Aleksi Renvall

Improving cybersecurity through ISO/IEC 27001 information security standard

in the context of SMEs

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

26 November 2018

Helsinki Metropolia University of Applied Sciences

Author(s)	Aleksi Renvall
Title	Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs
Number of Pages Date	67 pages 26 November 2018
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Janne Salonen, Principal Lecturer, Helsinki Metropolia University of Applied Sciences

This Master's Thesis targets to several goals. Ambition is to introduce cybersecurity related topics, which are all attached to each other in the big picture and improve information security.

The first section of the research enlightens some of the existing cybersecurity threats and fundamentals of information security. Understanding threats, risks and protection of information have become more important for small and medium-sized enterprises (SME) than ever before.

The second section introduces ISO/IEC 27001 information security standard and its structure. Some of the other popular information security standards and best practices are shortly introduced as well, as they complete use of ISO/IEC 27001 and generally improve cybersecurity.

The last section demonstrates what needs to be taken into account, when enhancing the information security policy from ISO/IEC 27001 point of view. This section also gives insight, what ISO/IEC 27001 standard certification means, demands and how to prepare for ISO/IEC 27001 certification process.

The research does not detail exact technics or instructions how to mitigate threats and build information security management system (ISMS). Instead, the central idea is to raise awareness about the challenges of securing information and how ISO/IEC 27001 standard can be used for improvements in the protection processes.

The main goal of this Master's Thesis becomes fulfilled if SMEs explore this study and begin to consider, what is their individual level of risk management and how cybersecurity could be improved with ISO/IEC 27001 standard. The ultimate goal actualizes if the study manages to point SMEs to get interested achieving ISO certification.

Purpose of the research, besides mentioned objectives, is to educate myself about cybersecurity, information security, ISO/IEC 27001 and other information security standards. Motive for the thesis comes from my own curiosity towards the world of cybersecurity. Method for completing this project is self-study through multiple articles, researches and educational material available on internet and books. Voluminous amount of sources made possible to finalize the Master's Thesis in advance defined time frame and with planned procedures.

Keywords	ISO/IEC 27001, SME, Cybersecurity, Information security, Standard, Risk management, ISMS, Certification

Contents

Abbreviations / Acronyms

ISO	International Organization of Standardization
IEC	International Electrotechnical Commission
SME	Small and medium-sized enterprise
ISMS	Information security management system
IDS	Intrusion detect system
IPS	Intrusion prevent system
IT	Information technology
APT	Advanced Persistent Threat
OWASP	Open Web Application Security Project
InfoSec	Information security
CISQ	Consortium for IT Software Quality
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation
PCI	Payment Card Industry
HID	Human interface device
GDRP	General Data Protection Regulation
DoS	Denial of service
DDoS	Distributed denial of service
IoT	Internet of Things
NIST	National Institute of Standards
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
VPN	Virtual Privat Network
AES	Advanced Encryption Standard
NTP	Network Time Protocol
SYN	Synchronized
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
ERM	Enterprise Risk Management
ACK	Acknowledges
SoA	Statement of Applicability
CISO	Chief information security officer
CIO	Chief information officer
CDO	Chief data officer

1 Introduction

1.1 Cybersecurity and information security

In today's world, there is a new word for traditional expressions *computer security* and *IT security*. One of the most general information sources *Wikipedia* describes term *cybersecurity* as follows:

> "The protection of computer systems from the theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide." [1.]

This description is fairly accurate and cybersecurity is basically connected everything related to information technology and internet. Specially information security has a major interface with cybersecurity, in most contexts these two are even the same concept. The difference is information security's expansion outside of the digital information, still both expressions can be used when discussing protection of SMEs information. Cybersecurity has not only become a fashion word, its meaning in managing and protecting companies business has been lately highly increased. In present day's business world, digital information is the central resource and source of almost all the information companies are possessing. Without access to information, business stops or at least becomes very difficult to run. Important information's integrity, confidentiality and accessibility must be ensured all the time.

Cybersecurity threats and incidents have been rapidly increasing year by year since information technology started to develop. In addition threats and cyberattacks are also evolving to much more complex. This is the vital reason, why all companies should pay attention for improvements with cybersecurity. One of the goals of this Master's Thesis aims to raise SMEs awareness of cybersecurity threats and importance of information security. Chapter 2 of the study concentrates on presenting some top cybersecurity threats and cyberattack vectors SMEs are facing at the moment. Even the same methods are used for cyberattacks against large-scale corporations and governments, are there in those cases elements from other sectors as well. Such things are often involved as spying, cyberterrorism and information warfare. Therefore approach for improving governmental level cybersecurity is considerably more diverse. Chapter 3 presents information security's basic principles and role in companies daily activities. This study does not state exact technical mitigating solutions for incidents or how to prevent threats to

actualise. These procedures are something that every SME needs to define in their individual security policy.

1.2 SMEs and information security standards

According to research of the *Federation of Finnish Enterprises*, 98.8% of all companies in Finland are SMEs with personnel between 2 - 50 persons. That is significant high percentage, as definition of SME is less than 250 employees in a company. 93.3% of companies have maximum 10 employees. In private sector 65% of employees work in companies less than 250 people and output 50% of turnover of Finnish businesses. Number of SMEs are globally quite similar. [2.]

Small and medium size businesses are universally so common that it was obvious to choose approach of this Master's Thesis to be SMEs. Title might also have been *Improving cybersecurity through ISO/IEC 27001 information security standard in the context of organizations,* but large-scale multinational corporations are gigantic and complex wholeness. Even ISO/IEC 27001 standard can be used in all size of companies and organizations, in case of mega enterprises, there are geographically differences with the laws and regulations that must be accounted differently. That approach would have extended this research excessively wide. Alternatively all the topics would have been only superficial. Regardless that scope of the research is for SMEs, introduced matters can be applied to any size company. That is why expressions *company*, *enterprise* and *organization* are used beside SME.

Main focus is on introduction of popular ISO/IEC 27001 standard, and how it can improve SMEs cybersecurity against multiple risks and threats. ISO/IEC 27001 standard's principal purpose is to specify company's individual requirements for ISMS. Rising number of cyberattacks and threats require continuously deeper information security policies and ISMS than before. Micro-enterprises with minimum usage of information technology may not need ISO/IEC 27001 standard but can still get hacked. One network device is enough for exposing company's private matters for cybercriminals. So even SMEs that think they don't need information security, should take care of basic protection. Improving cybersecurity with ISO/IEC 27001 standard in the context of SMEs, as the topic of this thesis is, fit and serve best for the companies that work using information technology and handle classified information.

ISO/IEC 27001 information security standard is a set of best practice instructions, and its flexibility is the reason why it is suitable choice for any company. ISO/IEC 27001 standard presents methods to establish, implement, maintain and improve ISMS. With the standard, each SME can define more effortless own requirements for ISMS and cybersecurity. Use of it is useful already when company wants to simple adjustments for cybersecurity with the minimal budget and without external help. Simple way to explore the standard is for example creating a risk analysis checklist for administration's support. The checklist is convenient way to perform and document continual improvements. With major effort, ISO/IEC 27001 guides to build comprehensive ISMS and security policies for extremely demanding environments.

There are also wide range of other information security standards available for SMEs to achieve better cybersecurity. Depends on the industry and area of the company, sometimes an alternative solution may be more suitable choice than ISO/IEC 27001 standard. Often the best protection is guaranteed if ISO/IEC 27001 is used along other information security standards. This study describes main attributes of some popular standards and best practises such as PCI DSS, NIST CFS, COBIT, NERC and ITIL.

Governmental organizations have created frameworks for IT security as well. In Finland Ministry of Defence have provided two tools for gaining better information security. KATAKRI framework has been planned mainly for helping the authorities organizations, but also companies to determine protection for information and material. VAHTI group has been set up to develop cybersecurity functionality in central government with different surfaces and service providers. KATAKRI and VAHTI are both more wide set of instructions than official standards. In Chapter 4, information security standards and best practises are under closer review.

1.3 Improving risk management and ISO/IEC 27001 certification

Improving risk management of cybersecurity is the central idea of this Master's Thesis, and should be a basic procedure for SMEs or even requirement in some areas. Especially when company practice IT actions, which are related to payment transfers, sensitive information or customer information. SMEs that are already aware of possible security threats and risks, have created security policies for information protection through a collection of processes, tools and procedures. Security policies are contained from fire-

walls, intrusion detection systems (IDS), intrusion prevention systems (IPS), access controls, personnel education and information security standards. All these elements combined together is powerful way to protect information and from what comprehensive ISMS is built.

When SME decides to invest on cybersecurity improvements and establish ISO/IEC 27001 based ISMS, it is very important to have management's support. Full support guarantees continuance with maintaining and improvements, which are probably the two most important part of information security policies. With ISMS, information security policy and risk management are easier to handle and under administrators control. ISO/IEC 27001 standard makes possible to develop suitable ISMS for any level of information security. In Chapter 5, this study concentrates on how ISO/IEC 27001 standard can improve SMEs risk management procedures and cybersecurity.

In the best case scenario, SME may receive ISO/IEC 27001:2013 information security certificate. Target of the certification can be whole ISMS or some parts of it. Certification increase significantly reputation and market status of the company. ISO/IEC 27001 certification indicates that company takes business seriously and information is in safe. SMEs that have a desire to keep their information security maximized, have to be ready to go through regular security audits and certification processes. Chapter 6 of the research describes how SMEs can prepare for certification process.

