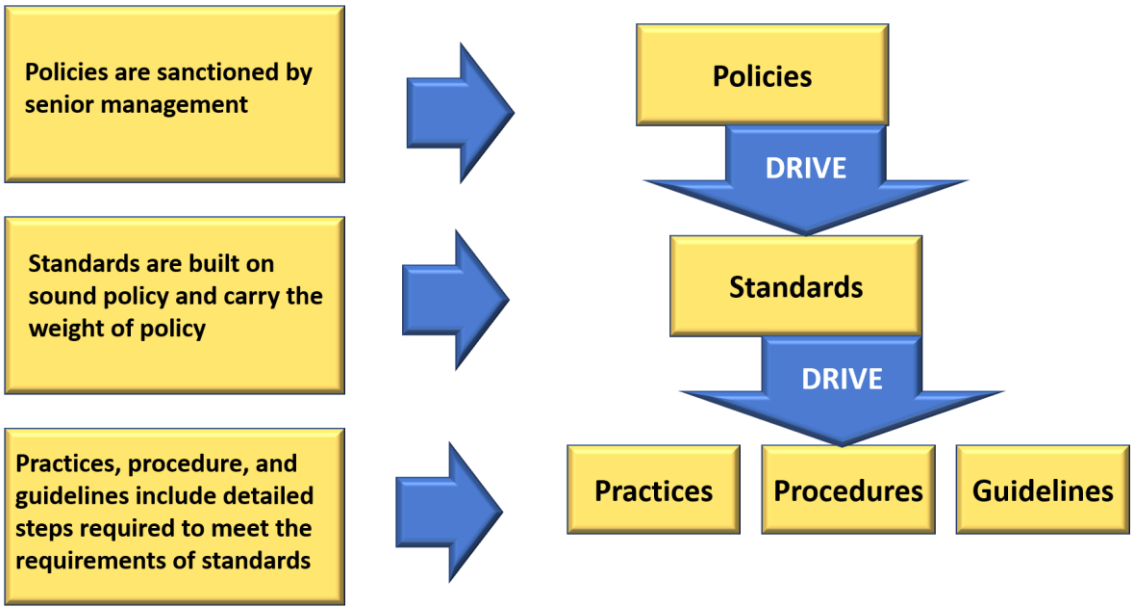

Figure 5. Policies, standards, and practices (adapted from Whitman & Mattord, 2012).

Organizations should not just concentrate to distributing procedures to legitimate employees but providing proper education to protect those procedures also. Safeguarding procedures is as important as securing information system. All critical information and procedures must be disseminated only on a need-to-know bases (Whitman & Mattord, 2012). Guideline is a set of administrative instructions, recommendations, or general statements which are designed to achieve policy aims. They provide framework for implementing procedures. They can change often depending on environment and must be reviewed more often than policies and standards. Guideline is suggested best practice. Guidelines helps user to understand security policy and help management and owners to understand security best practices. Relationship between policy, standards, and

guidelines is that policy is concerned about answering the question “why” aspects of computing behavior. Standards are answering the question “what,” and guidelines are answering to question “how” aspects of the security policy (Raggad, 2010). Practices or IT security practices (execution) can be thought as an execution of procedures to operative policy. It is sometimes called “an endpoint security problem.” It starts with training to achieve IT security policy awareness. Internal controls (behavioral, technical) support it. It is monitored, enforced with sanctions such as penalties and rewards (Baskerville & Dhillon, 2008).

2.7 Risk management in IS

According to Finne [2000] aim of risk management is defined by Caelli, Longley, Shain & Michael (1989) to “identify, measure and control uncertain events” and do this for pursuing to minimize loses and optimize invested money for security. When we are dealing with the security, it is not possible to achieve total risk elimination, this is because nature of information security and not all the risk are in the reach of the company. Risk management is in that way huge area (Finne, 2000). According to Venugopal (2010) in risk management there are two major tasks. They are risk assessment and risk treatment. Whitman & Mattord (2012) are defining risk management components as to be risk identification, risk assessment, and risk control. Risk identification consist of examination and documentation of risks that organization is facing and organizations information technology security posture. In risk assessment phase it is determined the extent of the organizations information assets are in risk or are exposing to it. in risk control phase control applications for reducing risks are set to protect the data and information systems. These relationships are shown in figure 6.

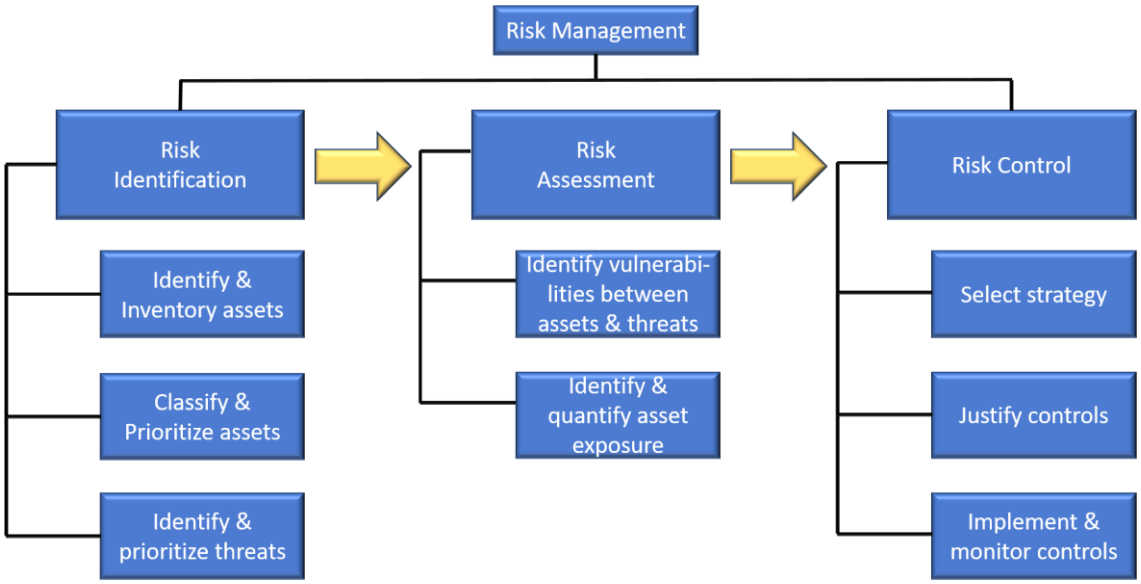

Figure 6. Components of Risk Management (adapted from Whitman & Mattord, 2012).

2.8 Information security governance

Governance can be described to be "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that enterprise's resources are used responsibly." In other words, governance describes the entire governing, or controlling process, which is used by the group to accomplish their objectives (Whitman & Mattord, 2012).

According to Raggad [2010] it is suggested by Harris (2006) "security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieve, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly". ISG effects can be demonstrated by comparing managerial profiles that are relevant to security with organization that has adopted ISG and organization that has not adopted ISG. In table 3 the features are listed.

Table 3. Organizations features in adoption of ISG (Adapted from Harris, 2006, [Raggad, 2010]).

Organization adopted ISG	Organization not adopted ISG
Board members understand that information security is critical to the company and demand to be updated quarterly on security performance and breaches.	Board members do not understand that information security is in their realm of responsibility, and focus solely on corporate governance and profits.
CEO, CFO, CIO and business unit managers participate in a risk management committee that meets each month, and information security is always one topic on the agenda to review.	CEO, CFO, and business unit managers feel that information security is the reponsibility of the CIO, chief information security officer (CISO), and IT department, and do not get involved.
Executive management set an acceptable risk level that is the basis for the company's security policies and all security activities.	The CISO employes boilerplate security policies, inserts his or her company's name, and has the CEO sign them.
Executive management holds business unit managers responsible for carrying out risk management activities for their specific business units.	All security activity takes place within the security department; thus, security works within a silo and is not integrated throughout the organization.
Critical business processes are documented along with the risks that are inherent in the various steps within the business processes.	Business processes are not documented and analyzed for potential risks that can affect operations, productivity, and profitability.
Employees are held accountable for any security breaches they participate in, either maliciously or accidentally	Policies and standards are developed, but no enforcement or accountability practices have been envisioned or deployed.
Security products, managed services, and consultants are purchased (or hired) and deployed in an informed manner. They are also constantly reviewed to ensure they are cost-effective.	Security products, managed services, and consultants are purchased (or hired) and deployed without any real research or performance metrics to be able to determine their ROI of effectiveness. Company has a false sense of security because it is using products, consultants, or managed services.
The organization is continuing to review its business processes, including security, with the goal of continuous improvement.	The organization does not analyze its performance for improvement, but continually marches forward and repeatedly makes the same mistakes.

Effective planning and managing IT security in an organization requires comprehensive IT security plan. Policy must be made and there considering IT security objectives, strategies, and other policies. This way top management is also showing their commitment to secure IT environment (von Solms, 1999). In figure 7 there is graphical illustration of main elements of information security management. There it all starts from corporate IT security policy it is followed by IT security organizational aspects, after that comes risk management part which holds corporate risk analysis strategic options, there are four different choices of options, they are baseline approach, informal approach, detailed risk analyses approach, and combined approach. These four choices are explained later in this chapter. Risk management holds also next three phases after corporate risk analysis strategic options phase. These three are first IT security recommendations phase, then second IT system security policy phase, and third IT security plan phase. After risk management starts implementation phase which holds two separate parts. First are the safeguards and second is the security awareness. After that follows follow up phase, which means monitoring all the previously mentioned steps.

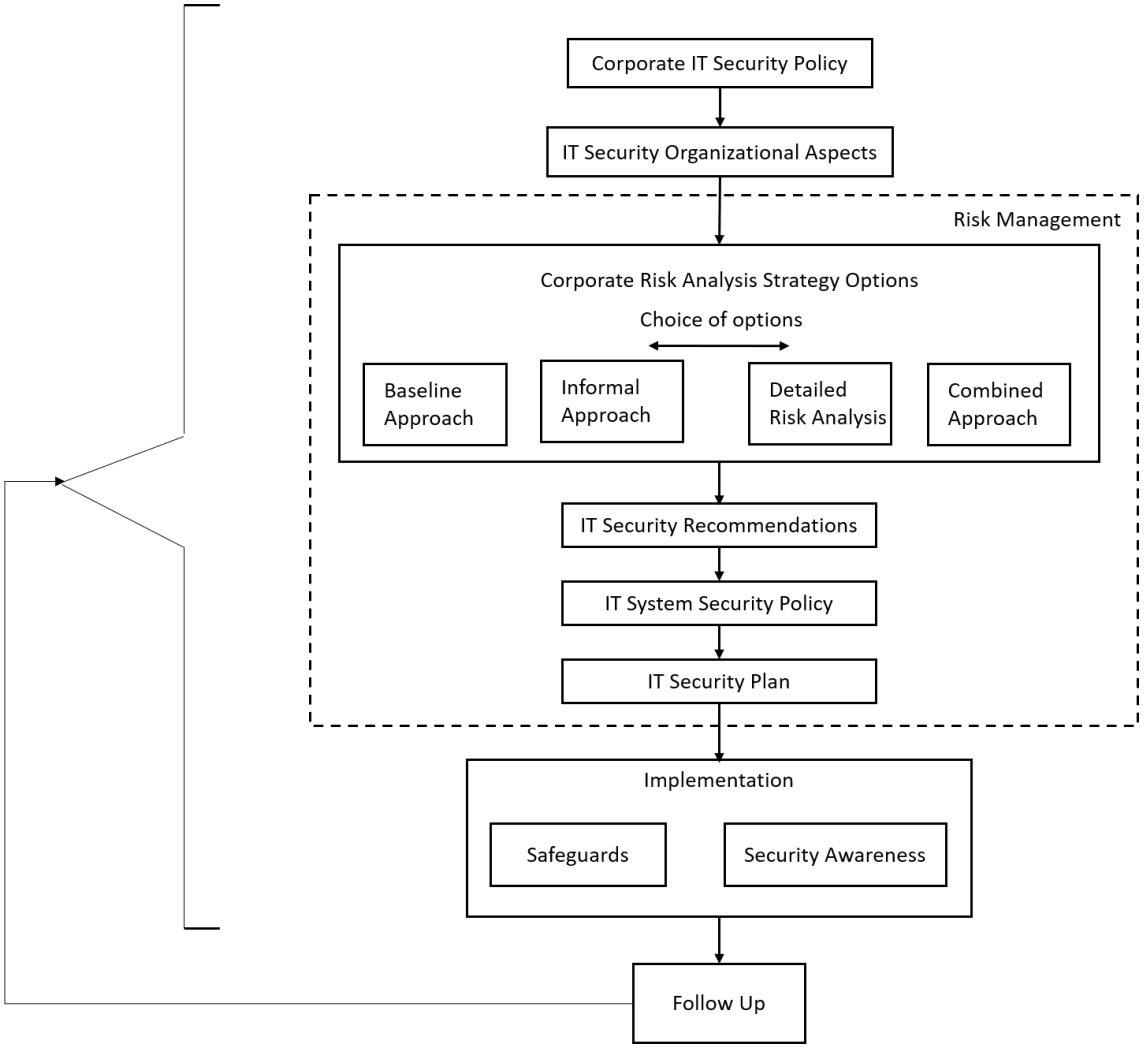

Figure 7. Main elements of information security management (adapted from von Solms, 1999).

Security risks are specific in different environment and therefore every organization needs to have strategy how to manage those security risks. We can name here four different options; these are presented in table 4.

Table 4. Risk management options (von Solms, 1999).

1.	A detailed risk analysis for all IT systems in the organization.
2.	An informal, pragmatic risk analysis using either internal or external security specialists.
3.	The baseline approach where an organization can suggest baseline (minimum) controls to all IT systems.
4.	A combined approach where a combination of these approaches are introduced to the various IT systems.

Security controls are recommended as a result of these four options. When security controls are successfully introduced, they will reduce security risks to acceptable level. To implement security controls effectively, IT security plan needs to be drafted. Plan must incorporate aspects such as operational costs of implementing safeguards, workloads, workforce, time schedules, etc. Then follows the actual implementation of the controls. It is important after implementation that there are operational and administrational procedures developed for supporting and enforcing the technical controls Following roles should be defined in every organization IT security forum, which approves standards and directives and resolves interdisciplinary issues, and corporate IT security officer, for focusing organizations all IT aspects (von Solms, 1999).

It is also important that there is security awareness program introduced in the organization which advocates information security policy and makes sure that operational and administrative procedures are understood and instills proper behavior. Introduced controls must be maintained to ensure their effective functioning. Ensuring the compliance with the IT security plan requires security audits or compliance checking. Incident reporting and investigation scheme needs to be there also, they are possible to integrate with the inter-organizational reporting schemes (von Solms, 1999). In the figure 8 there is the illustration of organizational aspects. There are the IT steering committee and IT security forum. Corporate level holds corporate management, corporate security officer, and corporate IT security officer. Corporate IT security officer has representation in IT steering committee and in IT security forum, it is also responsible of corporate IT security policy and directives. Corporate management has representation in IT steering committee. Department level holds department IT security officer which is also responsible of departments IT security policy and directives, it exits only if the department is sufficient size. Below there is the system/project level, it holds IT project or system security manager, which is also responsible of IT project or system security policy. IT steering committee and IT security forum has IT representatives and IT security forum has IT user representatives.