2 Cybersecurity threats

2.1 Understanding cybersecurity threats

SMEs that focus on having information in order and information security updated, should be primary aware how rapidly situations in cybersecurity sector are changing. Important aspect is also to realize, how extremely common cyberattacks around the world are and how they occur all the time everywhere. Before trying to prevent attacks and minimize risks, SMEs should understand what kind of threats they are facing in daily basis.

Even the smallest SMEs with a single computer for email usage, customer information handling or payment transactions, should take cybersecurity angle into account when performing basic IT actions. Scope for the universal information security incidents is extremely wide. Cyberattacks can be executed from any part of the world by governments, professional hackers, hacktivist groups or just a teenager competing against friends. Attacks may come up in various forms and nobody is guaranteed to be in safe. At the moment, there are no clear rules in cybersecurity world. It even appears to be a trend on the daily news to see clips about massive cyberattacks. Just following the daily media, it is quite easy to realize that for example governmental and corporation calibre cyber spying is a worldwide issue. Seems that even the intelligence agencies are performing reconnaissance actions on each other, and public can see some of this action on the news.

Cyberattacks against SMEs, information warfare and large-scale attacks against governments can be all operate with the same kind of methods. Though bigger operators have more funds and resources in use to execute more comprehensive attacks. Vulnerabilities on networks, devices and applications are universal. Universal are also people, which are considered to be the weakest link of cybersecurity. People can be under influence easily and they are imbalanced compared to machines, even those who are working at highly classified positions. Humanity makes personnel of the companies good targets for phishing campaigns and other scams.

Cyberattack can be straightforward, combination of complex attack vectors or anything between them. Attack might be also just distraction. Fake attacks are often meant to cause visible disruption and distract the attention from the real target. Meanwhile when the target concentrates to mitigate the incident, malwares might be installed or unexpected information is stolen unnoticed. Getting away after an attack, depends totally on

the tactics and skill level of attackers. Defenders success depends on the same matters and this is where information security standards role becomes important.

Motivation for cyberattacks might be spying for the war, stealing business secrets, making money, creating the hacker reputation or anything that benefits criminal actions. Internet as a crime platform has been expanded explosively and offers enormously possibilities for cybercriminals. Same time information security specialists are trying to adjust and develop own skills to manage existing circumstances.

Year by year increased number of cyberattacks is strong measurement how fast digitalization is evolving. Digitalization and fast development of the technics are helping the world in many ways, but there is also another side. Cyberattacks have become extremely sophisticated and Security Analysts around the globe have constantly found significantly more complex attacks. First half of 2017 *F-Secure Labs* detected an overall increase of 223% traffic in its honeypots comparing to second half of 2016. [3].

There are basically no sector or industry today, where information technology is not somehow involved. Attacks are part of the daily life and used for very common things such as political purposes. Investigations suggest that as big events as *United States Presidential campaigns* are being target of possible manipulation by cyber activists. [4.] The exact numbers of yearly information security incidents and attacks are very hard to estimate, as all the companies, organizations and governments do not publish this information.

Figure 1 below shows F-Secure's research about geographical area how cyberattacks have been divided in 2016 and 2017. When investigating the report more carefully, can be seen how attacks are really reaching all over the globe. Even *the Cold War* type of geopolitical tension might exist today between the governments in form of cyberwarfare. When SMEs realize how serious the threats are and how capable the enemies might be, there probably is a bigger chance to receive support of the management to take the cybersecurity seriously.

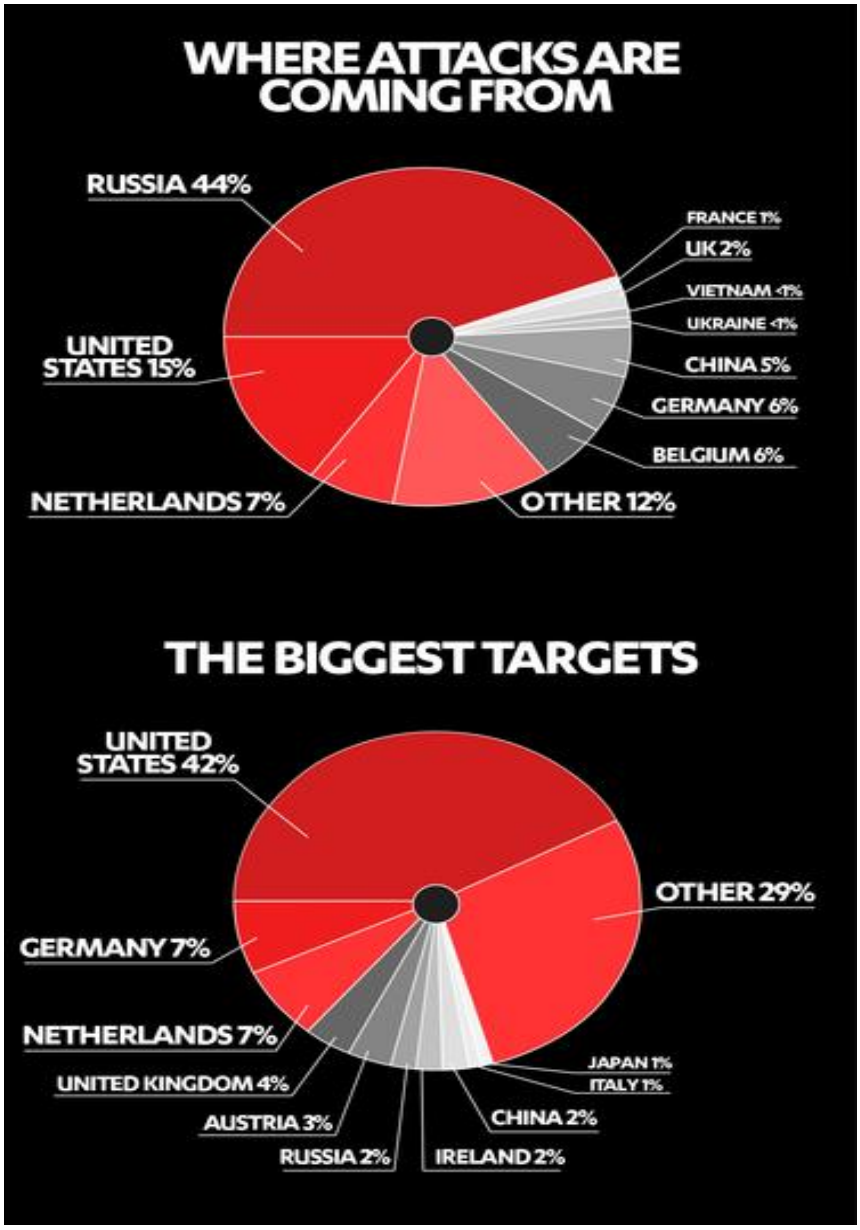

Figure 1. Geographical division of cyberattacks in 2017. [5.]

This chapter introduces some of the most used cyberattack approaches that SMEs IT departments and cybersecurity personnel should be aware of. List of the threats in following subtitles is not complete. Number of the existing threats is so large that introducing everything in this Master's Thesis is not practical. There are probably also totally new threats generated after finishing this part of the study. This Master's Thesis does not provide mitigating instructions. Quality of the mitigation can vary considerably depending on the size, area, wealth and security policies of SMEs. ISO/IEC 27001 information security standard offers guidance for every SMEs own needs for establishing ISMS where risks, threats and solutions are defined.

Chapter 5 in this thesis concentrates more closely on risk management and introduces how ISO/IEC 27001 standard can be used for planning improvements in cybersecurity via risk management procedures. With ISO/IEC 27001 based ISMS, SMEs can be more ready for all the threats listed in this chapter, as well as recover faster if the threats evolve to incidents.

2.1.1 APT

Advanced persistent threat (APT) as its name already suggests, is a complex set of sophisticated and continuous attack techniques. APT aims to achieve unnoticed foothold in a target network or systems. Multiple malwares or other attack vectors are used over a long period of time to exploit vulnerabilities. Usually APT attacks are patient, long-lasting and strictly planned to carefully chosen target. Commonly APT attack follows life cycle, which can be modified depending on how challenging the target is. As Figure 2. shows, APT has various steps. The most complicated APT attacks are often executed by organized and wealthy groups or organizations such as intelligence agencies. Talented hacker groups may also have ability to establish an advanced attack. The main purpose of APT attack is to spy target's information unnoticed long period of time and cover the tracks as good as possible.

Figure 2. Life cycle of APT. [6.]

Great example of APT attack is famous *Stuxnet* worm in Iran in 2010. According many sources, cyber forces from USA and Israel made an attack against Iranian nuclear program. *The New York Times* published an article on 1st of June 2012, how Stuxnet was part of *Operation Olympic Games* by these two nations. Iranian nuclear power plant was not connect to internet and is suspected that worm was installed via existing vulnerabilities with USB flash drive. Once Stuxnet was in the system, it started to send information to attackers management servers. An error in code made possible that Stuxnet managed to propagate itself around the internet and became detectable for researches. [7.]

Stuxnet is one of the best demonstrations of sophisticated cyberattack with great resources, wealth and skills, even it become exposed with small error in the code. Challenge for the SMEs with APT attacks is complexity. Presumably there are always more complex APT attacks taking place than researches can imagine at the time. If this is the case, cybersecurity specialists or departments may not even know what kind of threats they should be looking for. APTs are enormous threat and already justifiable reason to start using ISO/IEC 27001 standard, especially for SMEs possessing sensitive information.

2.1.2 Vulnerabilities

ISO 27005 Information security risk management standard defines vulnerability as:

> "A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission." [8.]

Definition unquestionably states how vulnerabilities are exploitable weaknesses that are used for stealing information or causing problems for the target. Vulnerability itself is just a flaw in a system, application, device or some part of the network. Even with the known and popular vulnerability, attacker still needs technics and tools to exploit the flaw to gain the access to the target.

Vulnerabilities can be found from anywhere at any moment. There are so many attack surfaces in the networks and devices that it is close to impossible for anyone to be totally unreachable from the attackers. Only the most prepared SMEs with sophisticated ISMS and highly skilled personnel can be quite well protected. Even the professionals have problems to stay protected from zero-day vulnerabilities due to unexpected time and

target where vulnerabilities may occur. Vendors provide update patches for zero-day flaws, but patching always takes time and funds when updating infrastructure of larger SME. The most alarming problem is that the targets may have been under the attack long time before zero-day vulnerabilities are even revealed in public. This leaves part of the companies attack surfaces unprotected and under quick decisions in challenging threat situations.

SMEs without well planned risk management policy are popular targets for attackers to perform vulnerability exploiting. Competition on the cybermarkets has been extremely intense for the last years, internet is expanding and number of devices are increasing every day. Existing situation on the markets makes possible to manufacture cheaper and poorly protected devices. Attackers are aware of this and using known vulnerabilities while trying to expose new flaws at the same time. Vulnerabilities are one of the most common threat type and there are several classifications and scoring systems for them, such as well-known U.S. governments *The National Vulnerability Database (NVD).* NVD offers list of *Common Vulnerabilities and Exposures (CVE)* and *Common Vulnerability Scoring System (CVS)* for them. [9.]

New vulnerabilities occur constantly and every year notable cybersecurity companies publish own threat lists, which are quite universal when comparing to each other. Global consulting company *Protiviti's* security labs offers several lists in its *2018 Security Threat Report.* These examples demonstrate few of the lists that are published:

"Vulnerabilities: Top Overall by Count (All Severity – External and Internal):

1. Microsoft Windows Remote Desktop Protocol Server MiTM Weakness | CVE-2005-1794
2. SSL RC4 Cipher Suites Supported CVE-2013-2566
3. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) | CVE-2014-3566
4. SSH Server CBC Mode Ciphers Enable CVE-2008-5161
5. SSL Certificate Signed Using Weak Hashing Algorithm CVE-2004-2761
6. Microsoft Windows SMB NULL Session Authentication CVE-1999-0519

7. SSL Version (v2) Protocol Detection
   CVE-2005-2969

8. SSL / TSL Renegotiation Handshakes MiTM Plaintext Data Injection
   CVE-2009-3555

9. TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
   CVE-2014- 8730

10. HTTP TRACE / TRACK Methods Allowed.
    CVE-2003-1567. ” [10.]

“Top 10 External Exploits:

1. Apache HTTP Server Byte Range DoS

2. MS15-034:Windows HTTP.sysRemote Code Execution Vulnerability

3. Apache 2.2<2.2.22 Multiple Vulnerabilities

4. Open SSL AES-NI Padding Oracle MitM Information Disclosure

5. MS15.004:Windows SMB Remote Code Execution (EternalBlue)

6. Microsoft Windows Unquoted Service Path Enumeration

7. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POO-DLE)

8. MS17-010:Windows SMB Remote Code Execution (EternalBlue)

9. PHP<5.3.9 Multiple Vulnerabilities

10. Cisco ASA/IOS IKE Fragmentation Vulnerabilities.” [10.]

Top 10 External Exploits list do not include severe vulnerability, Microsoft patch MS17-010, which was transport method for massive WannaCry ransomware. [10.]

2.1.3 OWASP Top 10

The Open Web Application Security Project (OWASP) foundation, not-for-profit online community is created to provide security documentation, tools and technologies for web applications. OWASP’s most known project is the Top 10 document for web application vulnerabilities. OWASP Top 10 represents the most critical web application security risks, some examples and prevent methods. It aims to raise web application awareness and offers instructions for minimizing risks and recovering from incidents. The Top 10 list is an excellent starting point to take application security more severely. The project is targeted to be adopt by any individual or company that is interested to improve secure use of web applications. [11.]

OWASP Top 10 is regularly updated and latest version - *Application Security Risks 2017* was released in December 2017. Official OWASP Top 10 and short descriptions are presented as follows:

> "A1:2017-Injection
> Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
>
> A2:2017-Broken Authentication
> Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
>
> A3:2017-Sensitive Data Exposure
> Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
>
> A4:2017-XML External Entities (XXE)
> Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
>
> A5:2017-Broken Access Control
> Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
>
> A6:2017-Security Misconfiguration
> Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
>
> A7:2017-Cross-Site Scripting (XSS)
> XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
>
> A8:2017-Insecure Deserialization
> Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
>
> A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring
Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring." [12.]

2.1.4 Phishing

Phishing remains yearly on the top of the most used cyberattack methods. Number of attacks have been increasing more than most of the other cyber threats, besides attacks have been evolving to more intricate. Phishing is commonly carried out by emails, spoofed emails or instant messages. Mass of the spam emails have multiplied four times from year 2016 to year 2017. Reason why phishing has been so used attack type, is simply a humanity. People are naturally curious, want to win prizes and receive discounts. Many are just unaware of phishing threats, so there will always be numerous gullible victims. Strong statement about phishing is that according to *IBM's X -Force* researchers, approximately half of all the emails are spam. Email phishing campaigns will probably stay one of the top attack vectors for long time, as daily email usage is still increasing. [12.]

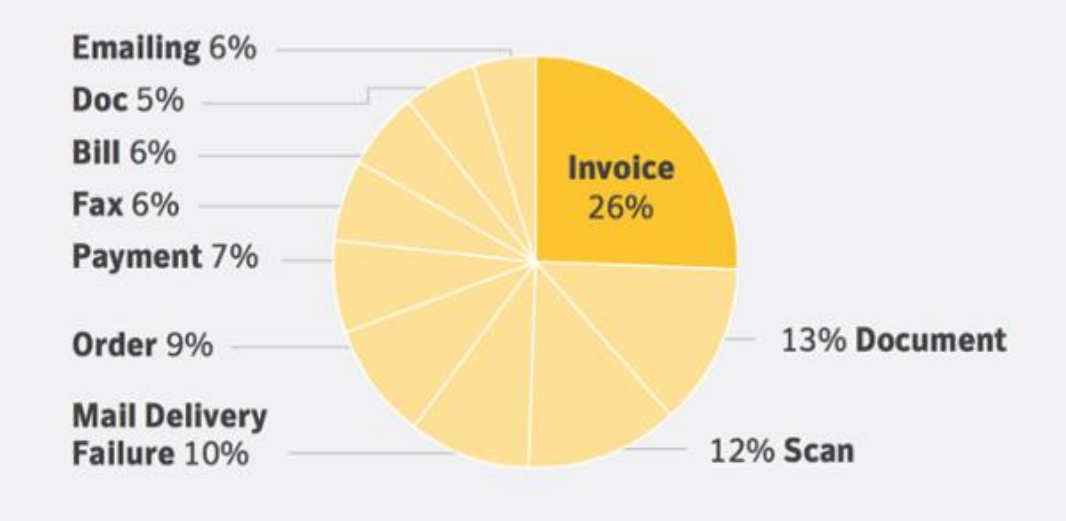

Figure 3. The most used trick tactics with phishing emails from Symantec 2017 ISTR. [13.]

Attackers are not only targeting to cheat ordinary citizens with malicious phishing emails, email is also one of the easiest unauthorized accesses to SMEs network. Companies email addresses are not too difficult to figure out and personnel read private emails at work places. This increases threats significantly. Some companies have strict security policy what personnel are allowed to do within closed intranets, and some of the websites are automatically blocked by antivirus programs. Regardless strict security policies, email traffic always makes companies vulnerable for phishing and spear-phishing campaigns. Single unintentional click on infected link or advertisement may allow attackers payload flow into companies network. Challenge with the email threats is that they are often tailored just for certain person, after gaining specific information with social engineering. Emails may contain detailed information about the person's job tasks, colleagues or company. Emails also seem to be nothing but ordinary email related to daily working tasks.