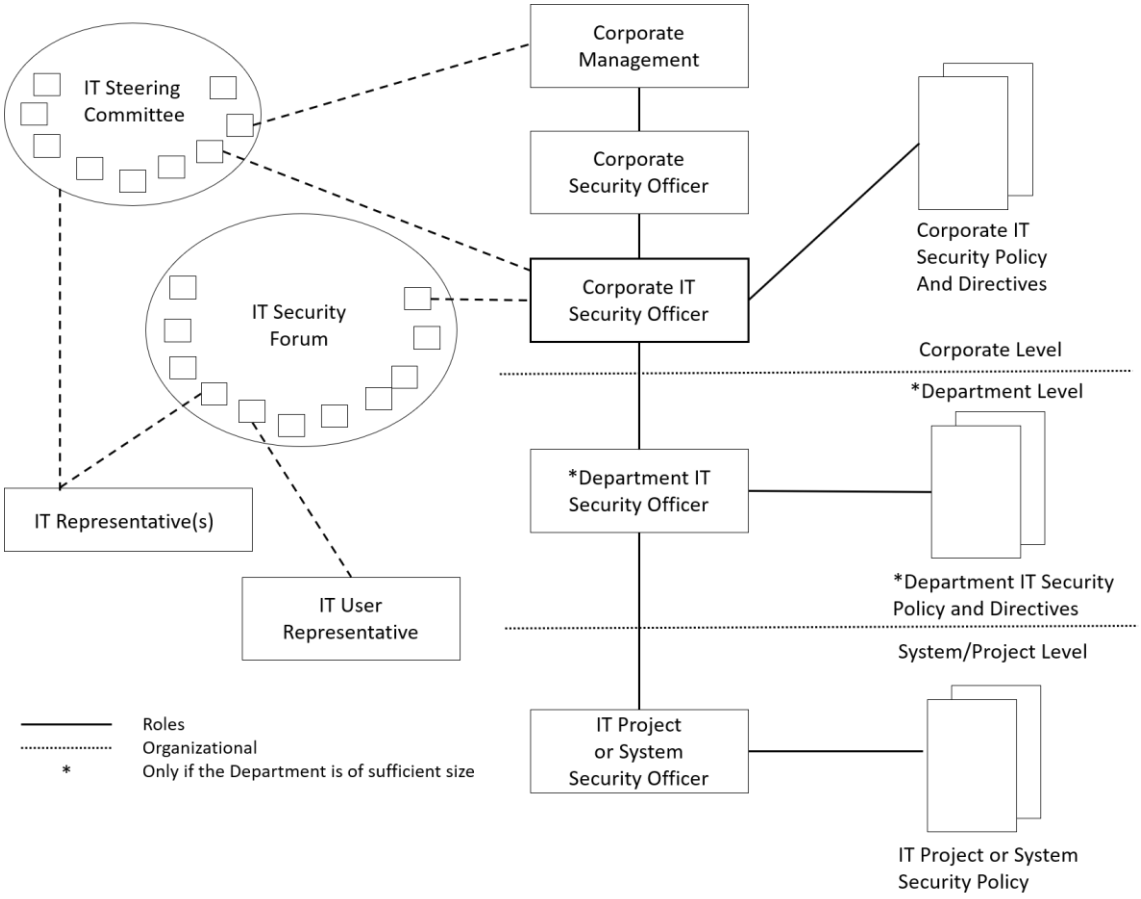

Figure 8. IT security organizational aspects (adapted from von Solms, 1999).

2.9 Information security architecture

Enterprise information security architecture (EISA) is based on enterprise architecture (EA), and it introduces framework for identification, analysis, and prioritization of business security requirements. This framework is used to choose the portfolio of the best integrated enterprise security solution and defining risks and threats (Shariati, Bahmani, & Shams, 2011). SABSA® is a comprehensive approach for executives when finding security solutions for business related problems, it is not technical approach, technical solutions solve tactical operational issues. Now days business and technology have been the same thing and companies need to look for competitive edge by incorporating

technologies. Security has been concentrating on confidentiality, integrity, and availability of the information. Concentrating to just these three attributes leave security gaps in the organization and their systems. There are more attributes than just these three that organizations needs to incorporate if they want to mitigate risks that are unique for a specific enterprise (Burkett, 2012). SABSA® taxonomy is based on business attributes, and it captures these attributes to show measurable organizational value (MOV) which is based on unique needs of the business attribute in stake. With this profiling method it is possible to measure security solution against predetermined solutions. Unnamed multinational banking group has used this approach successfully to ensure high-value internet transaction applications strategic development. Challenges that they faced and overcame using this targeted metrics approach were availability, interoperability with legacy systems and real-time transactions. SABSA® model answers to interrogatives who, what, when, where, why, and how. This model is good for aligning security to business strategy, it fills the security gaps in enterprise architecture and service management (Burkett, 2012). In this study SABSA® method is used for explaining the enterprise security architecture and its connection to strategy. Applying security just through operations meets the immediate and tactical information security need but it does not set up strategic and long-term solutions for organizations information protecting aches and pains. SABSA® is sort of road map for organizations to protect their assets it views organization with its six layers and development of security solutions is viewed through those layers, this development process is shown in figure 9.

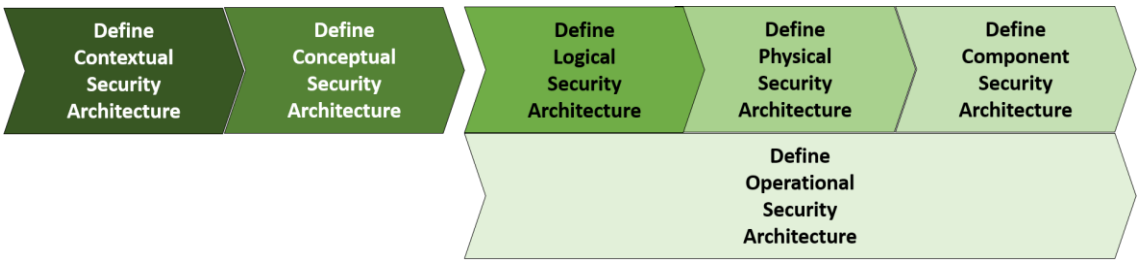

Figure 9. SABSA® development process (adapted from Burkett, 2012).

This method consists of six different layers which each stand for different stakeholders' point of view. SABSA® is a "time-tested" framework for secure information system building and it takes in account each layer. SABSA® is like software development where process starts from business need identification to develop specific product and it goes through different layers of development. In this SABSA® architecture model, there are six views and layers (Burkett, 2012). These six layers can be configured in a way where the operational bar is vertical across all the other five layers. This diagram (figure 10.) explains how the operational issues arise each of the five other layers (Sherwood, Clark, & Lynas, 2005).

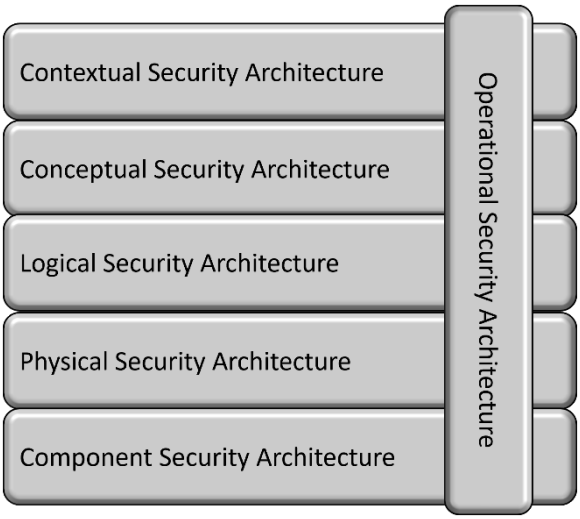

Figure 10. The SABSA® Model for Security Architecture Development (Sherwood, et al., 2005).

Each of these layers (view) have their own player and they ask six questions. These players and questions are presented in table 5. In the blue column there are the six point of views which are first the business view, then there is the second which is the architect's view, then there is the third which is the designers view, then there is the fourth which is the builders view, then there is the fifth which is the trade man's view, and then there is the sixth which is the facilities (Service) manager's view. In the green column there are the six questions (what, why, how, who, where, and when) for each of the point of views mentioned above (operational level).

Table 5. SABSA® questions in each layer (adapted from Sherwood, et al., 2005).

Business view	• What type of information system is it and for what will it be used? • Why will it be used? • How will it be used? • Who will used it? • Where will it be used? • When will it be used?
Architecture's view	• What you want to protect, in terms of business attributes profile? • Why the protection is important, terms of control objectives? • How you want to achieve the protection, in terms of high-level technical and management security strategies? • Who is involved in security management, in terms of entity relationship models, and the trust framework within which entities interact with one another? • Where you want to achieve the protection conceptualised in terms of security domains? • When is protection relevant, in terms of both points in time and periods of time?
Designer's view	• What? Business information is a logical representation of the real business. It is this business information that needs to be secured; • Why? Specifying the security policy requirements (high-level security policy, registration authority policy, certification authority policy, phycical domain policies, logical domain ppolicies, etc.) for securing business information; • How? Specifying the logical security services (intity authentication, confidentiality protection, integrity protection, non-reputadiation, system assurance, etc.) and how they fit together as common re-usable building blocks into a complex security system that meets the overall business requirements; • Who? Specifying the entities (users, security administrators, auditors, etc.) and their inter-relationships, attributes, authorised roles and privilege profiles in the form of a chema; • Where? Specifying the security domains and inter-domain relatioinships (logical security domains, physical security domains, security associations); • When? Specifying the security processing cycle (registration, cerification, login, session management, etc.)
Builder's view	• What? Specifying the business data model and the security-related data structures (tables, message, pointers, certificates, signatures, etc.); • Why? Specifying rules that drive logical cecision-making within the system (conditions, practices, procedures and actions); • How? Specifying security mechanisms (encryption, access control, digital signatures, virus scanning, etc.) and the physical machines upon which these mechanisms will be hosted; • Who? Specifying the people dependency in the form of the users, the applications that they use and the security user interface (screen formats and user interactions); • Where? Specitying security technology infrastructure (physical layout of the hardware, software and communication lines); • When? Specifying the time dependency in the form of execution control structures (sequences, events, lifetimes and time intervals).
Tradesman's view	• What? Data field specifications, address specifications and other detailed data structure specifications; • Why? Security standards; • How? Products and tools (both hardware and software); • Who? User identities, privileges, functions, actions and access control lists (ACLs); • Where? Computer processes, node addresses, and inter-process protocols; • When? Security step timings and sequencing.
Facilties (Service) manager's view	• What? Ensuring the operational continuity of the business systems and information processing, and maintaining the security of operational business data and information (confidentiality, integrity, availability, auditablity and accountability); • Why? To manage operational risks and hence to minimise operational failures and disruptions; • How? Performing specialised security-related operations (user security administration, system security administration, data back-ups, security monitoring, emergency response procedures, etc.); • Who? Providing operational support for the security-related needs of all users and their applications (busines users, operators, administrators, etc.); • Where? Maintaining the system integrity and security of all operational platforms and networks (by applying operational security standards and auditing the configuration against these standards); • When? Scheduling and executing a timetable of security-related operations.

As figure 10 shows operational layer has vertical relationship with other five layers. Operational security architecture must be interpreted in every other five layers in detail. Table 6 shows examples how this is done. There are examples on what kind of operational activities must be implied on different layers (Sherwood, Clark, & Lynas, 2005).

Table 6. The Operational Security Architecture (adapted from Sherwood, et al., 2005).

At the Contextual Layer	Business policymaking, business risk assessment process, business requirements, collection and specification, organisational and cultural development, etc.
At the Conceptual Layer	Major programmes for training and awareness, busines continuity management, audit and review, process development for registration, authorisation, administration and incident handling, development of standards and procedures, etc.
At the Logical Layer	Security policymaking, information classification, system classification, management of security, security of service management, negotiation of inter-operable standards for security services, audit trail monitoring and invocation of actions, etc.
At the Physical Layer	Development and execution of security rules, practices and procedures, including: cryptographic key management, communication of security parameters between parties, synchronisation between parties; ACL1 maintenance and distribution of ACE2, backup management (storing, labelling, indexing, etc.), virus pattern search maintenance, event log file management and archiving, etc.
At the Component Layer	Products, technology, evaluation and selection of standards and tools, project management, implementation management, operation and administration of individual components, etc.

Above we have introduced the abstractions of the six horizontal layers of this architecture model (contextual, conceptual, logical, physical, component, and operational). Each of these layers has also vertical cuts, where there are six questions asked at every layer, which is the vertical analyses (Sherwood, Clark, & Lynas, 2005). Questions asked in every contextual layer are presented in table 7. This might be confusing because operational level questions presented before in table 5 should be asked after these questions. These questions can be seeing in table 8 at first row.

Table 7. Six questions for every layer (adapted from Sherwood, et al., 2005).

Question 1.	*What* are you trying to do at this layer? - The assets to be protected by your security architecture;
Question 2.	*Why* are you doing it? - The motivation for wanting to apply security, expressed in the terms of this layer;
Question 3.	*How* are you trying to do it? – The functions needed to achieve security at this layer;
Question 4.	*Who* is involved? – The people and organizational aspects of security at this layer;
Question 5.	*Where* are your doing it? – The locations where you apply your security, relevant to this layer;
Question 6.	*When* are you doing it? – The time-related aspects of security relevant to this layer.

Six vertical architectural elements are summarized above for all six horizontal layers. This gives matrix where there are 6*6 cells, it is the model for the enterprise security architecture, the SABSA® matrix (see table 8). When issues raised by each cell are all addressed, then the range of questions have been answered, and the security architecture

is completed. Populating all the 36 questions is the process of developing enterprise security architecture (Sherwood, Clark, & Lynas, 2005).

Table 7. SABSA® Matrix for security architecture (adapted from Burkett, 2012).

LAYERS	ASSETS (What)	MOTIVATION (Why)	PROCESS (´How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)	VIEWS
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization & Relationships	Business Geography	Business Time Dependencies	Business
Conceptual	Business Atributes Profile	Control Objective	Security Strategies & Architectural Layering	Security Entity Model & Trust Framework	Security Domain Model	Security Related Lifetimes & Deadline	Architect
Logical	Business Information Mode	Security Policies	Security Services	Entity Schema & Privilidge Profiles	Security Domain Definitions & Accociations	Security Processing Cycle	Designer
Physical	Business Data Model	Security Rules, Practices, & Procedures	Security Mechanism	Users, Applications & the User Interface	Platform & Network Infrastructure	Control Structure Execution	Builder
Component	Detailed Data Structure	Security Standards	Security Products & Tools	Identities Functions, Actions, & ACLs	Pocesses, Nodes, Addresses Protocols	Security steps,Timing & Sequencing	Tradesman
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management & Support	Application, User Management, & Support	Security of Sites, Networks, & Platforms	Security Operations Schedule	Service Manager

The operational security architecture layer, which is the last row in table 8, refers to table 6. This operational layer can be broken out into a SABSA® Matrix and map each of the layers above. There are operational aspects associated with the other layers. In table 9 there are more detailed insights of this operational security architecture (Sherwood, Clark, & Lynas, 2005).

Table 8. The Operational Security Architecture Matrix (adapted from Sherwood, et al., 2005).

LAYERS	ASSETS (What)	MOTIVATION (Why)	PROCESS (´How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
Contextual	Business Requirements Collection; Information Classification	Business Risk Assessment; Corporate Policy Making	Business-Driven Information Security Management Programme	Business Security Organisaation Management	Business Fiel Operations Management	Business Calendar and Timetable Management
Conceptual	Business Continuity Management	Security Audit & Assurance Levels; Measurement, Metrics & Benchmarking	Incident Response Disaster Recovery; Change Control Programme	Security Training, Awareness And Culture Development	Security Domain Management	Security Operations Schedule Management
Logical	Information Security; System Integrity	Detailed Security Policy Making: Policy Compliance: Monitoring: Intelligence Gathering	Intrusion Detection; Event Monitoring; Process Development; Security Services Management; System Development controls; Configuration Management	Access Control & Privilidge Prrofile Administration	Application Security Adminsitration & Management	Managing Application Deadlines & Cut-off
Physical	Database Security Software Integrity	Vulnerability Assessment; Penetration Testing: Threat Assessment	Rule Definition; Key Management; ACL Maintenance; Back-Up Admin; Computer Forensic; Event Log Admin; Anti-Virus Admin	Users Support and Help Desk	Network Security Management; Site Security Management	User Account Aging; Password Aging; Crypto Key Aging; Administering Time Windows For Access Control
Component	Product & Tool Security & Integrity	CERT Notifications; Research on Threats & Vulnerabilities	Product Procurement; Project Managemetn; Operations Management	Personnel Vetting; User Administration	Platform, Workstation And Equipment Security Management	Time-out Configuration; Detailed Operation sequence

To summarize SABSA® Model presented on this paper has six layers:

- Contextual security architecture – the view of the business
- Conceptual security architecture – the view of the architecture
- Logical security architecture – the view of the designer
- Physical security architecture – the view of the builder
- Component security architecture – the view of the tradesman
- Operational security architecture – the view of the facilities manager (Sherwood, et al., 2005).

There are operational aspects in all the layers and operational layer can be visualized as cutting across five other layers. In each layer six basic questions asked: What? Why? How? Who? Where? When? When horizontal analyses are combined with the six question

vertical analyses, it will produce 36 – cell table which is the SABSA® Matrix (Sherwood, et al., 2005).

2.10 Information security controls

According to McLeod & Schell (2007) “control is mechanism that is implemented to either protect the firm from risks or to minimize the impact of the risks on the firm should they occur.” And he continues that controls fall in three different categories, these categories are: technical controls, formal controls, and informal controls. Osborne (2006) argues that when we are talking about IT systems there are three main categories which are: protective control, detective control, and recovery control, and system security is combination of these three security control main areas. Systems strength is sum of time to resistant to attack, react to breach, and recover from a breach. One category which is not usually used when dealing with computers is administrative control.