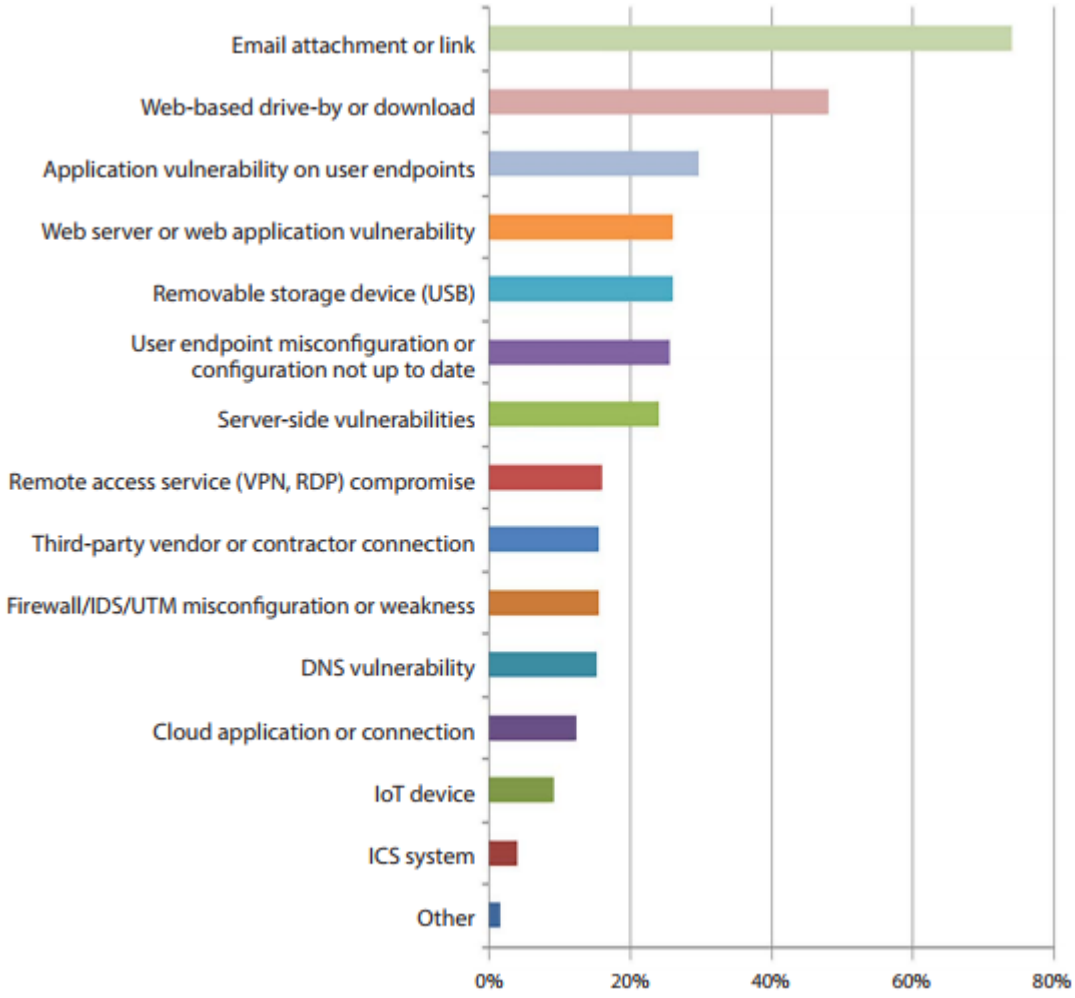

Figure 4. Vectors to enter companies according to SANS 2017 Threat Landscape Survey. [14.]

2.1.5 DoS and DDoS

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are trending cyberthreats at the moment. These attack vectors, specially DoS attack is relatively easy to execute. DoS attack requires only a single device and simple tools, which are easy to purchase from internet. With little bit of knowledge, it is quite easy to send large amount of unwanted traffic to destination IP address and overwhelm victim's services.

Wide study of *University of Twente, UC San Diego* and *Saarland University* have addressed that nearly 30 000 DoS and DDoS attacks are being operated every day. [15.] Volume of the attacks have been significantly increasing in last five years as *Atlas's* statistics in Figure 5. Increase of volume with DDoS attacks. [16.]indicates.

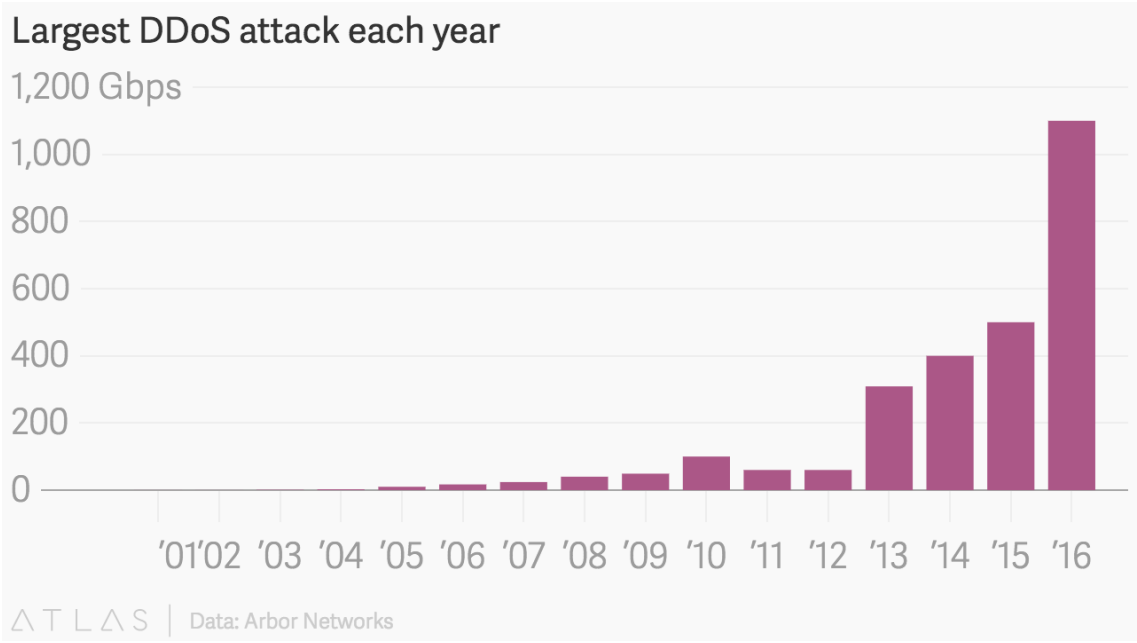

Figure 5. Increase of volume with DDoS attacks. [16.]

DDoS attack is more complex than DoS, but accomplished attacker can find instructions easily from internet. Another, fast and easy way is to purchase tailored attack from *Darknet*. Spreading use of internet and rising number of devices have made own platform for example for DDoS attacks made by IoT devices. IoT based botnets such as *Mirai* and *Reaper* have been massive attacks and disabled large geological areas. Researches have predicted that in a near future, it is possible to execute so powerful DDoS attack that it will take down the whole internet for some time. [15.]

Wednesday 28th of February 2018, the popular developer platform *GitHub* experienced the biggest DDoS attack internet has recorded so far. Powerful attack hit GitHub with the traffic volume of 1.35 terabits per second. Alarming fact is how attack did not use botnets like powerful attacks normally do. Instead it was based on new trend, where attacker spoofs the victims IP address. Then data packets are sent to Memcahced servers, which return the packets back to victims address 50 times bigger. Memcahced servers are originally meant to speed up network functionality and should not be visible to the public internet. Some of the servers are without protection and hackers can use them effortlessly for unauthorized purposes. Taking over of Memcached servers is demonstrative example how hackers are always finding new attack methods. [17.].

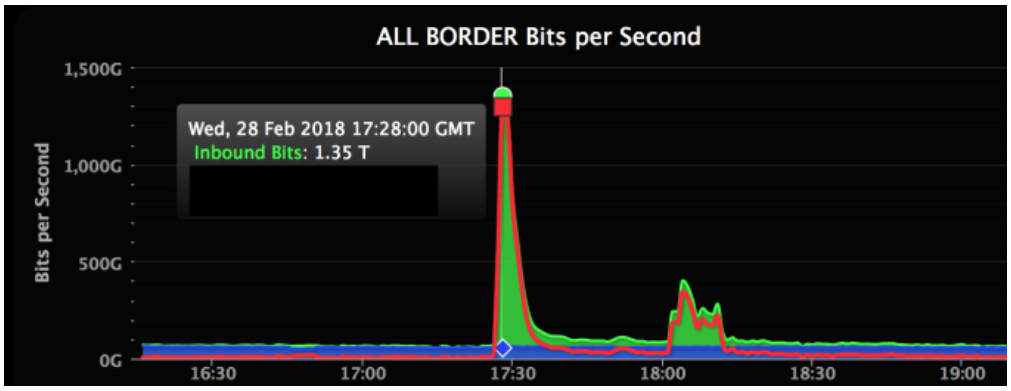

Figure 6. World record DDoS attack against GitHub in February 2018. [17.]

DoS and DDoS attacks are usually designed for volume, protocol or application based cyberattacks. Next paragraphs introduces some of the most common ways how DoS and DDoS attacks are tailored:

- *UDP Flood attack* floods UDP packets to target's random ports. Host starts to check application listening at the ports. When there are no applications, packets with unreachable status are sent back. Eventually this slows the traffic and may cause inaccessibility.

- *ICMP Flood attack* has the same principle than UDP flood. ICMP sends Echo requests, also known as pings packets, to target without waiting replies. Procedure causes significant slowness with the victim's bandwidth.

- *SYN Flood attack* uses weakness in the establishment of TCP connection. TCP needs SYN-ACK answer from the host for SYN request. Answer is not coming or it is coming from spoofed IP address. Eventually this function prevents creation of new connections and attack denies availability of the service.

- *Ping of Death attack* is based on manipulation of IP packets. Fragmented packets are reassembled on the host side and result is larger than packet's maximum size, 65,535 bytes. This may lead memory buffer overflow and services do not work properly or at all anymore.

- *Slowloris attack* is often used for more carefully targeted purposes. This type of DDoS attack is possible to run to take down a single server without causing problems to other servers or ports. Attack is based on sending partial connection requests. As long as concurrent connections are full, additional connections are not possible to establish.

- *NTP Amplification DDoS attack* is named after NTP servers, which are possible to exploit from the public internet. Amplified UDP traffic can multiply traffic even 200 times higher than it originally was, and therefore deny service in the destination.

- *HTTP Flood attack* impacts on server or application by exploiting seemingly legit HTTP GET or POST requests. Target is trying to respond to every request, when maximum resources are reached, high usage of server or application denies services. [18.]

2.1.6 Data storage and physical threats

When stated that cybersecurity threats may come in numerous ways, personnel of SMEs probably not at first consider CD's, external hard drives or USB flash drives. Items and devices, which are not disposed in the right way after companies abandon them, can be considered as a massive security risk. Incorrectly discarded device should be already a failure within information security policy. Hackers have multiple methods to perform forensics for devices and recover even deleted data. Removable data storage devices and equipment may also hide trojans, worms, viruses and any kind of malwares.

USA Department of Homeland Security made a test in 2011 and dropped disks and USB sticks on parking lots of federal agencies and government contractors. As high as 60% of these devices were later connected to networks at the offices. When USB stick had the logo of the Department of Homeland Security on them, percentage rose to remarkable 90%. [19.] Since 2011 personnel's cybersecurity education has decreased the percentage of plugged USB sticks with similar tests. Regardless of training, about half of the USB sticks are still connected to network according to researches. Tests like these are exposing how human curiosity remains as the sore spot of cybersecurity. [20.]

Advanced data storage threats, such as USB look-a-like rubber ducky is a tricky threat and difficult to detect. Target recognizes falsely rubber ducky as a common HID device in its USB port. In reality device is a rubber ducky that executes a payload into the target's system. Depends on the script written on payload, attacker can execute arbitrary code, edit the files and capture or infect the host computer. [21.]

Figure 7. Rubber ducky [21.]

2.1.7 Social engineering

As the previous subtitles already in this research have been stating, mankind really is the weakest link of cybersecurity. This fact comes quite obvious when researching generally social engineering. Social engineering is the way to effect on human behaviour psychologically. Curiosity, gullibility, hurry, angry and sadness are used to trick personnel to grant access to companies facilities, information and systems without hack or physical break in. Emotional behaviour with knowledge of names and titles of co-workers can convince personnel to step outside of the security procedures. Even personnel's

continuous education should be included in a security policy, people are still opening doors for polite business-like people. Same human nature makes people clicking fascinating but harmful links and check what is on found USB stick.

Aspired information might be passwords, access, bank information, information about the personnel or anything that support criminal purposes. Attackers often use plenty of time to search all available information of the target and people around it. After preparation period comes the actual attempt to gain unauthorized accesses. Social engineering is frequently the best option for attackers, especially against the targets with powerful ISMS. Information security company *Lares Consulting's* founder Chris Nickerson has led years penetration testing for customers. One test included research of the target company's information on public sources and convincing reception staff to enter stranger into the building. Nickerson pretended to be Cisco technician on his 4$ Cisco t-shirt and also managed to get access for his team members. Inside the office building Nickerson dropped malicious USB sticks and hacked company's network from inside. [22.]

Nickerson's test is the perfect example how social engineering works at its best. Same kind of procedures are carried out with phone or email. Studying the target carefully for weeks and pretending to be someone, who should get the requested information. Social engineering may be one of the most challenging parts of cybersecurity. In companies there are so many people working on different roles and quick-witted criminals are always ready to take advantage of it. It may take only one open door to enter building or single password to access IT systems. Digitalization also exposes new tricking surfaces, specially between unexperienced IT users, elderly and criminals. Despite strict procedures and security controls, attackers always try old and new social engineering tricks. Risks for criminals from social engineering are relatively low and success high. Social engineering will probably remain in the list of the top security threats as long as humans live on the Earth.

2.1.8 Ransomware

Ransomware in computing language means the same thing than traditional blackmailing. Ransomware's first step is planting the malicious software usually on the victim's computer or server. Malwares that are designed for ransomware, are commonly installed through phishing emails or tricking the target visit on harmful websites. Infection is block-

ing users accesses to systems or encrypt victims data disks. At this point, warning message appears on the screen demanding ransoms, which are often in cryptocurrency. Message includes instructions how to use decryption key and release computer for the victim again, after the payment. [23.]

New era of ransomware has been defined to start in 2013 with *CryptoLocker* ransomware. In five years after CryptoLocker, attackers skills and complexity of ransomwares have increased cumulative according to *CSO Online Media.* Cyber defenders were not ready for such a ransomware as CryptoLocker was in 2013. It managed to surprise many IT users and infected approximately 500 000 machines, some of the owners paid ransoms in prepaid cash vouchers or bitcoins. It is believed that totally 3 million dollars were collected under the attack. CryptoLocker launched the real momentum on development of efficient ransomwares. [23.]

In 2017 the world witnessed probably the two most famous ransomware attacks yet. *WannaCry* received wide media coverage and took over more than 300 000 targets including high level instances such as banks, *United Kingdom's National Health Service* and ISP provider *Telefonica*. WannaCry was spread with EternalBlue exploit, which is originally NSA's design. Another massive attack in 2017 was *NotPetya* ransomware, affecting on as many machines as WannaCry and caused probably even more costs worldwide. NotPetya used EternalBlue as well and started to spread as a fake Ukranian tax-filing update. The biggest challenge with the ransomware extortionist is that there are no guarantees that encrypted disks are set free, even if ransoms are paid. Anyone might get selected to be a victim. Companies without proper ISMS with important data are the most fascinating targets for the hackers. [24.]

2.1.9 Brute-force

Companies with the lack of demonstrative personnel's information security guidance and strong password policy, are always tempting targets for brute-force attackers. One of the most common brute-force attack method is entering as many passwords to log ins in a row that the right password is found. This method is known as a *dictionary attack* and it is operated with simple automatic scripts. Dictionary's database can include passwords from few to millions. Another traditional brute-force attack is operated by entering random combination of letters, numbers and special characters as long as the right combination

is solved. Brute-force attack is also possible to execute also in backwards. In *reverse attack*, redefined passwords are tried to pair with multiple usernames. [24.]

Brute-force attacks are used against multiple targets. Basically everything that is behind username and password combination such as devices, systems, applications, hash, software and services on the web can be the targets. Brute-force attacks can be run on easy or more complex levels. Internet offers several brute-force tools for anyone just to download them without fees. Arguably all these are the reasons, why brute-force is so widely used as an attack vector. Brute-force is also an excellent method for companies to pursuit penetration testing. [25.]

2.1.10 Darknet

Below the visible internet or so called *surface web* is found very wide hidden part of the internet, *the deep web*. The deep web contains approximately more than 90% of all information on internet. Contents are mainly governmental and organizational databases. Along the deep web there is hiding the darknet network, which is accessible only via Tor or some alternative tools or software. The darknet has become extremely popular for criminals, but also for non-criminal users and purposes, because of its anonymity. The darknet creates safe platform for communication between military, law enforcement, journalists and many other group of people who require anonymity. [26.]

The darknet offers perfect platform for criminals. It makes possible to purchase weapons, drugs, contract kills, documents, DDoS attacks or anything that traditional black markets as well. Major concern is how the darknet allows communication possibilities for terrorists and pedophile rings. Exceptionally dangerous is that the darknet brings these markets and anonymities to reachable for anyone who has a basic knowledge of internet usage. [26.]

Last years have made purchasing services and products from the darknet markets common threats for companies cybersecurity personnel. Specially expanding selection and low prices of cyberattacks have already led to stable business models among the hackers and criminals. Below Figure 8. shows some cyberattack products from black markets according to security company *Armor*. [27.]

HACKING TOOLS & SERVICES	
Account Hacking Program	**$12.99** (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts **$15 - $60**
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental **$750** I Monthly Full Rental **$1,200** I Monthly Support **$150**
Disdain Exploit Kit	Day **$80**, Week **$500**, Month **$1,400**
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day **$2,000** Unlimited Traffic, Month **$15,000**
Microsoft Office Exploit Builder	Lite exploit builder **$650** Full Version **$1,000**
WordPress Exploit	**$100**
Password Stealer	**$50**
Android Malware Loader	**$1,500**
Western Union Hacking Bug For World Wide Transfer	**$300**
DDoS Attacks	Week long attack **$500 - $1,200**
ATM Skimmers: Wincor, Slimm, NCR, Diebold	**$700 - $1,500**
Hacking Tutorials	Multiple Tutorials **$5 - $50**

Figure 8. Example of hacking tools and services available on the darknet in 2018. [27.]

2.1.11 Miscellaneous threats

Threats, risks and vulnerabilities may occur in so many different forms that companies that want to be ready for possible incidents, do need systematic approach for risk management. Use of ISO/IEC 27001 is a major step to right direction to achieve this approach. Building comprehensive ISMS is already a next level protection. Smaller SMEs with simple IT can manage cybersecurity without ISMS, but are definitely more safe if at

least some of the cybersecurity risks and threats are recognized. ISO/IEC 27001 standard guides companies to better risk recognition in all circumstances. Every SME need to create own list of the threats they may face. Below is an example of incomplete list about the some of the threats that are not introduced more closely in this Master's Thesis:

- Bomb attack or threat
- Cable security
- Complicated user interfaces
- Contractual breaches
- Damages from 3rd parties
- Disaster caused by human or nature
- Disclosures or leakages after cyberattacks
- Eavesdropping
- Equipment sensitivity to temperature, humidity and voltage changes
- Embezzlement
- Errors by human or technics
- Falsifications and frauds
- Inadequacy at any area
- Lack of security policies
- Lack of documentation
- Legislation breaches
- Misuse of responsibilities or tools
- Physical protection for facilities and persons
- Pollution
- Strikes
- Terrorist attacks
- Testing and maintenance environments
- Thefts
- Too much power or knowledge in one person
- Unauthorized use of access, responsibilities and systems
- Vandalism. [28.]

3 Information security

3.1 Brief history of Information security

Information security or InfoSec, is involved with all the information, physical and electronic. Particularly information security covers all the information that is wanted to keep in safe from any kind of unauthorized use. InfoSec's history can be calculated to as far as c. 50 B.C. and inventor is presented to be Julius Caesar himself. Military commanders and diplomats realized already at ancient times that they need a mechanism for secret messaging. Caesar is the first known practiser for encryption, and today there is cryptographic technique called *Caesar's Cipher* after his invention. Through the centuries governmental messages and mail of important persons have been protected with encryptions, guarded soldiers, sealed boxes and many other inventive ways. [29.]