Tipton & Krause (2004) suggest that when providing information security controls there can be physical, technical, or administrative. These three control categories can be classified further to be either detective or preventive control. Detective controls try to recognize unwanted events after occurence. Commonly detective controls are such as audit trails, intrusion detection methods, and check-sums. Preventive controls purpose is to avoid unwanted events to occur. Preventive controls restricts the computing resources use freely, on the other hand user acceptation of these restrictions adjust the degree that these controls can be applied. Security awareness program can increase the tolerance of users to accept preventive controls, when they are understanding better how preventive controls build trust to their own computing systems security.

There are also three other types of controls that supplement detective and preventive controls. Usually they are described as deterrent, corrective, and recovery. Deterrent controls purpose is to discourage individuals to perform intentionally violations of

information security procedures or policies. Deterrent controls are usually implemented in a way that they are constrains which makes it undesirable or difficult to perform actions that are unauthorized or they can be consequence threats that sort of scare the potential intruder to perform information security violation, these can be such as severe punishment or embarrassment. Corrective controls can be the cure for unauthorized activity which was allowed or return to circumstances in situation what they were before security violation. Corrective controls execution could be changes to existing administrative, physical, and technical controls. Recovery controls help organization to recover their financial loses caused by violation of security and they can restore lost capabilities or computer resources (eduonix, 2016). In addition to controls mentioned above. Miller & Gregory, (2012) lists one more control type, it is called compensating control, it provides alternative ways for achieving tasks. Purpose of compensating control is to provide substitute controls in situation when other effective controls are not feasible or possible options for management.

Major categories in controls are physical, technical, and administrative controls, and these three deterrent, corrective, and recovery are more or less to be considered to be special cases within the major categories. They don't clearly belong to detective or preventive categories. Deterrent could be thought to be preventive because it can turn intruder away, but on the other hand deterrence also involves detection of violations, and this could be what intruder fears most. Corrective controls are connected to technical and administrative controls and they are not preventive or detective. Corrective controls are linked to technical controls for example in a way when anti-viral software is removing a virus and to administrative controls for example when damaged database is restored in backup procedure (Tipton & Krause, 2004). In table 10 these categories and their subcategories are listed.

Table 9. Information security controls (adapted from Tipton & Krause, 2004).

PHYSICAL CONTROLS	TECHNICAL CONTROLS	ADMINISTRATIVE CONTORLS
PREVENTIVE	**PREVENTIVE**	**PREVENTIVE**
• Backup files and documentation • Fences • Security quards • Badge systems • Locks and keys • Backup power • Biometric access controls • Site selection • Fire extinquishers	• Access control software • Anti-virus software • Library control systems • Passwords • Smart cards • Encryption • Dial-up access control and callback systems	• Security awareness and technical training • Separation of duties • Procedures for recruiting and terminating employees • Security policies and procedures • Supervision • Disaster recovery and contingency plans • User registration for computer access
DETECTIVE	**DETECTIVE**	**DETECTIVE**
• Motion detectors • Smoke and fire detectors • Closed-circuit television monitoring • Sensors and alarms	• Audit trails • Intrusion-detection expert systems	• Security reviews and audits • Performance evaluations • Required vacations • Background investigations • Rotation of duties

In short administrative controls are such as policies and procedures which are implemented as a part of overall information security strategy. They ensure that physical and technical controls are understood and implemented properly in accordance with the organization's security policy. Most often they are detective and preventive, but they can also be implemented as compensating and deterrent controls (Miller & Gregory, 2012).

Technical controls also called logical controls are the software and hardware mechanisms, they are used to implement access controls. They can be used in addition to preventive and detective as a corrective, deterrent, and recovery purposes. Physical controls are the ones that ensures physical environments safety and security and they are primarily detective or preventive. They are also deterrent, because for example in many cases security guards, fences, locked doors, dogs or video cameras and motion detectors function also as a deterrent control (Miller & Gregory, 2012).

Control framework can be thought as a slowly moving side of the information security process. Risk management can be thought as a dynamic side things. Strategic initiatives change this framework slowly. Organizations maturity can be measured with how

capable this framework is to successfully respond organizations day-to-day needs. Risk management is primary tool to verify the framework in a particular context, and indicating where tactical solutions or modifications are necessary. As organizations maturity level increases, it is expected that risk assessments will more drive control framework than policy. This reflects organizations ability to react quickly to changes in the business environment (Purser, 2004). This is illustrated in figure 11.

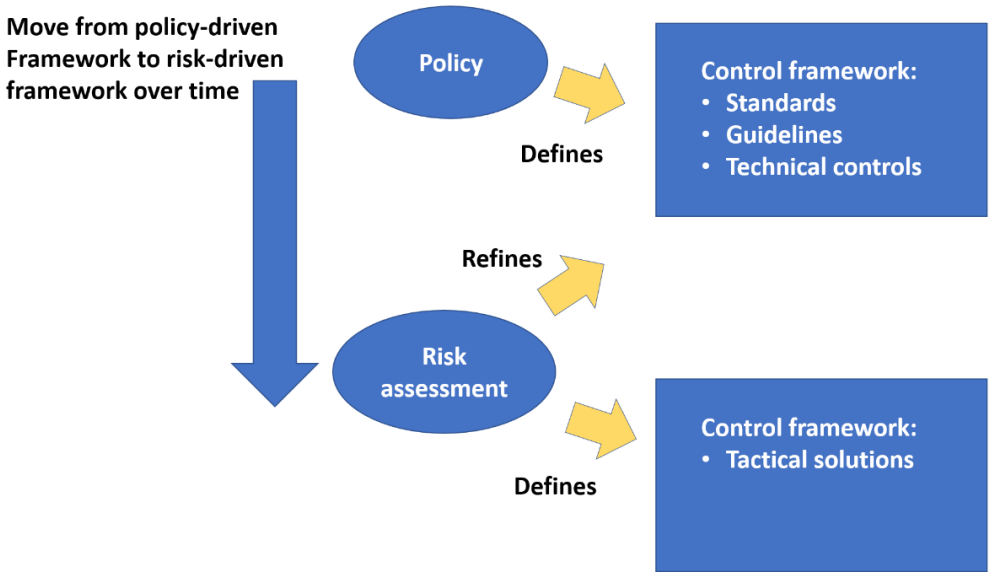

Figure 11. Relationship between policy, risk analyses, and control framework (adapted from Purser, 2004).

2.11 Management and culture theory in context of information security

Management in organization can be described to being organized into three different levels, where in every level they have different activities. First there is the upper management, they are concerned about the strategic planning, second level is the middle management, they are concerned about the functional management, and third level is the lower management, they are concerned about the operational management. Senior and upper management are involved company's vision, the business goals, and the

objectives. Functional managers understand how their functional units or divisions work, and what functional roles individuals have within the organization, and how their unit is affected directly by security. In the lower levels there are operational managers and staff, they are close to actual operation of the company. They know about the technical and the procedural requirements, and the systems and how they are used. They have also understood about how mechanism of the security is integrating into systems. They know how to configure them, and how it is affecting to their daily productivity (Raggad, 2010).

It can be said that in management refers those activities that managers are performing, in which they aim to achieve predefined objectives, which are returning economic and non-economic benefits to the company and its environment. Manager is responsible of directing those activities and their effective realization. Information security is often part of IT function, if that is the case then security manager should fully understand functional IT units strategic plan and obtain CIO's support to defining mission for the security division. Vision's must be consistent with strategic plan and mission of IT unit. Vision of the IT unit must be consistent with organizational strategic plan and mission. In theory we can say that all strategic plans, missions, visions, values, goals, objectives, and operational programs must be consistent with each another. Strategic plans have, strategic mission, strategic vision, strategic goals, strategic values, and strategic programs. Functional plans have functional mission, functional vision, functional goals, functional values, and functional programs. Operational plans have operational mission, operational vision, operational goals, operational values, and operational programs. Strategic plans have time period of 3 to 5 years, functional plans activities are shorter. Operational plans activities are immediate actions, and they have more accurate goals (Raggad, 2010).

Culture of information security provides guide and structure to behavior of humans when they are interacting with ICT, and it enables to avoid those actions which may cause risks security of organizations information assets. Mandating employees' behavior with regulations does not bring same effective results than having a culture which promotes good security-related human behavior, using knowledge, artifacts, values, and

assumptions. Security is effective when employees know, understand, and accept the precautions that are necessary. (AlHogail, 2015) According to AlHogail [2015] it is suggested by Schlieger & Teufel (2003) to make information security to be natural aspect of employees' daily activities, all socio-cultural measures that support technical security methods must be included in information security culture. According to AlHogail [2015] it is suggested by Ramachandran, Rao & Goles (2008) security related behavior of the group is guided and shaped by security-related ideas, beliefs, and values, those must be identified.

According to AlHogail [2015] it is argued by Malcolmson (2009) organization's security could be impacted with security culture. "It could affect how employees interact with the organization's systems and procedures at any point in time and results in acceptable or unacceptable behavior." According to (AlHogail, 2015) it is argued by (Ahogail & Mirza, 2014) definition of information culture can be "The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organization with the aim of influencing employees' security behavior to preserve information security".

Organizations have most often a dominant culture and subcultures. When majority of the employees share the core values of the organization it is the dominant culture and when smaller group of employees share values related to their work environment, department, peer group, nationality, or geographical area it is the subculture (Martins & Martins, 2016 [da Veiga & Martins, 2017]). IS culture is a subculture of organizational culture. Then organizational culture is the dominant culture, and it is the way that majority of employees are doing things (Schlieger & Teufel, 2003; Van Niekerk & Von Solms, 2005 [da Veiga & Martins, 2017]).

The IS culture is in this case a subculture of an organizational culture which is directed through the strategy, leadership, and organizational policies, and in addition with the IS policy. Inside IS culture there are mini-cultures or subcultures, they differentiate

between the groups of employees. Things that affect the differentiation are such as office or geographical location, job level, gender, religion, or generation group (Martins & Martins, 2016; Reynolds, 2010; Trice & Beyer, 1993 [da Veiga & Martins, 2017]). Organizations may have various IS subcultures, they can be in line with the dominant IS culture or they can oppose it, in this context it is called as a counterculture (Martin, 2001 [da Veiga & Martins, 2017]). Figure 12 depicts how IS culture is developed, how IS strategy and vision of management and legal and regulatory issues are directing it, and how intrinsic, extrinsic issues, and IS policies are influencing the culture, and how employee behavior foster the culture.

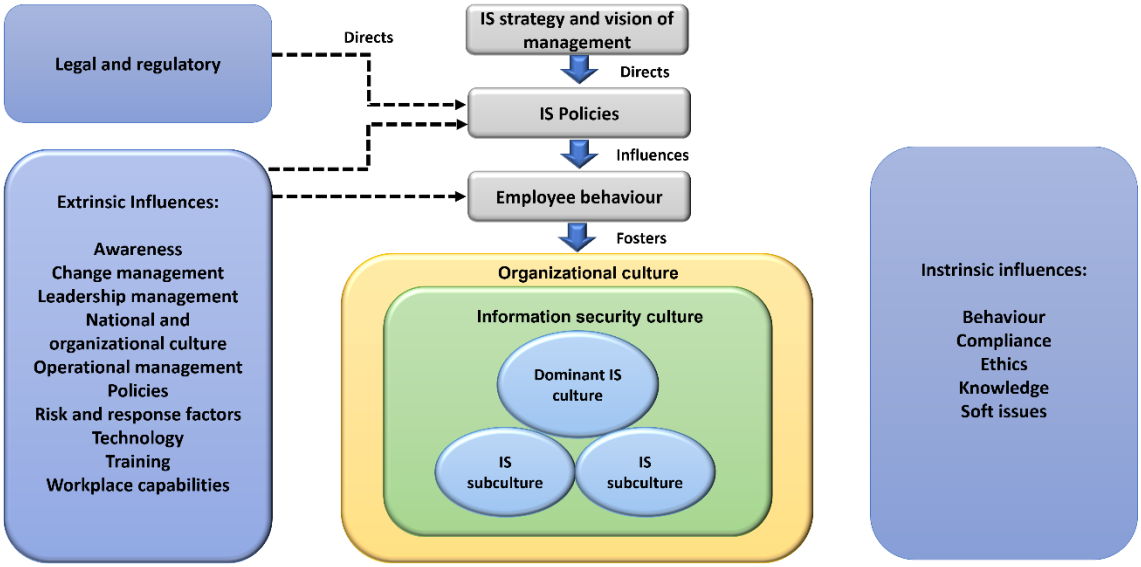

Figure 12. Development of and IS culture (adapted from Hellriegel, et al., 1998 [da Veiga & Martins, 2017]).

Leadership or management and their organizational roles plays critical role when forming the desired culture. They are the ones that needs to define organizations IS strategy and lead it by example (da Veiga & Martins, 2017).

3 Project management methodologies and IS standards & best practice methodologies

It is emphasized usually that information security is a process and not a project. Though information security elements in program must be managed as a project. Technically skilled IT or information security experts are needed routinely in organizations to lead project, or they can also use general managers and experienced project managers for leading information security projects. It is also possible to use both approaches simultaneously by assigning sometimes those tasks to general manager and sometimes to technical manager and so that quality deliverables, time issues and budget are in order in all elements of the information security program (Whitman & Mattord, 2008).

Project management methodology is a combination of logically related practices, methods and processes that are strictly defined, and they determine best way to plan, develop, control, and deliver a project. This is done through continuous implementation process until the project is successfully completed and terminated. It is scientifically proven approach to project design, execution, and completion in systematical and discipline way. Project methodology allows to control the entire process of management through effective decision making and problem solving, and at the same time ensuring the success of specific processes, approaches, techniques, methods, and technologies. Methodology provides typically skeleton where every step is described in dept. Project manager can implement and deliver project according to the schedule, budget, and client specification (MyMG, 2020).

Project management methodology should be chosen appropriately, and it should incorporate possibility to achieve following achievements:

- Stakeholder needs defined.
- Establish common language so that team understand it and know what is expected from them.
- Completed cost estimates which are accurate and credible.

- Methodological approach for every task
- Early conflict spotting and solving.
- Deliverables producing and handed over as expected.
- Lessons are learned and quick implementation of solutions for them (MyMG, 2020)

3.1 Review of different project management methodologies

Project management methodologies can be divided in two, there is traditional and modern approaches. Traditional approaches have project management processes that have series of consecutive stages. They are called waterfall methods in IT and software development. Design, development and delivering a product or service is done by step-by-step sequences. It requires that the implementation process be successively, and they have milestone planning and team building. Workflow in linear sequence. Traditional project management includes following stages:

- Initiation, where specification requirements are set.
- Planning and design
- Execution with construction and coding
- Control and integration
- Validation where testing and debugging is done.
- Closure (Installation and maintenance) (MyMG, 2020)

Modern approaches provide alternative way to project management they are not focusing on linear processes. Some methods are better in software and IT development, but there are methods that can be implemented in production, process improvement, product engineering etc. These modern approaches are using different kind of models in their management processes (MyMG, 2020). In software development projects IT security projects are required almost in every area from complex collaborative systems to mobile applications. Project management processes are influencing the success or failure of

these projects. IT security projects need particularly good project management processes in order to be successful, they must be adapted to specific characteristics of those processes (Alecu, Pocatilu, & Capisizu, 2011).

Software product development is becoming increasingly complex and there are demands to launch them faster. This creates need for project management methodologies that responds to this demand. There has been shift from classical methods in 2001 one when agile methodology was introduced and 2009 when DevOps (Development Operations) concept was introduced. DepOps can bring benefits to company by increasing enterprises efficiency and agility in their software development management. DevOps is an extension of the agile methodology which is emerging from the need of validate and delivering software products faster (Banica, Radulescu, Rosca, & Hagiu, 2017).

3.2 Information security standards & best practices

According to Diesch [2020] it is pointed out by Hedström (2011) that international standards and best practices are commonly used to build information security management to organization. Diesch (2020) remarks that ”best practices” and ”standards” terms are used often as synonyms, but the difference between them is that “standards” are usually validated by some international standardization organization and “best practices” are published independently as also other frameworks.