More complex encryption techniques were developed in the nineteenth century when World Wars created explosively demand for more difficult message cracking. One great example is German's *Enigma Machine* in the Second World War, which is inspiration for numerous movies and books. Enigma Machine's encoding was consider unbreakable, until English computer scientist *Alan Tuning* decrypted the code. Decryption was one of the main attributes that helped the Allies to win the war against the Nazis. [29.]

At the end of the twentieth century, business around internet, computers and telecommunication launched to rocket like growth. Shortly later information security protocols, techniques and systems followed and started to be more popular as well. The new age of computing science and growing number of IT users set new needs and demands also for information security standardization. Anyone, person or company on the internet is not immune for the information security threats. Internet is basically everywhere and expanding as fast as volume of devices. As a result of this, information security standards, models and policies have become or should become part of the basic procedures with SMEs. [29.]

3.2 Principles and key concept of InfoSec

Basic principles with information security in generally have been proposed following features: responsibility, awareness, response, ethics, democracy, risk assessment, security management, possession, implementation, security design, reassessment, availability, utility, access control, data quality, compliance etc. Standards, policies and guidelines

are useful to plan considering all these values. All the most popular standards support these same matters, but main responsibility is with the companies how they carry out own implementations.

Modern day already allows entering to internet with billions of devices almost from anywhere in the world, even during the tourist flights. Cybercriminals of today do not necessarily need to access physically facilities to steal valuable and important information. This angle has redefined the need of information security and current situation requires robust ruleset and standardization. Even there are several information security frameworks and guidance available for free or with low fee, different parts of the world develop unequally. Differences of SMEs information security can be regionally tremendous. Companies that want information security to be up to date, have no options but to obey information security standards such as ISO/IEC 27001.

Committee on National Security Systems official definition for information security states:

> "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [30.]

This definition has several tailored concepts for preventing misuse of information, but from reputation, the most used one probably is the CIA triad model. The CIA model consist of three objectives, which aims to protect IT devices, systems and information. *Confidently, integrity* and *availability* are the core of the model. The CIA triad is considered as fundamental of information security, and is important to keep along already when company starts to design ISMS. The CIA triad model may not be enough specific for all companies when designing ISMS, but adapting ISO/IEC 27001 standard using CIA's objectives guarantees good results. [31.] Next subtitles view shortly meaning of the each CIA objective.

3.2.1 Confidentially

Company's security policy should be particularly strict when handling sensitive or classified information. Basically in today's world, almost every information companies are handling is electric information. Some of the information might be also in form of paper, but sending and receiving information are these days mainly electric transmissions. Lost or

misuse of classified information such as company secrets, government documents, funding information and customer data might lead to serious consequences. Sensitive information of public persons is leaking to media every day, secret agents may get exposed, companies can lose billions of euros or even wars could be started when information handling fails. The CIA triad model enhances protection of information by limiting unauthorized access and use of classified information. Confidentiality in the CIA triad model presents the set of rules that are limiting access to information. [31.]

3.2.2 Integrity

Corruption, manipulation or unauthorized changes of data are all possible with information that is not on secure device, storage or network. Loss of integrity realises when unauthorized changes are made. Unauthorized changes on information may occur unnoticed, by human error or tampering on purpose. Specially on financial industry, robust data integrity is vital to gain the trust for the business clients. Otherwise everyday life in the world does not work properly. The CIA model's integrity emphasizes that all company's data should be classified and therefore stay unchanged, whenever data has been stored, transmitted or used without legitimate need for the action. Performing integrity in the right way with the CIA triad model is indicator that information is accurate and trustworthy [31.]

3.2.3 Availability

Those who are restricted to access the information they should have a rightful access, are experiencing loss of availability. Loss of availability concerns also information, which is erased by unauthorized actions. Cyberattack that prevents access to website or service, is popular attack method and often operated with DDoS techniques. The CIA triad model's availability part supports improvements for authentication and authorization. These two powerful elements together create clear ruleset for information handling, and are automatized to grant or restrict the access. Important part of the security policy is a procedure that confirms the access or attempt of the access took place. Nonrepudiation must be proved with logfiles or some kind of permanent mark in the system. Availability of the CIA triad model is basically guarantee of authorized people accessing the rightful information. [31.]

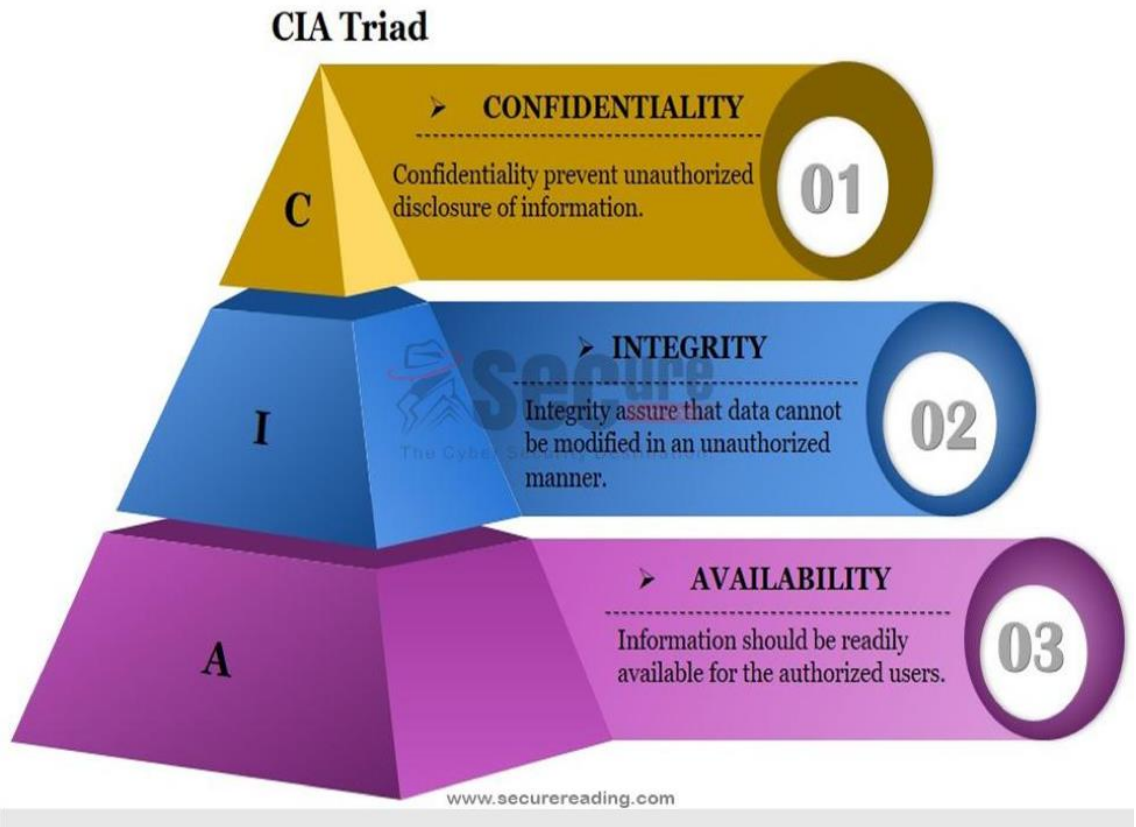

Figure 9. CIA Triad model. [31.]

3.3 Threats, risk management and information security

Threats to information security occur in multiple ways and develop side by side with the technics. Information security threats have been there even before Cesar's days and will be there in the future, as long as people are passing on information. Chapter 2 in this thesis presented some of the top threats of cybersecurity. There are no ready-made prevent systems or ISMS for companies to purchase against information security threats. Definite issue though is that protection is needed, even for the smallest SMEs.

Risk management can be done in several ways. Companies are recommended to hire external specialists and consults to detect their infrastructure and make improvements from the results. Usually these specialists follow known information security standards and frameworks. In bigger companies efficient way to maintain information security is lead it with internal team or department. Smaller SMEs may get educated easier from the courses or just follow existing security guidelines such as ISO, NIST, COBIT, PCI DSS, KATAKTRI etc. Sometimes the best results come from adopting something from

several of them. In following subtitles, some basic parts of information security are introduced. Chapter 5 concentrates more closely on information security risk management from ISO/IEC 27001 point of view.

3.3.1 Security controls

Security controls are purposed to keep information as safe as possible through the CIA triad model's fundamentals, confidentiality, integrity and availability. In a book *Information Security: A practical Approach (*Bhaskar & Ahson 2008) Bhaskar and Ahson are representing that security controls should be chosen considering information system's risk assessment. Processes of risk assessment should be able to identify vulnerabilities and threats of each information system. From the results, suitable security controls are then optimized for risk and incident treatment processes. [32.]

Security controls are divided to three categories, *physical, technical* and *administrative*. Physical security controls consist policy of physical access to premises where company's information is located. Protection can be implemented with guards, door access control, CCTV, antitheft alarm systems, fire alarms, air conditions etc. Technical security controls aim restricting access to technical systems, which are connected to classified information. Technical or logical controls instead may consist from firewalls, IDS, access control, data encryptions etc. Administrative security controls for each company is an individual combination of policies and procedures. Administrative control can be for example education of personnel how to act right and safe in a work environment. Laws and regulations affect strongly on security policies and which security controls are wise to implement. Administrative security control affects with both, physical and technical controls. All these three security control types together create strong protection for information, but without functional ISMS, managing them effectively is difficult. [33.]