Accoring to Diesch, Plaff, & Krcmar, [2020] it is suggested by ISO/IEC (2018) that ISO/IEC 27000-series is the most common standard coming from international standard organization. Also according to Diesch, et al. [2020] it is suggested by Siponen and Williamson (2009) that this standard is accepted widely, and that it is playing important role, organization information security is possible to certify with this standard. According to Diesch (2020) the ISO/IEC 27000-series has basic definitions of requirements which can be used to information security management system implementation. It also

specifies control guidance, implementation guidance, management measures, and risk management. There are also special sub-norms included in this series, for example for telecommunication organizations there is ISO/IEC 27011, it deals them only.

In addition to standards concerning information security management, there are best practices or frameworks such as NIST SP8000-series, the standard of good practices which is from the Information Security Forum (ISF), or framework called COBIT. These mentioned best practices are for information security management system implementation. They define and develop controls and address information security problems with risk mitigation strategy. Security standards are providing organizations basis to reducing risks and they are doing this by developing, implementing and measuring security management (Diesch, et al., 2020).

ISMF (Information security management framework) consist of different documents which clearly define policies, procedures, and processes that are abided by the organization. When done properly, it will allow security leaders to manage intelligently organizations cyber risks. There are hundreds of ISMF's from which to choose. They can be such as NIST Cyber security framework, ISO 27000 family, and PCI DSS (Therault, 2022). GRC (Governance, Risk and Compliance) they can be described as a strategy and structure of an organization that keeps its secure and on track. Corporate governance defines the principles and agreements that are followed in the company. It also provides needed controls and support to achieve overall goals. Risk managent identifies threats and introduces processes against threats. Compliance management ensures that organization follows regulations and proper accounting practices, and ethics (SAP, 2022).

4 Research design and methodology

Qualitative research means research where qualitative data is used. Such data are interviews, documents, observation data from participant. Actual data is then used to explain and understand social phenomena (Myers, 1997). This research was done using qualitative approach. Literature research was conducted to make a theoretical framework which would work as a foundation for the road map. Empirical part of the research was interviews and their purpose was to complement and support literature review framework for assisting to create the road map. Literature for the theoretical part of the paper was from University library hardcovers, eBooks, articles from scientific journals and web sources.

The subject of the research in case study can be an organization (for example, a workplace, a company, an educational institution, or a project) or a group (an organized group or an informal group). A case can also be a process, such as when examining the preparation of an issue for social decision-making, a change sought in a project, or even an environmental accident that has occurred and its handling. Sometimes a case deals with one individual; just as it is thought that a doctor or therapist has cases of patients and clients. Thus, the cases analyzed by different studies can be quite different in scale (Günther & Hasanen, 2022). Research method was closest to case study because we are researching process of information security in companies, or we can say that because information security road map will eventually lead there.

The figure 13. below shows an ideal type of model of the course of the research process. However, the different stages of the process interact with each other: the next stage of the process can affect the previous stages more precisely, and sometimes the idea of research can change significantly along the way. Tasks in different phases are often overlapped. Research ethics issues are considered at all stages of the research. Writing is also part of the process all the time (Vuori, 2022).

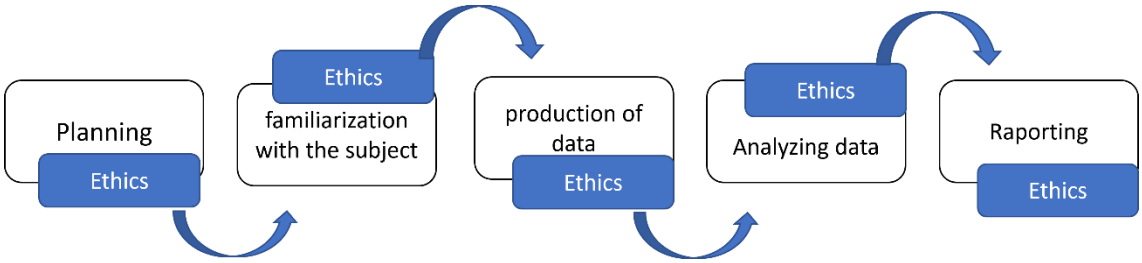

Figure 13. Research process (adapted from Vuori, 2022).

Few words about research environment, information was sought from University of Vaasa library online materials such as ProQuest Ebook Central, and databases such as EBSCO, IEEE and Science Direct. Hard cover books from the library of University of Oulu and National Repository Library. Data for the empirical part of the work was gathered through interviews. Interviewed persons were found by searching information security officers from Linkedin. Interviews were done using Microsoft Teams application. Actual interview was combination of an expert interview and theme interview. According to Hyvärinen, Suoninen and Vuori, (2022) the concept of a thematic interview is hardly known in English but is most often referred to as a semi-structured interview.

In a thematic interview, the questions may not be precisely worded in advance or always presented in the same format. The researcher first reads the literature on his / her research topic, chooses his / her own perspective and questions, and then decides which are the key themes for the research. The interviewer then asks freely, formulating questions on these themes. The popularity of the thematic interview is since the freedom to answer gives the right to the interviewees. It is also relatively easy to analyze the themes by theme. However, it is good to keep in mind that the themes set in advance by the researcher may not be the same as those that, when analyzing the material, prove essential in structuring the content of the material (Hirsjärvi & Hurme 2001 [Hyvärinen, Suoninen & Vuori 2022]).

The purpose of interviewing experts is, for example, to find out how companies, state administrations or municipalities operate or have acted in dealing with the matter under investigation. An expert is thus part of the preparation and decision-making, or at least

a person who may have followed it closely. It may follow that the researcher and the expert have conflicting interests and the expert may not have the willingness of the average interviewee to assist the researcher. The interviewer needs to be able to change his approach: sometimes it is good to present oneself as an expert, sometimes highlighting ignorance can provide more information (Alastalo, Åkerman & Vaittinen 2017 [Hyvärinen et al. 2022]).

Interview questions were formed based on a literature review to support and supplement the whole work. Main parts of the interviews were transcripted and transcriptions are in chapter 5. According to Kallio (2022) qualitative materials are often speech and interaction between two or more people. Transcription, the decomposition of speech and activity into written form, is a key part of the process of capturing and analyzing qualitative data. The key question in spelling is with what accuracy the speech is decoded. The accuracy of the spelling is particularly affected by the type of questions the study is looking for answers to. The chosen method of analysis is also affected. Are you interested in the substance, the different discourses, or the course of the interaction? Transcription is a description of what happens in a situation. Even superficial literature should answer the question "what is said?". For example, interview materials are often collected to obtain information about the interviewees 'perspectives, opinions, and understanding of a particular phenomenon. In this case, one is interested in the content of the speech. For the accuracy of the spelling, it is enough that the matter is understood. The quarrels, breaks, and other details contained in the speech are not central, but what the interviewee has to say about it.

Because of the confidentially reasons there are no mention or indication of companies or persons who participated in this study. There are eight interviewees', three of them were CISOs', one CIO, one CSO, one Lead information security manager, one director of information security and quality, and one information security manager. Companies were mostly in technology industry, but there was one consulting and financial company.

Experience from information security varies from 5 to 23 years and being sum of 107 and average of 13.4 years.

5 Results of the research

In this chapter there are transcriptions of the information security experts' interviews and proposal for the road map to information security. Because of the confidentiality reasons we are not indicating in the transcriptions who has said this and from which company this information is. Chapter headlines are basically the interview questions. Actual interview questions are listed in Appendix.

5.1 Best standards and best practices for implementing and maintaining information security

This subchapter consists of four own subchapters each of them containing main parts of the transcriptions of the answered interview questions concerning what are the best standards and best practices for implementing and maintaining information security? Subsection of this question refined the question to show what exactly they are for strategy, for policy, for standards, and for practices, for procedures, and for guidelines. Of course, asking question which is the best standard and best practice for implementing IS standards is little bit confusing, but it is relevant question if there is one.

5.1.1 Strategies

There is no one standard above others. ISO 27000 and ISF can be used for creating requirement frame, and CMMI maturity model to define the target level. Vital importance in standards and best practices is that you are using something, so that all the areas of information security are covered. It removes risks such as that information security team does only things that they think are interesting, or what they are good at it, and they leave things neglected because they do not like it. Standards does not have to be followed slavishly, or do exactly as they say, essential there is that it ensures company's information security program covers all the relevant areas. If organization does not have

Internet of things devices, then it does not need to cover that, still and all, these must be conscious decisions.

It depends so much about the organization, its maturity, size, industry, and customer's demand what they want from their suppliers and partners. CIS 20 critical security controls is good for getting the basics in order, and it is a good, prioritized list. ISO 27000 standard is recognized and identified globally, so as being most know standard, the customers also most often require it. In North America, NIST is probably more important. ISF is also important, it provides best practices for IS. ISO 27000 has detailed guidance how things could be done, but ISF has lots of ready-made models, which can be incorporated to security policy, standards, and procedures. They have lot of templates, but they cost money. Relevant there is that information security is managed and reviewed through audit, both internal and external. In main part of the management system, there is always technology, processes, and people.

Information security development and maintaining is not just about installing box to customers or own network and wishing that it will do it. Instead, it should be based on strategy. When starting from zero, then organization must define how it will organize itself and where particular things are done, it must define its whole governance model. One entity there is information security and company must choose how it will deal information security. In information security entirety organization must decide how to create strategies, annual plans, who is accepting things, and who has the authority to make decisions.

This is sort of normal framework which must put in place. In this context it is common to consider different kind of options that there are available in markets. Most commonly they are NIST, COBIT and ISO 27000, but if organization does not want to take clearly approach where standard is in the center, ISF standard of good practices is suitable way to approach, because it is more practical oriented approach compared to other mentioned standards. The problem that there is in these standards is that they are very black

and white, and in many things, they are far away from practice and that is why ISF is convenient when starting from zero. ISF is also originally build so that it is compatible with mentioned standards. It is based on research that ISF has done, and it incorporates framework for bench marking which enables organization to compare itself to others who are using the same framework. Essential precondition is that audition and health check have been done for the mentioned framework.

ISO 27000 is a management system standard, and systematic and process-oriented approach for information security, and not so much control framework. In long run it leads to structure which truly revolves around continuous development. It is difficult standard to communicate to the top management or uninitiated people. NIST framework can be used parallel there, it is intuitive and easy to communicate identification, protection, detection etc. Management system is based on ISO 27000's activities and controls are balanced with NIST classes, so controls are mapped together. This kind of arrangement requires tool, GRC (governance risk compliant), because larger organizations have several implementations, and it is difficult to remain visibility.

In some organizations there might be legal requirements or customers' demands which drive organization to start with standards such as SOC 2 (computer room standard) and ISAE 3402 (snapshot about how things work at the time of audit). These standards are practical standards, while ISO 27000 and NIST are more for processes, methodologies, and management systems. It depends on the company, which is best standard to start, for example if there are credit card payments, then it is PCI DSS, which starts from the implementation of controls.

ISO 27000 is standard that is formulated from management systems quality aspects, it describes what should be taken in consideration when managing security. It does not help implementing, and it does not guarantee secure product. It makes companies consider such issues that they would not otherwise do. Another thing there is verification, which in this case means that we must be able to show to auditor our systems. They can

come any time to review our systems, so that we do not have to trust just to Information security manager. With ISAE 3000 compliant assurance testing model combined with SOC2 standard, organizations can prove that their operative model fulfills certain requirements, and we can assume that it will produce security. None of these standards do not guarantee security, but they are proof that something has been done.

ISF standard of good practices is good when starting from zero because it steers with practical orientation and not acting like legal system which is the case in most of these standards and with other standards there must be work done before they can be considered as an applicable alternative. ISMF gives just a framework and in practice there must be defined who is doing what and everything must take to practical and operational level. This will require strategy at the beginning where the most critical issues are defined and make action plans for every sector. These are put in practice as a project or as another implementation options.

On the other hand, there is a unified consensus in ICT sector that separate security/cyber security strategy is not relevant. There is no such standard solution that everybody would do things in same way, which also means that we cannot deal strategy issues in unified way. But if company has information security management system for example corresponding to ISO 27000 and if it is functioning properly, it will produce risk maps and risk assessments which are inputs for the strategy work.

5.1.2 Policy

When having a control framework approach there must be strategic level which incorporates information security and privacy policy. From there it will go to the tactical level where there are general components about privacy and information security, such as information classification, how identification principles work (ID access management), IT service security standards, and end user security standards. One of the interviewed companies had in this context strategy, policy, and standards in their strategic level. In

operative level there are instructions and procedures kind of things. More descriptive way of dividing these levels would have been strategic, tactical, operative, and tool layer. In tool layer there are things such as e-Learning. The whole card deck starts from CIA and how is the information handled there, because that is the foundation pillar.

If company wants to audit itself against standard, then different standards bring different kind of requirements. Standards may have demands such as use policies for example for emails, use of internet, or use of different kind of applications. They also communicate what is allowed for staff, so that they know what is allowed and what is not. This could be something like to what you can use company software's and equipment's and to what you cannot. In this kind of situation, it is possible to report deviations if something that is not allowed for staff, is not understood.

5.1.3 Standards

Standards are minimum requirements, which standard to choose is a business decision. Meeting the requirements of ISO 27000 will in practice produce a minimum level of security. Each company should assess their own risk field, what kind of risk there are exposed to, and on the other hand what kind of risks the whole industry is exposed. If companies want a comprehensive information security, they need to develop further.

5.1.4 Practices, Procedures, and guidelines

In policies it should defined what is allowed and what is not and enable perception of what is allowed and what is not. In operative level there are instructions and procedures kind of things. In the table 11 we have listed and summarized the standards and best practices which came out from interviews.

Table 10. Summary of the Standards and best practices.

Standard/Best practice	Purpose(pros&cons)
ISO 27000 ISO/IEC 27000 International Organization for Standardization International Electrotechnical Commission	• Management system standard, • Systematic process oriented approach • Continuous development • Dificult to communicate • Good for creating requirement frame • Most often required by the customer
ISF Information Security Forum Standard of Good Practice for Information Security	• Practical approach (good when organization is not standard centered, and it is starting from zero) • Good for creating requirement frame • Provides best practices • Enables benchmarking to others
CMMI Capability Maturity Model Integration	• Good for: define the target level
NIST (Cyber Security Framework) National Institute of Standards and Technology	• More important in North America • Paraller use with ISO 27000 • Easy to communicate • Controls balanced with NIST classes (when using ISO 27000)
CIS 20 Center for Internet Security: Critical Security Controls for Effective Cyber Defense	• Critical security controls (prioritized list) • Good for getting basics in order
COBIT Control Objectives for Information and Related Technologies	• Commonly used best practice
SOC 2 System and Organization Controls Type: Trust Services Criteria	• Computer room standard • Customer demands • Legal requirements
ISAE 3402 International Standard on Assurance Engagements 3402	• Snapshot how things work at the time of audit • Customer demands • Legal requirements
PCI DSS Payment Card Industry Data Security Standard	• When credit cards are used • Starts from implementation of controls
GRC Governance, Risk and Compliance	• Large organizations have several implementations, it is difficult to remain visibility, helps there

5.2 Project management methods for implementing and maintaining information security?

Project management machinery is set off when organization must move more than just one unit. Otherwise work related to information security and privacy is normal process work. This can be slow down and boring, but if we notice that there is gap somewhere,

or we must get something new, and it cannot be done within limits of normal processes and resources, then we need project. In other words, when normal organization cannot do simultaneously synchronized change of several different organization units, then we establish project. This applies to business related changes also. Otherwise, project management is just a tool. In software house, it is not advisable to do software, with waterfall methods, it should be agile from start to end. With Jira agile ticket system, it is possible to model in all the company's assets, risks, treatment plans, policies, IS controls, incidents, and change logs or change management. They can be linked together, and it is possible to make handovers to teams or each other. It is possible to make fast reports from status of issue. For example, if we have expanding ISO 27000 related project for each new site, which are about to be affiliated to certification.

There can be 151 tickets which must be finished successfully before certification is possible. Agile thinking there is that every demand is fed to the backlog, and they are divided to stages according to backlog's view. Everybody can see, in which stage we are now and what are we doing currently. Project orientation has a tool value, but lean management, operating management, resource management, and work monitoring can be in the DNA of the company. When all the attributes are entered into Jira, it is possible to easily print reports.

First thing that must be cleared out here is what kind of projects are we talking about, are they development projects where we are building something totally new or are the projects concerning continues improvement or are we talking about customer projects where we are doing something for the customer. All these have different kind of needs. There is no individual all-embracing project method. From a point of view of Research and development and IT, there is usually gate model used, where certain criteria must be filled before it gets through the gate and moves to the next phase of the project. Process starts from idea phase and from which it moves to planning phase and on the end to the execution or implementation phase.

Many companies aim to avoid separate information security projects. Nevertheless, when driving up mode of operation it is most efficient to implement as a project or for example when aiming to improve identity access management entity. There is clearly a project which must be done to take the step. More common approach is secure by design philosophy, which means that everything we are doing has to be information secure. Information security demands are incorporated into the projects. In gate check model gates has an information security component which must be checked and verify before access through gate is admitted. For example, in IT development projects specifications there must be relevant components in each case involving security. They monitored throughout the whole project so that they are considered continuously and that they are found in the product.

This is the only working way. Afterword's it is difficult to get information security demands in there, so building them from the beginning is rational way of doing. It is a guideline requirement set which must be filled. For example, when building a system with external access through web interface, there must be necessary information requirements defined. Those requirements are mirrored to see are they met. If there are exceptions made, then there must be log about who has decided to deviate from the rules and on what grounds, is it a permanent deviation or temporary and when it is verified next time. Information security as privacy must be incorporated into general project management methods and not to be as a separate component.

When we start to implement or improving information security standard or things related to it, project management methods itself does not have any meaning, on the contrary, whatever the method is that the organization is using should be chosen to be the one that is used, because things must incorporate to there, so that the rest of the organization starts to change its behavior. IS department should use PM methods that others are using. If there is not any systematic method for something, then it has meaning, because implementing IS controls requires method. If there are no processes, it is then difficult to implement controls which requires or are relying on processes. Existence of

methodologies to ease implementing controls, because then we can hang controls to something that already exists. In our organization IT development is in SCRUM model and those who are aiming to achieve certifications are using more DevOps model kind of approach. When we are doing something according to agile methods, then IS is embedded into those cycles. ISO 27000 has strongly PDCA-cycle underlying it, which is continuous improvement, as are other ISO management systems also, such as quality and environmental certificates. Interesting question in the future is that how to implant continuous improvement of IS to LEAN philosophy.

In agile enterprise model individual teams or tribes are responsible of area. Aim of this is to reduce handovers. For example, team is responsible of information security of cloud service, it develops individually needed capabilities, and maintains and ensures that those capabilities are continuously updated and sufficient. This will reduce handovers, so that there is no need for separate development and maintaining organization, the same team develops and maintains these activities and this same goes for whole business model. The benefit that we are gaining compared to waterfall method is likely that handovers are reduced. In waterfall method planning phase can take 1,5 years. In agile model it is built in, and we can once in every 3 months, change plans, road maps, and other doings. We can change them radically, if needed. If situation changes, we can change our directions. This is relevant in the area of information security, in the sense that, despite that there are long-term plans, situation may change, so that some external threat grows, or we identify that there are lacks in somewhere, which we have not noticed yet. We can respond to these fast. We use Enterprise agile model, which is not project management method, it is operation model for organization, which includes development and management practices.

Information security implementations and projects does not need any security standard or IS specific model. It is important that the project management methods that are used in organization are also used in information security, and IS projects are carried out with the methods that organization is using in its other projects. Quite often, and not just in

the sense of resources, project manager comes from the PMO, and he or she does not have any substance knowledge about IS. PM ensures that all the elements of project management that are used in other projects in the organization, are there. It does not matter is the project something else, such as IT, or business, there must be starting from requirement definition to risk identification and closing the project, all the information security issues considered. Project management is important, when implementing information security. There can be projects that last for years, several things must be thought and integrate systems to processes and elsewhere. Without project management it is impossible to ensure that things are progressing. Implementing standards requires organized actions for example for audits.

If information security department has capability and resources to function accordingly with established Prince2 or PMP model, are they probably good. If things are done agile according to Scrum, they are working. Biggest problem is that we might take raisins from the bun, and just take the pleasant things in, which cause least work, and on the other hand we forget those things where we must ensure, that things were done. Effect analyses and different kind of gate checkpoints are necessary. Worst mistake is to implement project just as a technical deployment and forget risk identification, change management, and roll-back planning.

Things are done by the annual planning cycle as in ISO 27000. After that we make risk assessments and based on that we develop operations, it is continuous improving and maintaining. In the case that there is something bigger to be done, then project might be rational way of implement it. It is strange to associate project management and IS maintaining, because projects have start, end and resources. Information security after all is a continuous process where there can be single improvements, but things must run all a time. Gluing information security on the top of everything and showing that there has been something done, does not produce best possible protection methods for risks. Compliance thinking where we follow just regulations is not clever way of operating for business, things can go wrong. Nevertheless, project management is important when we

have large and complex things to do or there are risks involved, then project is the way it should be handled, and you get successful result and even better if it is well managed project.

5.3 Biggest challenges implementing and maintaining information security?

One of the biggest challenges is to get information security part of everyday doing and to everything that we are doing. Everybody has the responsibility to member it. It is good example of subject where everybody is responsible. General knowledge about information security is a component of company culture and it must be incorporated to daily actions such as work safety, there must be general ground rules from which cannot be deviated, these are related to behavior. There many kinds of IS risks, for example what are you talking about during your free time or what are you reading in the train so that somebody else can see it. In addition, there are technical controls, which can be build, they are also part of this. Information security as part of daily operations is difficult issue, because there is “I can slip from these rules” kind of mentality. The general knowledge and acting like it is a big challenge. Tricky things are also the cost of information security, one can use plenty of money and still it does not guarantee the safety and take away possibility of intrusion. General knowledge grows over the time. One effective way of increasing the knowledge is e-Learning which must do at certain intervals such as annually and it is a condition of employment.

One challenge is the correctness of investment and controls, and their relation to risks exposed. In IS it is difficult to measure risks probability or effect of it. In traditional risk management the risk probability and effect are evaluated and there we get heat map or fourfold table, where are high risks or big effect risks, and rare small risks, which are not worth of big effort. In IS these kinds of maps are not exactly possible to build, because significant individual breaches for example, are so rare. There is no statistics existing

about their effects, so that we could predict the cost of the breach. This is probably the biggest problem, to measure risks effect and then measure controls and investments. Are they in right level or is there somewhere too much or too little? The whole business machine needs decision making governance steering mechanism about how information security wholeness is going to be taken forward in the company, this requires work. Strategy must be verified, is it the right one, how it is embarked in annual plans, what kind of undertakings there is, how much money we need, what kind of partners do we need. These kind of things does not happen by itself; we need goal setting.

Change management concerning standards is also one big challenge because you must ensure that the requirements of the standards are also met over the time. There are lot of horror scenarios used to get financing for information security and management understands it into certain level. It might be challenging justify investment, but when using risk analyses and continuous planning it is possible. It is associated with historical reasons, IS has little bit bad reputation because back in time there have been driven some things into organizations and bought new systems without thorough analyses.

Company management understands that there are measures that must be implemented and IS function's job is to define those measures. The pace of change and matching it to the functioning of the organization, the focus too much around the technique, and the low level of assessments and self-criticism. On the other hand, the big problem is that we are so out of the whole industry that you do not even see the need for security until it collapses. It is better to even do technical security if you do not know how to do it, than to forget that life cycle. In table 12 there are listed challenges when implementing and maintaining strategies, policies, standards, practices, procedures, and guidelines, and added with some managerial implications.

Table 11. Challenges when implementing and maintaining subject.

Subject	Challenges and managerial implications
Strategy	• Management sees IS as an IT issue and outsource it to IT department. • Management does not understand strategic importance of IS which results fiddlling with technical controls and forgeting risk management approach • How big investments to do? • How much veto right to person who is responsible and what way to intervene other people's doings? (For example case where top management do not want to regularly take information security in their agenda, or they do not give information security manager formal role or possibility to report.) • Persuading and having compassion of senior managment. • If business is build such that IS is hindering it, then no sense to make any proposals about it. IS manager must make sure that possible benefits of IS issues for business are utilized (this can be also a result of bad personal relationship). • In strategic level IS must be company's own business and not something that is owned by IS manager, it is then about awareness of the senior management. • Strategy is made in silos, and it is not linked with business, then it is little bit separate, and it does not get support and ownership from business. It must be aligned with business strategy. • The biggest challenges, is to understand, what are to most important things in terms of business. Information security can be easily thought as a technical thing, "buy this equipment, and you will get protection and all the troubles are gone." It is one of the most important things in business risk management.
Policy	• Policies must provide some practical help to business. How business can implement their own business in a way that it is secure. Anybody can write IS policies, which in practice are just instructions and orders, it can be done without strategic understanding. How to secure that they are followed is challenge and requires continuous tuning. • Business management support and understanding are significantly important. Still not a big challenge.
Standards	• Main challenge is to, which standard or standards to choose. It must be interest of the business and bring value to customers. • It depends about the corporate culture, how policy is realized. If organization is not very process oriented, then implementing systematic ISO 27000 can be very painful. Because there is no strong background of following processes and working in the way that it leaves evidence. Audit logs leave evidence about operating according to processes. Logs also give visibility about how controls are functioning. That gives confidence and trust that risks are in that level as they are wanted to be. • Ownership must be in the right level, who is responsible of implementing things. If large IS department and separate security administration, IT and businesspersons, then process owners should define standards and procedures, so that all details are defined at right level. For example, ISO 27000 is about maturity levels and knowhow how to do it.
Practices, procedures and guidelines	• If organizations operations are very process oriented then taking procedures to practice is easy, maintaining is a problem, if there is no any standardized systematic way of operating. It is challenge even if controls are in place, and there is overall picture, and measuring and follow up of IS is done with metrics and using continous improvement model and detecting and correcting flaws. ISO 27000 for example can ease that. • ISO 27000 best practices requires document maintaining annually, or every second year, it so wide set of documents that must be communicated to people, this can be challenge to smaller companies. • Awareness and communication are important. Lots of details, must ensured that they are known and used. Not recommended to same people to do policies, practices, procedures, and guidelines, because then they would be neglected and not updated. • It is about creating culture of follow up, enforcement, and monitoring. Creating the IS culture is biggest challenge. • Organizations will not be successful if security understanding security needs accurate guidance, severe penalties, and whistleblowing. • It must be positive, engaging, people must feel that they are benefiting when working together. • Must be chance to say if instructions are interfering work. • Must be positive athmosphere where people think and expect good from others.

5.4 Biggest challenges in information security today and future?

The environment and the entire world have changed to be more hostile place, whether the case is about criminals or other actors. Crimes made in internet are producing

increased incomes to criminals. There are big challenges. It is important to understand technology development and how to protect things. For example, cloud services which are excellent services that can be used to many things, but if there is not enough understanding what will change when we move to cloud, it is possible to make expensive and inconvenient mistakes. In cloud services we must understand the new boundary conditions concerning what must be protected. There are different kind of breaches occurring and that creates instant spurts, where we start to develop something to protect something, will those initiatives reach the goal, so that we can get all the possible benefits from them. This requires know how and understanding. To achieve all the benefits, projects must be well controlled and managed, and we must go back to them time to time, when it comes to individual doing.

Cybercrimes have become more professional. They have more resources, and they are getting more organized. Person who commits cybercrimes, does not need to have technical competence, they can operate successfully without it, because there are subcontracting chains existing. Challenges are different depending on the industry. In manufacturing industry biggest challenge is supply chain risks. Raw-material suppliers and subcontractor does not necessarily have enough IS awareness, or their practices are not in proper or mature level. This is biggest challenge in manufacturing industry today and in future. In other industries, personal data of consumers causes lot of challenges. There it can be turned around and to opportunity to take care things well. EU's GDPR causes lots of headaches if there is lot of personal data to handle. In industrial automation risk will increase. There are long life cycles in the machinery, and they have been taken in use in a time where they were standalone models. In that time, there were not any IS features installed in these machines. When these machines are connected to external world through digitalization, it will bring significant IS risks. We have not seen yet any big wave, where IS attacks would be targeted to industrial automation. All the forecasts predict that, there will be big problems. There will be state level attacks to it. It is delicious target for hybrid attacks.

Cloud services are new mode of operation, and they require new way of thinking, and they bring lot of risks, but also opportunities. If functions are exported to cloud, how to ensure that it is always available there. There are lot of biases, but also opportunities. There are functions that can never export to cloud. One big challenge is supply chain software development, corporate own systems and how to risks or threats coming from there can be prevented. There are lot of examples in supply chain software development threats. It also depends about the industry/sector where there can have totally different level intrusion and breach risk simple just because of what kind of customers they have. There are examples of intrusion through company's law firm because and used the special status of that contractor, it has been known that their information security levels are not in the same level than other suppliers.

There are risks in hardware product components, can component manufactures be trusted. Technically it is difficult to analyze software or hardware, it requires significant investments, if you want to be sure that there is nothing that does not belong there. In software's it requires time, special knowledge, money, and resources. In hardware it requires dismantling of products which is very laborious and expensive. Next big challenge might be something that we did not understand to expect. The development of automation and technology among the cyber criminals, the transformation of national player to plain cyber criminals, and challenges in access management cloud and multi supplier environment, is challenge.

Today there is lot of concerns about intellectual property rights. Also, there is lot of interaction with the customer and lot of customers information already in the delivery process and in service processes there are continuously customers information, how to handle and protect that information and ensure that we do not mix different customers information and that customers cannot access each other's information. This can be even more important than protecting own information. This can be noticeably big challenge in organizations and customers wants also answers to question how their data is handled. This kind of mechanism can drive companies to implement ISO 27000 standard.

In fact, we can see in Finnish manufacturing industry that customers are demanding same requirements from us that we did to our suppliers 20 years ago in IT sector. How are they ensuring that no one gets access to their servers and then that drove them to implement ISO 27000 standards to their server rooms? Only response to audit performed by each customer is to acquire external certificate and customer must be satisfied with that. This is good example of what drives development of information security. Customers' demands to their suppliers what they need to meet to be their supplier.

One big challenge is that the number of external requirements is growing. Authorities, and customers are requiring more from organizations, and often they are different requirement, so simply the awareness and knowledge of all these requirements, what external stakeholders set, is a challenge. Understanding, being aware, and implementing them is noticeably important thing. There are requirements coming from customers in growing amounts, but also own suppliers have more partners, and supply chains are not anymore chains, they are networks. There can be thousands or even tens of thousands different organization in these networks. How to control all that, especially if you are the organization that is at the end responsible for the information security. Number of variables is large, and it is not enough to take care of just own security, there are players in the networks, whose IS you must ensure, and on the other hand you must ensure that you are delivering required level of information security. This is noticeably big challenge. The number of potential threats is increasing. Digitalization causes increase in attacks, and they are global. Finnish companies are facing same threats than organizations in Africa or Australia. Still the biggest challenge is how to control supply chain and all the player in that network.

One big challenge is maintaining information, because there you must know in what kind of threats you must prepare. Individual company sees just what kind of threats they have been facing, but intelligence can gather information. What kind of threats we are facing in future, is a challenge? Another issue is what is the right level of security. If there have not been any incidents, does that mean that it is enough, or are we just lucky, or has

there something happened, we just do not know it. In credit risks, if risks are increasing, they just take less credits in. In information security it is not possible to let some risk to realize, even one is too much. Understanding the threats and staying on the nerves of the time is challenging. There have been examples, where intruder has access to data and started to use it immediately. Standards require months to fix these vulnerabilities. There have been cases where vulnerabilities been utilized just in few hours after the breach. IT department have had few hours to fix the vulnerability. So, the need for fast reaction time is also a big challenge.

Basic thoughts will stay, but after every few years, there will be some new platform, modern technology, or some other new mega trend, in which people will jump into and forget basics. IS will realize when we know whose data, we are processing, and on whose behalf, we are running the system. If there are requirements for confidentially, integrity, or availability, whose responsibility it is to monitor that these issues come true. These things are forgetting when we frantically jump into something, for example from data server to SharePoint, from Passeli to workday, or from excel to Salesforce. Staying in technological development is not the problem, it is keeping basics in people minds when moving into some new system. Basic information security requirements must be implemented and fulfilled in new system also. In every system they are implemented differently. Challenge there is that will you get to inform these propellant hat and credit card busting guys early enough before they have been able to root the system deep into organizations processes, without considering security.

5.5 Project management methods in information security, their role and importance

Project management at itself is a way of getting this done, if we start project and we do not assess risks related to product, we just assume that they are defined already in project assignment. That is good, but we should always ensure in what kind of world the

product is about to be made. Whether it is about product development or software project or something like that, there substantial portion of the security is made already in development phase. If we leave access management undone, then it does not exist there, when we drive our product into production. Security during driving or production is different thing, there we detect things and then act accordingly. Appropriate requirements and demands must be entered to the project, if they are not entered, then despite that, you must be able to define at initial stages of the project, what things consider.