3.3.2 Defence in depth and layered security

Concept *defence in depth* originates from military strategy and means more delaying attack than preventing it. In cybersecurity world it is used in the context of *layered security* on information protection. Great examples are honeypots that are made for attracting hackers. Honeypots also enable security specialists investigate cyberattacks to minimize damages in the future. The central idea of defence in depth is to defend attacks on several surfaces with several methods. Layered security operates with the same approach.

In the big picture layered security is part of defence of depth, which is wider wholeness. Defence in depth can be divided to same categories than security controls, which are physical, technical and administrative. These multi surface layered security approaches are quite effective, as each layer provides own protection for the core. Layered security protection is based on collection of tools, hardware, software, security patches etc. Defence in depth instead is more comprehensive concept and includes also such parts as alerts, monitoring, recovery and forensics. [34.]

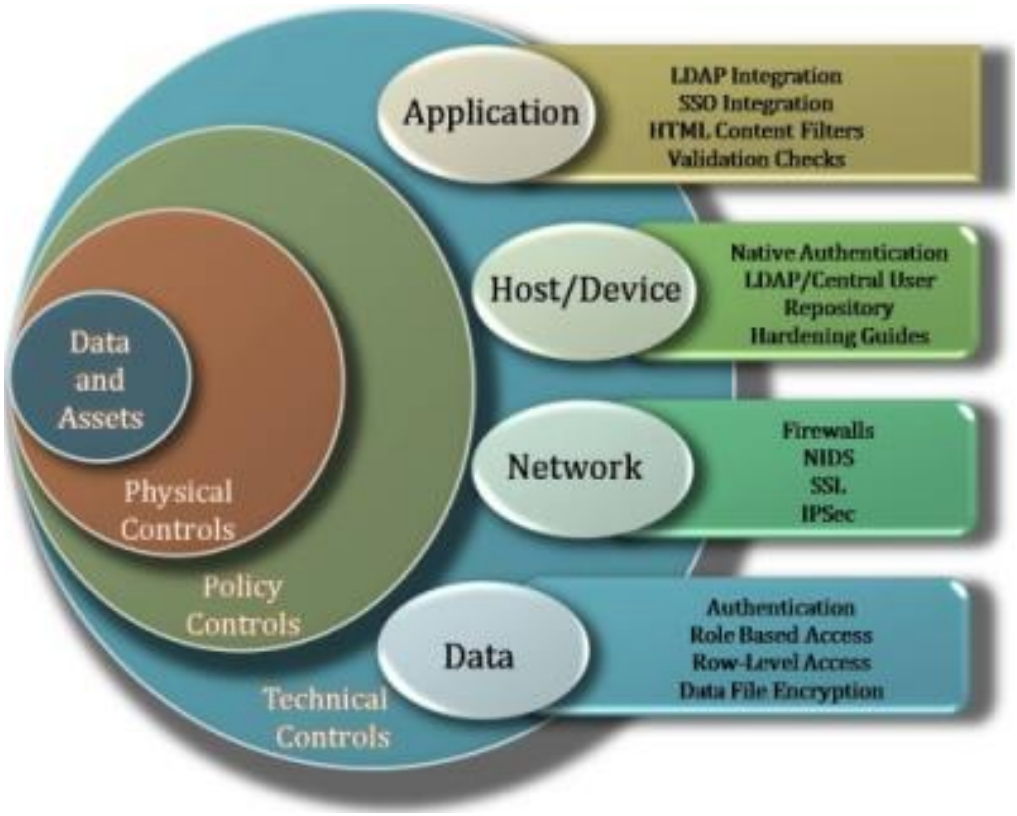

Figure 10. Layered security is sometimes called *the Onion Approach*. [35.]

3.3.3 Information classification and ISO/IEC 27001

Classification of information has been procedure already before time of electronic information technology. When information is mainly on computing devices, system for classification is more complex than just a stamp on the paper. ISO/IEC 27001 standard supports information classification based on confidentiality. In a blog *Information classification according to ISO 27001* (Dejan Kosutic 2018) ISO expert Kosutic suggests that com-

panies should develop individual policy for information classification. This policy is recommended to follow four-step process, which includes asset inventory, classification of information, information labelling and information handling. [36.]

Figure 11. Four-step process for information classification. [36.]

- Asset inventory includes the knowledge of all classified information company possesses and who is responsible of each part of it. Information can be in various forms such as in documents, emails, storages, databases, systems etc.

- ISO/IEC 270001 does not define classification levels for information. Levels should be develop for company's own needs and existing regulations. Commonly in business world classification includes confidential, restricted, internal and public levels. On governmental or sensitive sector, there are more levels such as unofficial, secret, top secret, unclassified and protected.

- Once the company's information classification levels are defined, information must be labelled in the right way. The asset's owner is usually responsible of labelling information of each asset.

- Handling classification of each asset's information is the most slow and complex part of whole classification process. Rules how information is handled, must be created for every asset on every classification level. ISO/IEC 27001 standard provides framework how to go through information classification. The framework is flexible and allows companies to use freedom in creation of individual information classification policies. [36.]

3.3.4 Access control

Processes behind access control consist from combination of *identification*, *authentication* and *authorization*. These three elements are strongly included in the CIA triad model and therefore notable parts of the information security's fundamentals. Identification is authorized normally with username, PIN, password, token, finger print, eye scan or with some other confirmation combination. Some companies prefer even stronger methods when simple authentication procedure is not secure enough. Instead simple combination, two-factor authentication methods have become more popular. Personnel may as well need VPN tunnels, or access through several access servers before being on server where information is located. Once authentication for user is granted, system's rules should automatically know, which information is displayed and what actions user can perform. Company's security policy procedure should first classify sensitivity of all information and then define access controls based on the results of classification. [29.]

3.3.5 Cryptography and ISO/IEC 27001

At present day, information is transferred around the world more than ever before. Companies and business are also more global than ever before. Organizational information, also sensitive is usually sent via emails and online communication services. Information is transferred globally via international core network elements, hosted by international ISPs. Companies support remote work and information is moved around in computers, mobile devices, servers, external hard drives etc. All these are examples, where information is under risks and companies should consider cryptographical actions for better

cybersecurity. In cryptography, the point is simply to protect information from unauthorized use. Information is transformed to unusable form and then returned to usable form for authorized users. Information security is improved significantly with cryptographical methods. [37.]

ISO/IEC 27001 specialist Antonio Segovia presents useful opinions of cryptographic security controls in a blog *How to use cryptography according to ISO 27001 control A.10*. (Antonio Jose Segovia 2018). According to Segovia, suitable and strong enough cipher algorithms, like AES specifications are strong options for encryption implementation. Depends on the level of protected information, there should be suitable cryptographic controls chosen for each asset in a risk management plan. Cryptographic controls can be implemented with several software tools depending of the context. Encryption objects are usually files, hard disks, devices, emails, web transactions, connections etc. Laws and regulations apply between countries and must be taken into account, especially with the global companies. [37.]

3.4 ISMS

Information security management system's core function is to create protection for confidentially, integrity and availability of information. SMEs have freedom to plan their own ISMS as they want, but with frameworks and standards it is faster and easier. ISO/IEC 27001 standard's main purpose is help with definition of requirements for ISMS. ISO Expert Kosutic explains in ISO blog *What is an Information Security Management System (ISMS) according to ISO 27001?* (Dejan Kosutic 2016) that ISMS is the main attribute of ISO/IEC 27001 implementation. [38.]

ISMS is possible to apply to information of some certain part, area or whole company. ISMS is not only a technical approach, it unifies risk management using policies, procedures, processes, people, assets and IT systems. Well planned ISMS is central architect to manage all these elements. Within companies there are not two exactly same kind of implementation with ISMS, as every company with own infrastructure and people is unique. This is the reason why companies must at first when planning ISMS, identify prioritised business processes and needed level of information security. ISMS is recommended to build from risk management point of view. In Chapter 5 of this thesis, founding ISO/IEC 27001 risk management plan is viewed on more profound level. [38.]

3.4.1 Benefits of ISMS

ISMS offers multiple benefits for companies that decide to start using controlled approach for information security. Once ISMS is operational and under administration's management, it also should be continuously under development. Continuity guarantees performance evaluation and improvements, which have an effect on trustworthiness of whole company. Practical ISMS may also bring more stable atmosphere as information security is under control. Surprising benefit is how company's rules and processes are getting indirectly unified, when personnel or all the departments act in the same way with information handling. ISMS may as well save money while it prevents cyberattacks and makes recovery faster after the incidents. ISO/IEC 27001 based ISMS may even earn money as it increases company's reputation and is strong marketing asset. Some of the major benefits of ISMS are:

- Company's information is in more safe
- Less risks and threats becomes incidents
- Unifies processes
- Cost effectiveness
- Need of changes and innovations are easier to detect
- Recovery time after cyberattacks
- Chance to add organizational value with ISMS or certificated ISMS. [39.]

3.4.2 Challenges without information security policy

Since the beginning of the internet, information security threats have increased from year to year. One of the goals of this Master's Thesis is to present how understanding cybersecurity challenges have become more fundamental in digitalizing business oriented world. Part of the goal is enlighten how there are also solutions to get and stay protected with the threats and risks. All SMEs usually are possessing some kind of customer information, maintain online stores, have branch offices or personnel occasionally work from home. Any of these with internet usage are already security risks and expose company for attackers. Some of the hackers are specifically after poorly secured SMEs, just because lack of proper protection and ISMS.