Agile project management methods do not fit to everything. It is good for making product or software and when introducing them. In software's you must first plan what to do, and it is same in information security, you must know what you need and what kind of products there are available and how do they fit into bigger picture. In most of the cases they are introduced incrementally and wait that trust to new technology is developed. Information security sets requirements to every process and project in organization, either directly or indirectly.

Project management methods are rarely monitored in this context. Other areas such as IT management, or business projects are usually mature, because they might have been done several times. IS projects are not so mature, because their solutions are new. We are constantly trying to tackle changing threats, and because of that, there are new solutions coming all a time in use, so that we can response to these threats. Agile is often best PM method when building a respond for fast and continuously changing threats. In waterfall methods it can take year, and during that time, situation might change many times.

Updates and emergency changes are made in operations, and there are not any project management methods involved. Agile methods are good when there is something latest information, we do not have to run down existing projects and leave them unfinished, because things are done in small pieces. When using agile methods and doing things in smaller pieces, organization gains the benefits of projects fast, and it will not leave

unfinished projects. Information security must be baked into that methodology which is used. There must be information security controls taken in consideration. It does not matter which methodology is used if information security is baked in there. Key role there is how information security is considered in different phases of the project. It is like quality, which must be there in the whole life cycle.

Project management must work to get results done safely. On the other hand, need for change might be so hard, that we must do big projects fast, and without any larger project model. We also must separate technical changes, and process changes, and for example training project. They have similarities, but there is also differences how they should be implemented.

We do not experience that using different project management methods will enhance information security. It is a tool for change management. Especially when we are implementing new business, acquiring new product, platform, or system. They are projects, and there the responsible person must be get caught enough early phase, before they have drove system to production, and come hopefully ask that, can you test security of the new system. Only thing that we can then do is to discover how screwed up it is done, and the damage is already there. Essential there is that do we get information security integrated unequivocally at early phase in terms of life cycle management. It is also continuous challenge. If project model has gates, or other checkups, without passing these, management will not give approval to move on, that might force to take security in consideration. It does not guarantee that security will be good, there might be hypocrisy.

5.6 What is the role and importance of Risk Management in IS?

Important, relevant there is the capability to communicate information security risks as a business risk. Otherwise, it is difficult to get budgets and the whole project. It is important to be able to communicate to senior management, what kind of business risks

there are in information security risks. It must direct resource usage, be credible and timely. We can have different opinions about its results, there is no one clear meter for it. If we turn everything to money, many risks will be added in cost of security breach, which on the other hand is no single scenario.

It is central issue here, only job that IS has, is to mitigate risks, and if there is not any systematic risk management, probability that we are investing in wrong things is high. It is possible that we invest too much to somewhere, and on the other hand something important is neglected. Risk management is an integral part of information security.
Risk management is one of the corner stones in this context. If IS decisions and operations are not based on risk assessment, then what are they based on. They cannot be based on how I feel and vibes or what kind of products there are in markets, which is not sustainable way. Risks that company is exposed must be identified with risk analyses, so that it is possible to evaluate needed controls and how much are they mitigating risks. This is essential part of information security. IS department does not necessarily own any of the information security risks. They are owned by those parties that owns the assets which are exposed to risks. It depends about the company who can take the risks and in which level the decision can be made in some business area. If there are many business areas, it can vary how one of those can danger the whole company by taking some risks. Risk assessment function does this job and then management approves them based on reports or information that risk assessment produces. It is possible that one business area can take some risks on their own, but some risks are so high that that they cannot be taken in that level. Particularly if these risks are affecting the whole company and not just to that business area.

Information security is part of risk management framework. IS is thus linked to top-level risk management. There are internal and external risks. Business continuing measuring and evaluating recovery plan times and what kind of risk we can take, which is based on risk acceptance. There is no perfect risk management, no money is enough for that. IS should be seen as part of the risk management. There must be corporate IS steering

group and chairperson such as risk manager. Risk must be controlled. It is only rational way to evaluate IS related investments or development projects. Against what risks we are doing this, there are lot of things that we can do. Privacy goes along side of this. The measures we take must be based on risk assessments. On the top of that, there are things that must be done always.

Risk management is integral part of the information security. If there is no credible risk management process, then it is difficult to imagine that there will be any good outcome from information security, and it is not implemented cost efficiently. Risk management enables those findings and opportunities that come to our attention can be utilized in IS management. Communicate risks about systems, processes, and products, to persons responsible of businesses, so that they can make decision whether investing on something, or something that is going wrong, will it be accepted or not, and if accepted, with what risk coefficient. We support business, and there are different kind of ways from which to choose, how to deal with something, what size risks organization is willing to take. What are things where nothing can happen. If information security is not integrated in risk management, then there will not be any good outcomes.

Those risks that are in responsibility of IS department are easy. Then it is important to understand why things are done and what is the meaning of it. Other one is more complex, those risks that are in business unit's responsibility and are directly related to business. In there, information security unit's task is to advice business units, what kind of risks are involving in their business, and they must be dealt with somehow. They are issues where business unit can make their own decisions, in other words, take risks or mitigate them. There are always risks in business, and risk decisions must be done consciously, and in sufficient light of information.

5.7 What is the role and importance of management in IS?

If we little bit exaggerate, it is all about management. However, there are things that must be done there, and there are technologies that are in key role. It is management issue, starting from top management. If top management thinks that IS is technical issue, we do not get an optimal solution. If IS is just a thing that can be outsourced to IT department, then we are not doing risk management right, and we are not spotting opportunities that it might bring to business. Information security must be led by the business management, they must be committed, and define what risks are we taking and what risks are we mitigating. ISO 27000 is a management model, which must be management continuously for improving, monitoring that how is this working, should we do changes in structures. From point of view of Information security manager, it is all about management, technology is something that experts implement under the management.

It depends on the school if you think about it. Management is the thing that creates prerequisites or generate changes, and without it there is no information security. It is how deep we go in that management, there are different kind of habits in different organization cultures. For example, in there how closely people are managed or are we hiring people who already have sufficient capabilities and know how to do things directly. Security is a state which is achieved through management, we cannot think that it is something that realized and happens on its own, and it is choices it can be implemented in many ways, we can be short- or long-term thinkers, or do it cheap or expensive way. Behind all these things there must be somebody who is leading the operation. In modern organization it must be collective leadership and not dictating. Information security personnel must have professional leader who understands organizations, decision making, management, and leads people. The role of management is essential, without leadership it will not be successful.

Business management sets the goal level and can take position in which is acceptable risk level. This role belongs to either Board of directors or to acting business

management. In this context the IS department's role is to explain the situation, and what kind of risks are we exposed. There might be situations where IS department cannot successfully explain it, and business management does not understand what it is about. Management sets the target level and ensures that the level of IS is sufficient in terms of risk bearing capacity, and that there will not come unexpected problems to company. Another thing is that there must be mutual understanding about the target level, and management must support it or demonstrate it in practice that it is supporting it, and in that way showing that things are done this way. In tricky situations business management must do decisions on its own, whether it is taking care of IS risk or postponing it and is that decision that we can take. These things are essential when having a conversation with top management.

It is difficult to say is it more important than is some other area. In modern days if IS management is not in the company's management team, then the chain into top management must be in order. IS issue must be regularly reported to management. IS management must manage things well, because they are multidimensional, and they are not affecting just IT department or some department, but everyone. They must be administered and communicated organization wide, it is very demanding and important.

If there is no approval from management, then it is difficult to get anything done. Information security issues are impossible to drive to production or in practice, if there is no management approval, it is critical in IS issues. Everything cost money or work hours, depending on what is going to be done or who is going to be hired, these can be big investments. Management works also as an example, if they are following strictly IS requirements, it is difficult to subordinates say that they do not have to follow those, and everybody is following the same rules.

Information security is related to management and commitment. When building an entity, mandate and commitment from management team and board of directors is important, there must be expression of the will to act and how do we want to operate.

Mandate and expectations what should be done comes from there. It is an order to take care of this thing. Then you either hire or otherwise get somebody who can do it. Critical positions are in the organization and external help is used as needed. Own crew creates the comprehensive package which includes the objective, policies, and standards, and they practically guide the operation. In governance sense that is how the business machine is run annually. In practice there are different kind of management meetings, annual reviews, audits, and reporting. It could be reporting about current situation once a year to board of directors and three times to management team. The commitment of the management is essential, without it and mandate it is impossible to do anything.

5.8 Role and importance of culture in IS

Culture eats strategy for breakfast. Many times, when we make mistakes, they are caused because people are indifferent, and indifference is due the culture. This is very straightforward chain. Another thing is, how to develop culture. It is not a thing that is developed just saying “now we are developing culture.” Instead, it is developed by managing it, with systematic and goal-oriented actions. Culture is about commitment and today it is easier to get commitment because of all examples that we have had recently what happens when things go wrong. Information security is selling itself and it is easier to understand. Information security is part of the company culture and company culture is one of the strongest forces that company have, and it is difficult to change it.

Cultures significance is difficult to diminish in IS context. If organization encourages employees to inform about deviations and they are not punished from it, depending of course what it is about. In principle it will lead to culture which is open, and which is based on mutual trust. Employees dare to turn them self in. It is essential here to understand that these misconducts happen because employees are not aware about instructions, or they might have misunderstood instructions. In one way you could say that in many times it is information security managers fault, in that sense that IS training has

not been sufficient or often enough, or guidance has not been sufficient, or something else. Information security managers should look into mirror and ask that what is my part here, when these misconducts and deviations occur. So, we can say that it is also IS manager's fault. Management example is also important culture factor here. People can experience that IS is making their job more difficult, they must trust that they are not going to be accused every time that something happens, and so they react easier when they are trusted, and then they believe in that process and know that we are trying to fix a problem. Figure 14 presents context of secure culture.

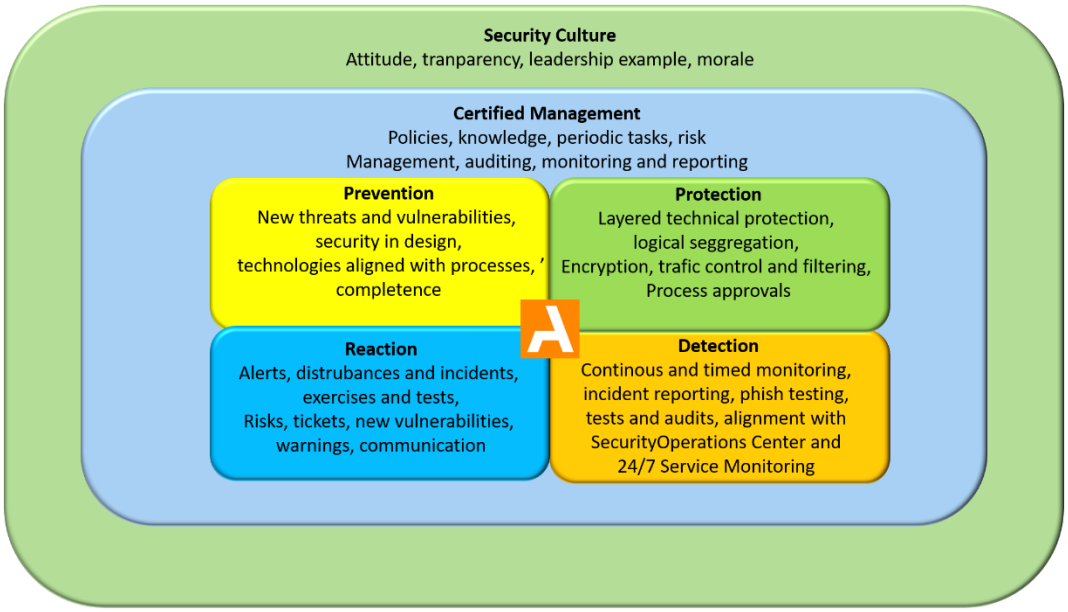

Figure 14. Security culture.

Culture has essential role in IS. People are the weakest link in IS and that is mitigated with culture. People must understand why IS is important in our daily activities, and what is their own responsibility, and act accordingly. In those roles where IS is implemented, whether it is in HR or IT, it is essential to that we do right things, and not slip away from it, it is essential for whole corporate culture. If average employees do not understand what kind of unwanted affects their actions may cause, more likely they fall to victims of some fraud such as phishing or they do something stupid.

Culture is the habits, skill, and practices of organization, and of people in it. There is a saying that, “people are the weakest link in IS.” This is not true, employee who possess sufficient understanding and skills can be strong link in cyber defense. People must know what is expected from them and in which kind of situations they must do some own choices or right decisions. Bad example of culture is when in IS training people are told that all confidential emails must be encrypted, but they are not providing any model, which they could use to identify confidential emails. They have to ques is this contract, project plan, or this customer data confidential. In addition, it is possible that they are not providing any tools for encrypting the emails. There is a good meaning but there is not built culture and conditions where people can act right. Good example is that it is identified that most of the breaches start with phishing, technical systems do not filter all of them out. People have been told and ensured that it is relevant threat to company and cleared out that if one of those is successful, they may spread ransomwares and company will be in news, or gets ransom demands and systems are not working, and we are in unpleasant situation.

General awareness about threats is important. Another example is where in phishing we want that everything suspicious is reported, but we do not tell where to. People will be sending emails to whomever. There must be uncomplicated way to act, and the right way to act must be the easiest way to act. Otherwise, nobody will not remember it or go to read instructions about it from intranet. There is a one button in emails, and you just must press that, and it is reported, and employee’s own responsibility is taken care of. People must be harnessed to do things that has meaning, which they can make a difference, and they understand that it matters to organization. They must know when to act, how to act, and have right equipment’s for it. Making culture is not just distributing information, there must be ensured that good practices are rooted to established practices in the organization, and people will do thing in right way automatically. Biggest obstacle if themes of culture are chosen to be subjects which are not relevant, and people do not understand why things must do so or subjects that people cannot do. People are part of the good perceiving capability, especially in external threats.

The role of management is precisely to create and foster culture where people understand what is expected from them, and they react positively acts to promoting personal security and privacy, but also for promoting collective security to customer's interest. In American organizations there is result or out kind of ethos, where if things do not go well CEO gets fired, and this same goes for IS manager, if there is breach. They want kind of persons who will take care of things with their own personality and with their own management style and own activities bring nothing else but success. In terms of culture this is not a clever way of doing things. It gives impression that organization is allowed just be there, and if there are problems, we just throw out one guy from top and then all the sins forgiven. Then new guy comes in and has a moment of leadership gust and need to leave fingerprints in 90 degree turns making. Organizations must give second change, which means that you can make mistakes, they should not be hide, they had to be admitted, and dealt openly. Only condition there is that lessons are learned. Another thing is that organization hires IS professionals who works for that those who are not experts dare to say if something is not right, and they themselves admit if they make mistakes, which they sometime do. People should not be diminished, laugh at, or punished if there are issues concerning security.

IS is not done only in IS department, it is done in the whole organization. The whole organization must be aware of that. It is heavy way of doing if things are done in a way that organization learns what is accepted and what is not. It must be brought to cultural level, as some other thing behavior or quality are natural thing in doing something. For example, customer service, where attitude towards customers is always polite, things must be also done securely. It must be installed to people backbones and into the culture, which is not ab easy job. It is not enough for culture to arrange annual IS training for organization, so that it is done. That is the level to reach so that we could get a continuous security for personnel, and that they can react and watch for pitfalls and threats.

5.9 Lacks and improvement suggestions in IS standards and best practices

Industry specific standards are challenge. Main idea is the same, but there might be industry related specific features, which might be inconvenient, if they are applied to some other industry. Balance between general and industry specific standards. Development of things is not shielded of the lack of standards, quote the contrary. More so it is depending on having understanding and will to develop.

Especially when implementing we notice that some things are left to be unclear, or are difficult, why is this done like this, why is this in so vital role here. These are generic issues and nothing serious. Also, there are not any established practices in supply chain security. There we must invent the wheel again always with different supplier. How do we deal with this supplier and how ensure this thing and so on? There are no ready-made practices for supply chain security. It is also same thing to downstream with our customers. Their awareness about IS is increasing and they want to ensure it. Every customer asks little bit different kind of questions, it is very laborious to gather own answers for each customer. It is completely unstructured field, there is order for some standard. One answer for it is to request ISO 27000 or equivalent from our own suppliers. Everybody does not have it, and it must be dealt with case by case. One meaning for certification is to communicate to customers, that we are taking care of these things and you do not have to come ask questions about it. Standards must apply differently in different industries, and they provide minimum level security and assure that fundamentals are in order. Companies must apply them to their own risk environment. They are not enough.

They are all flawed in terms of one individual company, because they are compromises and abstractions. Completely perfect model would be entirely company specific, which would not be generalized standard. Then we could be talking about for example ISAE 3000, in its reporting, risk-based framework is completely based on company's own

operations. There the general things are more the way reporting and evaluation is done against external operator. Biggest problem that there probably is, is that most of the best-known standards are those which are the most undefined, but they good for getting started. If standards minimum requirements are trusted completely blindsided, it might leave IS uncompleted. That is why we need own risk-based testing on the top. Standards are developing constantly and there are new versions coming all a time. World changes also digitalization change things and it is important to keep up with the phase. It is not enough to reach some level once you must develop continuously. In manufacturing sector everybody is improving all a time and if one stays to enjoy superior performance for a while then you fall in comparison.

Where do we start, and which standard serves the organization best? Often none of these standards directly serves any organization. They must be review piece by piece and find the relevant issues for that company. They are not usually such that all the controls are implemented straightly, but through risk identification and risk management controls that are relevant to that company are chosen. Essential there is that standard serves own organization, in that situation. Weaknesses that we can see in ISO 27000 is the age of it. Terminology, structure how its controls are listed, does not respond todays or futures demands, cloud or IoT type of model, or what kind of world it could be in the future. Weight of history can be seen in ISO 27000. ISO as an organization does not update its standards as flexible than some other standards such as ISF, which is small organization, and can more dynamically update its standards, because there is no heavy review and acceptance process. Most know big standards are quite heavy to update. Most dynamic and the ones that response to today's and futures demands are not so recognized among customer and other stakeholders.

Challenges that we have today are not going to be solved with additional standards. Top management awareness or external threat situation does not get improved with standards. For example, in finance sector there are lot of regulations, which look like legal requirements. Standards and requirement frameworks should be clear, they define

control objectives and risks which to respond, but they leave open how to respond. For example, emails must be encrypted, and key must so and so long, but they are not telling how. It would be too complicated, and not necessarily best solution for everyone. If standards would define system or technical control in one way, it would not last in time, and not the best solution for everybody. Standards are not the problem, if there are some major lacks, it is the preparation mechanism which is boring and specialized in nitpicking. You cannot use ISO without paying license fee. However, it is originally drawn up by industry players in hope that it would be universally recognized, and it would be followed broadly as possible. Access to it is therefore limited. If we hope that everybody would use and comply it, it should be public and in reach of everybody. These are small cosmetic issues. Bigger nuisance is when we are making contracts with our customers, partners, vendors, and other parties, there everybody comes with their own contract template, and from their own contract culture, there might come conflicts and egos are making noise when trying to make some sense into it.

For example, in contracts it is required that passwords be changed every two months. Instead, we should require long password and reserve right to crack the passwords, and not require users to change the password so often. We inform our contract partners that this is not relevant anymore. Then we hope that they will not come back to that issue. Contracting is big nuisance. legislation and export control define that encryption software's are weapons, and those application must be inspected, and they require separate export permit from authorities, if there were not any exemptions which would give a waiver from it.

5.10 Other observations and managerial implications

There has been talks about business networking for a long time, in terms of security and risk management, they require different kind of thinking. When we had everything to ourselves, things were done using waterfall method, and there were checkpoints. That

was much easier when we are thinking about information security. On the other hand, if we think about DevOps world, where there are lot of releases made frequently and the meaning of testing increases. The question there is on the end how well that coder or developer either know how, realize, wants, or bothers to consider security factors. Verifying there is lighter, and we must trust more to people, developers who are doing these things. This is a challenge. In addition to information security, privacy should be mentioned, because it is big part of this field and cannot be ignored in this context. If information is slip out it will cause reputation damages. It is also possible to win with this as being good at it, such as in environmental issues, where it is worth of keeping the company image good. There are also possible to create products related to information security, so there are also opportunities there.

There is a paradigm change going on in IS. There have been done controls, firewalls, system hardenings, and user right restrictions, which are like a wall in the castle, they are necessary, but they are not enough, because it is not possible to build such a wall that it is impossible to enemy get there. If the wall is four meter thick still there are wastewater going out somewhere, is that tunnel enabling intrusion, or if the wall is high, then somebody invents airplane. Preventive controls are not enough and the paradigm or focus change on right and left is going on. Left in sense of that IS is incorporated into business systems from the beginning, DevOps is that. There IS is built in the systems from the beginning, and teams make those individually, versus situation where we are doing internet services and front of them, we install firewalls and filters. So, in the other hand we must move beginning of the development to make IS and the other direction is to in addition to preventive controls, we must have good ability to observe and react to things. Ability to observe and react to is important, there are examples where intrusion has been detected nine months later, so criminals have had time to perpetrate their crimes there.

We have been coaching top management and board of directors to thing when assessing own organizations security, then one must challenge person responsible for the IS to present all the possible alternatives what they are using to assess effectiveness of those

IS operations. This is because one can always show how many incidents there have been, how much money we have used, and how many firewalls we have in network. Have they made any difference and how sure are you that right things have been measured? These issues are the responsibility of the organization's top management. They have monopoly to go ask about these things from information security officer, which ordinary employee cannot do, director of the board can. It is not enough from IS officer to answer that we have ISO certificate, it does not answer the question, have you done right things and does this certainly protect us from attacks. Information security is area effects and results of something that has done today can show years later. So, one must understand that these decisions have effects for years. GDPR and legislation brings challenges. How for example American software's and equipment's fit to Finnish legislation and to GDPR. They partly restrict operation, but on the other hand it is good that this is not a wild west. We would hope that in business management they would identify better the meaning of IS, even when making decisions not to invest that those would be conscious decisions, and that we would not learn things through hard way.

Old standards do not respond completely to demands that new models such as DevOps, DevSecOps, and Industry 4.0 are bringing. For example, in finance sector there is security of duties, which means that it is regulated, and responsibilities and roles must be separated clearly. In DevOps model organizations operate differently than traditional organizations, there things are published and put into production. There is not any standard which could be used to tackle all the IS risk that are coming from Industry 4.0. They must be clued or somehow applied. Standards do not provide direct solutions todays or futures challenges.

There must be somebody who understands links between security standards, business, and company's processes, and which is most functional model at a given time. Standards do not solve challenges, there must be personnel interpreting and applying it that environment. It does not matter what are we doing, one must always remember to assess the effectiveness of success. Is the objective reached, or did we just move problems to

somewhere else? In here, co-operation with professionals from quality function is necessary. Have they made any difference and how ensured are you that right things have been measured? These issues are the responsibility of the organization's top management. They have monopoly to go ask about these things from information security officer, which ordinary employee cannot do, director of the board can. It is not enough from IS officer to answer that we have ISO certificate, it does not answer the question, have you done right things and does this certainly protect us from attacks.

5.11 Suggestion for the road map

To support market, product and technology integrated planning we need an approach and road mapping has been used to that. It results a document called road map. Road maps also need continuous updating (Carlos, Amaral, & Caetano, 2018). "A road map is a strategic plan that defines a goal or desired outcome and includes the major steps or milestones needed to reach it." Road maps serve also as a communication tool. It helps to articulate strategic thinking and explains the plan and why reach the goal (ProductPlan, 2022). Road map can also be defined as a visual way to quickly communicate a strategy or plan. This is high level broad definition, but it applies to all road maps and to any party who has any influence into companies' business goals (Roadmunk, 2022).

According to Airfocus (2022) "a road map is a high-level strategic overview of a significant business initiative. Road maps are typically used to manage the development of a new product or the execution of a company-wide project." Benefits of having road map is that with it, it is possible to keep team members on the same page when we are talking about scope, objectives, and timeline. Drawback of road map can be such as if it is not updated frequently, initiatives may veer from the original course, and projects can derail because of the unplanned dependencies. They should be used as a living working document

otherwise, they become counterproductive. According to SCALED AGILE (2021) they are the glue that links strategy to tactics.

Based on the research study, road map for the information security is formed. Road map in this study starts with the phase where risks are assessed, because it is essential to know and understand in which kind of environment the overall information security system is build. Risk assessment produces inputs to strategy work and strategy produces controls for information security. Brown, (2018) presents road map for IS in three step process where first step is risk assessment, second step is where security policy and strategy are created, and third one is where planning for implementation, security testing, and risk management is done. Road map in this study follows the same in next two steps where there in second phase is security policy and strategy creation, and third phase is where planning of implementation, security testing, and risk management is conducted.

Last two phases are more driving things into the organization rather than just doing things. First of these last two phases is to drive standards into the organization, which ever standard/standards have been chosen to implement. Second phase is to drive practices, procedures, and guidelines into the organization structures. Of course, this may be in real life much more challenging and complicated than it is appearing in this suggestion, and some of these phases are not something that it is done once they must be revised regularly. Road map does not include any time scale or specific standards, best practices, or contingency planning yet, because those are related to industry and environment where the company operates, and it is meant to be a living document and so being it requires continuous updating. Theoretical framework gives lots of concepts to think about when updating this road map. Figure 15 is visual illustration of the road map.

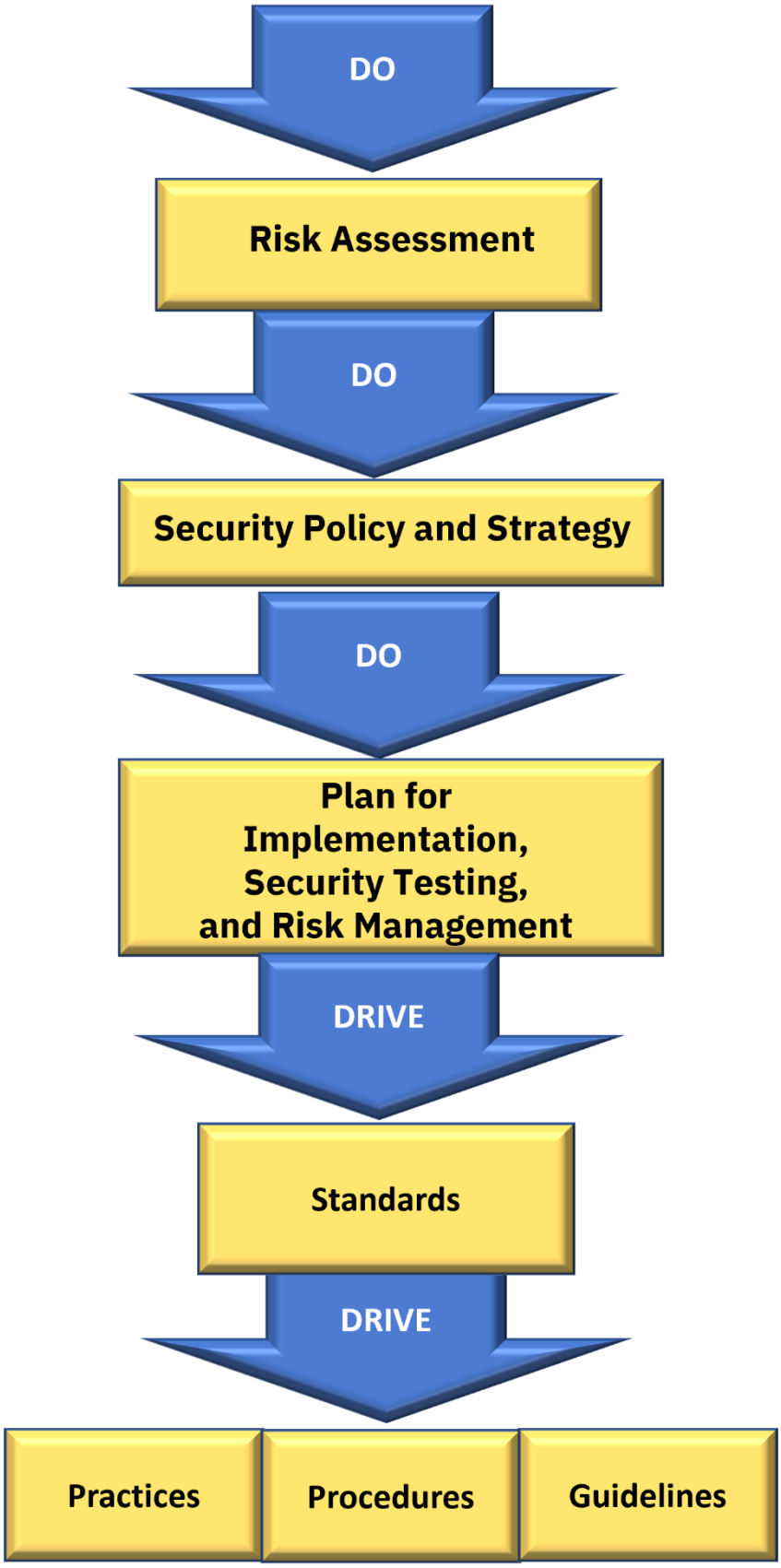

Figure 15. Road map for information security.

5.11.1 Challenges of implementation of IS

Challenges when implementing information security can be such as how to get IS part of the everyday doing, or how to measure investments and controls to match risks exposed, are they at the right level, or are there exaggeration or underestimation. Information security has also little bit bad reputation because back in history there has been cases where new system has been bought without thorough analyses. The pace of change and matching that into functioning of the organization can be challenge. The focus can be too much around the techniques, and assessments and self-criticism can be low level.

From strategic point of view, it is typical that management sees IS as an IT issue and then outsource it to IT department. It might be challenging to get management understand the strategic importance of IS how severe it is, and what goals to take and how to prioritize them. If management do not understand it, then easily fiddling with technical controls, and forgetting wide risk management perspective. It is not enough to just ask how big investments we are doing, it is also about how much veto is given to person responsible, so that he or she can intervene other people's doings. One of the most important challenges is to understand most important things in terms of business. Mitigating risks that organization is facing is secondary thing.

Policy making is not difficult, how well it is followed is. It needs business management support and understanding. Corporate culture plays key role in how policy is realized. Process oriented organizations have easier job to implement ISO 27000 which is very systematic, whereas organizations that are not process oriented, it might turn out to be very painful. When considering standards, the main challenge there is which standard to use. It must be in the interest of the business and bring value to customer. Running bureaucracy can be consuming and this might be challenge to smaller companies. Pressure coming from customer and will to use can also be very consuming. Creating right culture for the information security can be the biggest challenge.

5.11.2 Future research proposals

According to our interviews we found some lacks and improvement suggestions and we are interpreting those as future research proposals. Firstly, industry specific standards are challenge and finding a balance between general and industry specific standards. Secondly there are no established practices in supply chain security and wheel must be invented always again. There are no ready-made practices for supply chain security. No agreement templates for suppliers. Thirdly is the age of ISO 27000. Terminology, structure how its controls are listed, does not respond today's demands. ISO as an organization does not update its standards as flexible than some other standards. ISF is a small organization and updates its standards more dynamically, because they do not have heavy review and acceptance process. Fourthly standards and requirement frameworks should be clear, they define control objectives and risks which to respond, but they leave open how to respond.

Fifthly in DevOps world where there are lot of releases made frequently and the meaning of testing increases, which is different than in waterfall world. How to ensure that coder or developer know how, realize, wants, or bothers to consider security factors. Final sixthly privacy is not mentioned in this research, and it should be mentioned in information security context.

6 Discussion

Theoretical framework in this study covers CIA triad, expanded information security definition, information security classification, information security controls, IS governance, IS architecture, information security strategy, risk management, and management and culture in information security. In our empirical part we had set of questions that we asked from industry experts. Our purpose was not to find some exact answers and measures, purpose was more to raise a discussion around IS and hear expert opinions about Information security related issues. There was not any standard better than other and it depends about organization, its maturity, size, industry, and what customers' demands.

Although ISO 27000 was mentioned most of the interviewed companies. It is a management system standard, process-oriented systematic approach for IS, which in long run will lead to structure that truly revolves around continuous development, but difficult to communicate. It is not a control framework and NIST framework can be use parallel as a control framework. Which is common that there are different standards and best practices used parallel in organizations. Sometimes some practice can used as a vehicle to get for example ISO 27000 certification. In ICT sector has consensus that separate information/cyber security strategy is not relevant. Properly functioning information security management system such as ISO 27000 will produce risk maps and risk assessments which are inputs for strategy work.

Strategic level in control framework approach incorporates information security and privacy policy. Tactical level holds general components about privacy and IS. Operative level there are instructions and procedures kind of things. Tool layer could be added to this, where there are things like e-Learning. Standards are basically minimum requirements and choosing one is business decision. Standards do not guarantee security, but they prove that something has been done. In policies there should be defined what is allowed and what is not.

Project management method does not have any meaning when implementing or improving IS standard. There should be used the same methods that rest of the organization is using and information security should be integrated into those methods. Project management machinery is set off when organization must move more than one unit, otherwise IS and privacy work is normal process work. Key issue here is how information security is considered in separate phases of the project, like quality which is there in the whole life cycle.

Despite this research does not provide any groundbreaking new information it still provides valuable insight about information security from security practitioners. As there are eight Information experts giving their opinion to questions of this research and literation and transcripts of those interviews were made, and their main parts are included to this research. There are examples what kind of problems practitioners face and their opinions about standards. This kind of approach and perspectives are not very common in existing literature. Literature part presents SABSA® model and its executive level approach, which is quite unknown among the practitioners.

Cyber criminals have become more professional, they have more resources, and they are more organized. Technical competences are not necessarily needed because there is subcontracting chain existing. Cloud services are new mode of operation, and require new way of thinking, there are lot of opportunities but also risks. There are risks in hardware product components, can manufactures be trusted. It requires significant resources to analyze software or hardware products. Next massive thing might be something that we did not understand to expect. In service processes there are customers information used all a time, how to make sure that customers cannot access each other's information, this can be more important than protecting own information. Growth of the external requirements is a challenge today, supply chains are networks, where there can be tens of thousands different organizations. Basic ideas will stay, but after every few years there will be some new platform, technology, or mega trend in which people will jump into and forget the basics. Risk management is important, and relevant there is the capability

to communicate information security risks as a business risk to senior management. IS job is to mitigate risks and therefore we need systematic risk management. IS is part of risk management framework and it is linked to top-level risk management. Top management must understand that IS is not some technical issue which can be outsourced to IT department. IS should be managed by business management, and they define what risks are we taking and what are we mitigating. Information security personnel must have professional leader who understands organizations, decision making, management, and leading people. IS department role being to explain the situation and risk exposure, business management sets the goal level and defines acceptable risk level.

Company culture is one of the strongest forces that company have, and information security is part of that. Company culture is difficult to change. Culture is the habits, skills, and practices of organization and of its people. It is said sometimes that people are the weakest link in IS. This is not true, people can be strong link when they possess sufficient understanding and skills of cyber security. They must understand what is expected from them and when to do own choices or decisions.

ISO 27000 weakness is the age of it. Terminology, structure how its controls are listed does not respond for todays or for futures demands, IoT or cloud type of model, or for the future world. ISO organization's the current approach looks like not have been validated it by all organizations using it, unlike ISF, which is small organization and does not have heavy review and acceptance process. There are no established practices in supply chain security. There companies must invent the wheel again always with different supplier. There are no ready-made practices for supply chain security. Standards and requirements frameworks should be clear, control objectives are defined, and which risks responding to, but they do not tell how to respond. Big nuisance is contract making with customers, partners, vendors, and other parties, they all come with their own template, and from their own contract culture, there might come conflicts.

Before business networking when companies had everything with themselves, and things were done using waterfall methods, and there were checkpoints, it was much easier than today. In DevOps world there are releases made frequently and meaning of testing has increased. On the end there it is how well that coder or developer know how, realize, wants, or bothers to take security factors into account. There verifying is lighter, and we must trust more to people, developers who are doing these things. In addition, privacy should be mentioned in this context, because it is also big part of this field.

Standards itself do not provide direct solutions, today or in future challenges on information security. There must be somebody who understands links between security standards, business, and processes that organization is running, and can choose most functional models for different situations. There must be always personnel which is interpreting and applying standards in that environment where the organization is operating. Recommendations to practitioners and researchers is to create or if there already is common forums to continue developing those and share insights and approaches so that the strengths and weaknesses of different industries could be utilized in other industries. When choosing standard for the company, it is essential to understand that different standards fit different kind of environment and size of the company. Most of the cases ISO 27000 is the end goal, but to reach that level might need some other standards first.

Questions of this research are basically made based on the literature review and trying to complement it and fill in the gaps in the literature with practical knowledge and wisdom. So, answering the question would this process where this research has been done be replicable is difficult, but the answer would be yes. So, we can say that this research is reliable. We believe that validity of this research is at least in good level. The aim of this research is to build a road map for the information security in the company. This research is high level approach, and it does not go to details. Questions for the interview were made based on the literature review and complement that with practical point of view of those theoretical issues. The lack of time prevented to get more interviews. Bigger sampling group could produce more information and make it easier to find

differences between companies for example in terms of size, and information would be easier to classified.

There were no biases found in this research. There might be biases in answers of interview, for example there were contradictory opinions about weakest link in IS. People who had background from the financial sector emphasized that people are not the weakest link, and at the same time interviewee from technology industry do vice versa and claim that it is exactly people who are the weakest link in the IS. There were also buyer and seller approach among the interviewed meaning that sometimes IS issues are demanded from the company and sometimes they are demanding IS issues from their supplier. Used sources were reliable, and they are documented in this paper, except of those who were interviewed. IS standards and methods will develop over the time, but basic assumption is that information on this research will mainly remain over the time and in the different circumstances. Answers in the interviews from different interviewees were supporting each other. At least some of these findings are possible to extrapolate, meaning that they are possible to transfer to other settings or group. Realities of this research have been presented in as faithful and as fair way as it was possible at the time.

7 References

Ahogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology, 2*(64), 540-549.

Airfocus. (2022, February 18). *airfocus*. Retrieved from Roadmap: https://airfocus.com/glossary/what-is-a-roadmap/

Alastalo, M., Åkerman, M., & Vaittinen, T. (2017). *Tutkimushaastattelun käsikirja.* (M. Hyvärinen, P. Nikander, & J. Ruusuvuori, Eds.) Tampere: Vastapaino.

Alecu, F., Pocatilu, P., & Capisizu, S. (2011). Project Management with IT Security Focus. *Jounal of Mobile, Embedded and Distributed Systems*, 186-192.

AlHogail, A. (2015). Desing and validation of information security culture framework. *Computers in Human Behavior*(49), 567-575.

Austin, R. D., & Darby, C. A. (2003). The Myth of Secure Computing. *Harvard Business Review*, 120-138.

Banica, L., Radulescu, M., Rosca, D., & Hagiu, A. (2017). Is DevOps another Project Management Methodology. *Informatica Economica*, 39-51.

Barman, S. (2002). *Writing Information Security Policies.* Indianapolis: New Riders.

Baskerville, R., & Dhillon, S. D. (2008). *Information Security Policy, Processes, and Practices.* Armonk: AMIS.

Brown, S. (2018, August 6). *Rutter Networking Technologies*. Retrieved December 10, 2021, from 3 Essential Components of Your IT Security Roadmap:

https://www.rutter-net.com/blog/3-essential-components-of-your-it-security-roadmap

Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture Through SABSA. *Information Security Journal: A Global Perspective*(21), 47-54.

Caelli, W., Longley, D., Shain, & Michael. (1989). *Information Secuiryt for Managers.* UK: Stockton Press.

Carlos, R., Amaral, D. C., & Caetano, M. (2018). Framework for continuous agile technolgy roadmap udating. *Innovation & Management Review*, 321-336.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for evaluating IT security investments". *Communications of the ACM*, 87-92.

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computer & Security*, 72-94.

Dhillon, G. (2001). *Information Security Management: Global Challenges in the New Millennium.* Hershey: Idea Group Publishing.

Diesch, R., Plaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, 1-21.

eduonix. (2016, Sebtember 8). *Networking and Security*. Retrieved from Learn Different types of Security Controls in CISSP: https://blog.eduonix.com/networking-and-security/learn-different-types-security-controls-cissp/

Fang, Y., Liang, Q., & Jia, Z. (2011). "Knowledge sharing risk warning of industry cluster: and engineering perspective". *Systems Engineering Procedia*, 412-421.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 410-430.

Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes. *Computers & Security*, 234-242.

Garcia, S., Lella, I., Malatras, A., Theocharidou, M., Tsekmezoglou, E., & Valeros, V. (2021, October 27). *Threat landscape for supply chain attacks.* European Union Agency for Cybersecurity. Retrieved January 27, 2022, from https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Günther, K., & Hasanen, K. (2022, January 31). *Laadullisen tutkimuksen verkkokäsikirja*. (J. Vuori, Editor) Retrieved from Tapaustutkimus: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/tapaustutkimus/

Hakala, M., Vainio, M., & Vuorinen, O. (2006). *Tietoturvallisuuden käsikirja.* Jyväskylä: Docendo Finland Oy.

Harris, S. (2006, August 17). *Techtarget*. Retrieved May 31, 2021, from Information governance: http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1211236,00.html

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems*, 373-384.

Hellriegel, D., Slocum, J. J., & Woodman, R. (1998). *Organisational behavior* (8th ed.). Cincinnati, OH: South-Western College.

Hirsjärvi, S., & Hurme, H. (2001). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö.* Helsinki: Yliopistopaino.

Hyvärinen, M., Suoninen, E., & Vuori, J. (2022, February 11). *Laadullisen tutkimuksen verkkokäsikirja*. (J. Vuori, Editor) Retrieved from Haastattelut: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelut/

Iltasanomat. (2022, January 10). *OP:n verkkosivut kaataneen kyberhyökkäyksen tekijöistä tai motiivista ei ole vielä tietoa*. Retrieved January 26, 2022, from https://www.is.fi/taloussanomat/art-2000008528707.html

ISACA. (2012). *COBIT for Information Security.* Rolling Meadows: ISACA.

ISO/IEC. (2018). *Information technology - Security techniques - information security mangement systems - Overview and vocabularity.* Switzerland: ISO/IEC.

Jansen, W. (2010). *Directions in Security Metrics Research.* Diane Publishing.

Kallio, A. (2022, February 18). *Laadullisen tutkimuksen verkkokäsikirja*. (J. Vuori, Editor) Retrieved from Litterointi: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-prosessi/litterointi/

Lee, W., Fan, W., Miller, M., Stolfo, S., & Zadok, E. (2002). "Toward cost.sensitive modelling for intrusion detection and response". *Journal of Computer Security*, 5-22.

Malatras, A., Lella, I., Theocharidou, M., & Tsekmezoglou, E. (2021, July 29). *Enisa Threat Landscape 2021.* European Union Agency for Cybersecurity. Retrieved January 27, 2022, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Malcolmson, J. (2009). What is security culture? does it differ in content from general organizational culture? *43rd Annual 2009 International Carnahan Conference on Security Technology* (pp. 361-366). Carnahan: IEEE.

Martin, J. (2001). *Organisational behaviour.* London: Thomson Learning.

Martins, E., & Martins, N. (2016). *Organisational culture* (3rd ed., Vol. Organisational behaviour). (R. SP., O. A., & R. G., Eds.) Cape Town: Pearson Education.

McLeod, R. J., & Schell, G. P. (2007). *Management Information Systems.* New Jersey: Pearson Prentice Hall.

Merriam-Webster. (2001). *Collegiate Dictionary.*

Miller, L., & Gregory, P. (2012). *CISSP For Dummies, 4th Edition.* For Dummies.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). *Strategy Safari: A Guided Tour through the Wilds of Strategic Management.* New York: Simon & Schuster.

Myers, M. D. (1997, June 1). Qualitative Research in Information Systems. *MIS quarterly*, Living version. Retrieved from https://www.researchgate.net/publication/220260372_Qualitative_Research_in_Information_Systems

MyMG. (2020, February 27). *MyManagementGuide*. Retrieved from MyManagementGuide: https://mymanagementguide.com/basics/project-methodology-definition/

MyMG. (2020, February 27). *Your Guide to Project Management Best Practices* . Retrieved from Project Management Methodology: Definition, Types, Examples: https://mymanagementguide.com/basics/project-methodology-definition/

National Institute of Standards and Technology. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14.* Gaithersburg: NIST.

Osborne, M. (2006). *How to Cheat at Managing Information Security.* Rockland: Syngress Publishing, Inc.

Panetta, K. (2021). *Gartner*. Retrieved January 24, 2022, from https://www.gartner.com/smarterwithgartner/how-to-respond-to-a-supply-chain-attack

ProductPlan. (2022, February 18). *ProductPlan*. Retrieved from Roadmap Basics: https://www.productplan.com/learn/roadmap-basics/

Purser, S. (2004). *A Practical Guide to Managing Information Security.* Norwood: ARTECH HOUSE, INC.

Raggad, B. G. (2010). *Information Security Management.* Boca Raton: CRC Press.

Ramachandran, S., Rao, S., & Goles, T. (2008). Information security cultures of four professions: a comparative study. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 454-454). Hawaii: IEEE.

Rees, J., Bandyopadhyay, S., & Spafford, E. (2003). A policy framework for information security. *Communications of the ACM*, 101-106.

Reynolds, C. (2010). *The Identification of organizational subcultures in an international energy company (Thesis).* New Zealand: Massey University.

Rhee, H., Ryu, Y., & Kim, C. T. (2012). "Unrealistic optimism on information security management". *Computers & Security*, 221-232.

Richot, B. (2013). An Enterprise Security Program and Architecture to Support Business Drivers. *Technology Innovation Management Review*, 25-33.

Roadmunk. (2022, February 18). *Roadmunk*. Retrieved from Why roadmap: https://roadmunk.com/guides/roadmap-definition/

SAP. (2022, February 24). *SAP insights*. Retrieved from What is GRC: https://insights.sap.com/what-is-grc/

SCALED AGILE. (2021, Febraury 10). *Scaled Agile*. Retrieved from Roadmap: https://www.scaledagileframework.com/roadmap/

Schlieger, T., & Teufel, S. (2003). Information security culture:From analysis to change. *South African Journal*(31), 46-52.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *The International Workshop on Trust and Privacy in Digital Business (TrustBus 2003) in conjuction with the 14th International Database and Expert Systems Applications (DEXA 2003) proceedings*.

Shariati, M., Bahmani, F., & Shams, F. (2011). Enterprise information security, a review of architectures and frameworks from interoperatbility perspective. *Procedia Computer Science*, 537-534.

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise Security Architecture A Business-Driven Approach* (First Edition ed.). San Francisco: CMP Books.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*(46), 267-270.

Smallwood, R. F. (2014). *Information governance: concepts, strategies and best practices.* New Jersey: John Wiley & Sons, Inc.

Suomen Standardoimisliitto SFS ry. (2012). *SFS-Käsikirja 327 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät.* Helsinki: Suomen Standardisoimisliitto SFS ry.

Therault, C. (2022, February 24). *TBGSECURITY*. Retrieved from What is an information security framework and why do I need one?: https://tbgsecurity.com/what-is-an-information-security-framework-and-why-do-i-need-one/

Threat Analysis Group. (2020, March 29). *Threatanalysis*. Retrieved from Treatanalysis: https://www.threatanalysis.com/security-risk-management/

Tipton, H. F., & Krause, M. (2004). *Information Security Management Handbook.* Boca Raton: CRC Press Company.

Trice, H., & Beyer, J. (1993). *The cultures of work organizations.* Englewood Cliffs: Prentice Hall.

Van Niekerk, J., & Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *The Information Security South Africa Conference (ISSA2005) proceeding*, 1-13.

Venugopal, I. (2010). *Information Security for Management.* Mumbai: Himalaya Publishing House.

von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security, 7*(1), 50-57.

Vose, D. (2008). *Risk Analyses: A Quantitative Guide.* New York, NY: John Wiley and Sons.

Vuori, J. (2022, January 31). *Laadullisen tutkimuksen verkkokäsikirja*. Retrieved January 28, 2022, from Tapaustutkimus: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusasetelma/tapaustutkimus/

Whitman, M. E., & Mattord, H. J. (2008). *Management of Information Security.* Boston: Thomson Course Techology.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security.* Boston: Course Technology Cengage Learning.

Appendix: Interview questions

1. What are in your opinion best standards and best practices for implementing and maintaining information security?

    a. Strategies

    b. Policy

    c. Standards

    d. Practices, Procedures, and guidelines

2. What kind of project management methods are good for implementing and maintaining information security?

    a. Strategies

    b. Policy

    c. Standards

    d. Practices, Procedures, and guidelines

3. What are the biggest challenges implementing and maintaining information security?

    a. Strategies

    b. Policy

    c. Standards

    d. Practices, procedures, and guidelines

4. What are generally the biggest challenges in information security today and future?

5. How you see project management methods in information security, what is their role and how important are they today, as we see in media constantly these severe information security breaches and intrusions (waterfall vs. agile)?

6. What is the role and importance of Risk Management in IS?

7. What is the role and importance of management in IS?

8. What is the role and importance of culture in IS (internal threats vs external threats)?

9. In your opinion are there any lacks in IS standards and best practices or improvement suggestions?

10. Are there anything else you would like to add into this or are there any suggestions for improvement (SecOps, DevSecOps, Industry 4.0)?