Personnel of companies should use common sense when they perform any actions on internet, and at least some information security rules or policies are needed. One particularly surprising threat is often overlooked, the people, even that is covered with ISO based ISMS. Companies personnel have become one of the biggest threats to information security. Unintended actions and lack of knowledge with basic IT skills are exposing companies for more security risks and threats. Building ISMS is often expensive project and companies should realise to invest also enough for personnel's better cybersecurity education. Management can sometimes be a roadblock and deny cybersecurity responsibilities to invest large amount of money at once in cybersecurity. Even in long distance perspective that would make business more reliable and reduce costs with cyberattacks. Some challenges without ISMS or information security policy may be for example:

- Lower level to end up for victim of cyberattacks
- Unstable atmosphere due the repetitive incidents
- Convince management to understand need for ISMS
- ISMS can be expensive investment in the beginning
- Funds and time for improving personnel's skills. [39.]

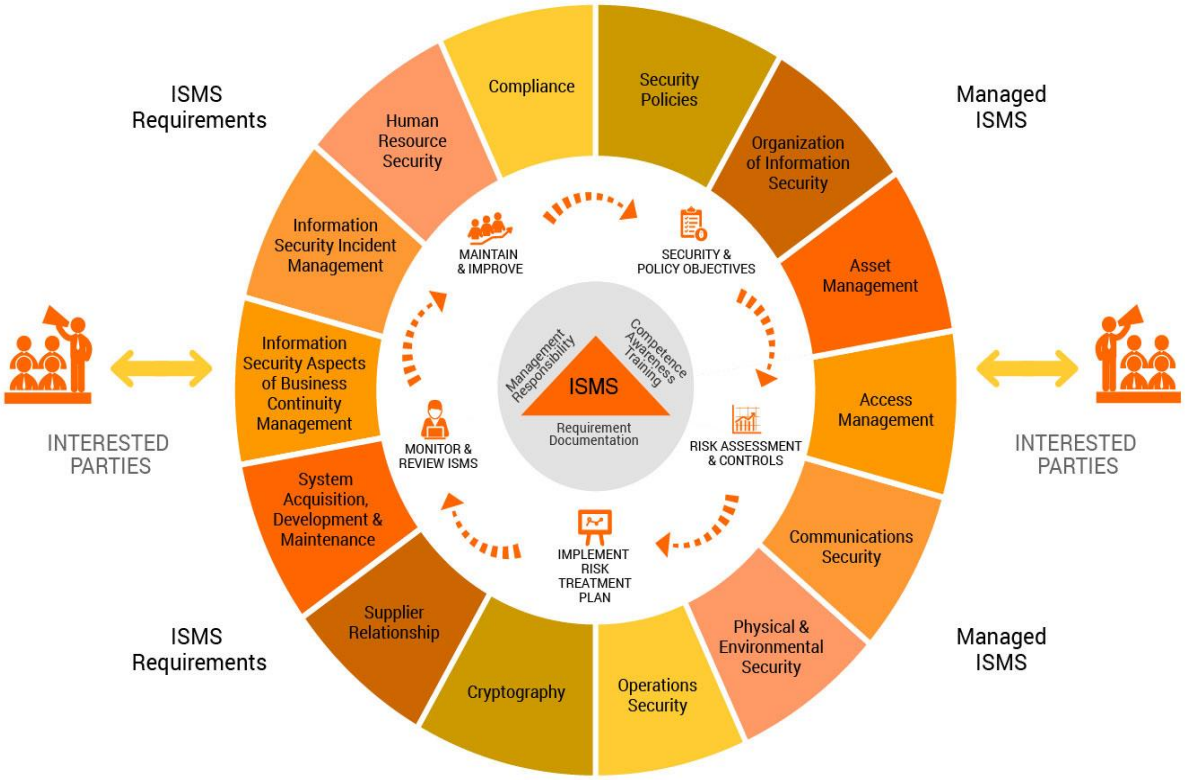

Figure 12. ISMS environment. [40.]

3.5 The EU General Data Protection Regulation and ISO/IEC 27001

The EU General Data Protection Regulation (GDRP) is a massive change in data privacy regulation and will replace 23 years old Data Protection Directive 95/46/EC on 25th of May 2018. The GRPR was created to harmonize data privacy laws for EU citizens in Europe. It also concerns personal data exported outside of *European Economic Area (EEA*) and *EU areas.* Changes are mainly benefits for citizens and demands effort and strict control from companies to update and maintain future's data handling procedures and security policies. Key changes under the GDRP are attached to increased territorial scope and extended jurisdiction of:

- Data processing
- Penalties for companies
- Strengthened consent
- Breach notification
- Right to access personal data
- Data erasure
- Data portability
- Privacy by design
- Data protection officers. [42.]

The GDPR supports companies to use international best practise standards. Use of the standards is proving continuous management of data security. One of the secure options to cover the GDPR is ISO/IEC 27001 information security standard. ISO/IEC 27001 comprehends three indispensable information security aspects, *processes, technology* and *the people*. Implementing information security policy with certificated standard that includes all these three aspects, points strongly that all the sectors of information security are taken seriously. It also indicates that appropriate ISMS has been deployed. With ISO based ISMS, company is also globally under orthodox security policy and in constantly evolving state. ISO/IEC 27001 controls include many similar rules for data security that GDRP demands for preventing data breaches. In *article 32* of the GDRP, there are listed some important information security requirements for companies:

"

- Take measures to pseudonymise and encrypt personal data.
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing." [42.]

Article 32 states as well:

> "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed." [42.]

SMEs that follow ISO/IEC 27001 standard correctly, have all examples above fairly covered. The GDRP does not give step by step instructions how to implement everything what article 32 states. Instead it gives accurate guidance specifications, what needs to be notified effectually to prevent the data breaches. It also recommends companies to adopt information security standards. Standards can be more accurate and help companies to cover GDPR demands. With ISO/IEC 27001 help, it is not only technical measurements which companies are set correctly. Standard also takes account processes and people. ISMS that have policies for auditing, monitoring, maintaining, improving and aims to certification is powerful evidence of company's quality for services. It also offers trust and relief that company's data policy corresponds the GDPR demands. ISO/IEC 27001 standard provides the GDPR compliance for the most parts, but recommendation by *IT Governance* is to use it with framework such as *BS 10012:2017 – Specification for a personal information management system (PIMS)* to achieve the best results. [42.]

4 ISO/IEC 27001 and other information security standards

4.1 Information security standards

Information security standards have been developed by cooperation of specialists and organizations around the world. Official standards are practical, reliable, robust and with good reputation. SMEs that are using information security standards and best practises frameworks are benefitting themselves greatly. Purposes of the information security standards are simply to achieve improvements for company's information security and minimize damages from cyberattacks. Indirectly usage of standards may unify processes, educate personnel and save funds. One of the many useful attributes of information security standards is making management of security policies easier. Information security standards provide planning, implementing and specially maintaining and improving security policies. Once security policy is set to work correctly, it protects assets such as company's information, networks, software, devices, applications, tools, customers and staff.

Depends on the organizational needs, companies can choose suitable standards or best practises from several options. There are many comprehensive standards, which can be certified like ISO/IEC 27001:2013 standard. Standards have been created different areas and industries taken into account. Using more than one information security standard at the same time enhance security. Specially smaller SMEs can benefit from using parts of several standards and best practises without large investments. Benefits of information security standards and certification is reflecting also to business world and may open new business possibilities. In this section of the thesis, ISO/IEC 27001 and some other important information security standards are under closer review.

4.2 ISO and IEC

The International Organization for Standardization (ISO) founded in 1947 is standard-setting organization, composed from non-governmental standards bodies from 162 countries. 776 committees and subcommittees are continuously helping with the product development. Finland's member organization is *Finnish Standards Association (SFS)*. ISO products international standards for almost all the aspects of industries and technologies. Main purposes of ISO are worldwide reliable, safe and quality products, systems

and services. ISO has so far published more than 20 000 *International Standards.* Reputation for ISO specification on products and services have been kept as a safety factor and a benefit in competition on the business markets. [43.]

ISO cooperates closely with *International Electrotechnical Commission (IEC)*, which is another big standardization organization with members from 60 countries. IEC is world's leading organization for preparing and publishing International Standards related electrotechnology. ISO and IEC have founded two joint committees for developing standards and terminology in the areas of electronic technology industries. Official name for ISO/IEC 27001:2013 information security standard comes from comprehensive cooperate of ISO and IEC. [44.]

4.3 ISO/IEC 27001 information security standard

ISO/IEC 27001 standard developed by ISO and IEC cooperation is probably the most popular and highly valued information security standard. ISO/IEC 27000 product family's history starts at late 1980's and ISO/IEC 27001 standard's latest form ISO/IEC 27001:2013 was published in 2013. Standard provides international set of instructions for requirements to build certifiable ISMS. Standard can be used without certification process, for improving cybersecurity to required level. ISO/IEC 27001 does not give specific technical specs how to build ISMS or offer ready risk management models. It is more framework and guidance that companies can use to decide appropriate protection by themselves. ISO/IEC 27001 standard's flexibility enables companies of all size and type, in every industry to use the standard when building, improving or maintaining cybersecurity. Standard is also quite compliance for new requirements coming with massive GDPR changes. [45.]

ISO/IEC 27001 includes ten clauses and Annex A, addendum consists from security controls. ISO/IEC 27001 is strongly related to ISO/IEC 27002, which includes basically the same security controls than annex A. The difference is that ISO/IEC 27001 is certifiable and used for creating risk assessment. ISO/IEC 27002 instead prescribes same security controls than Annex A in ISO/IEC 27001, but more comprehensively. Companies using ISO/IEC 27001 are able to choose suitable controls for its ISMS also outside of Annex A. Those that decide to apply for maximum information security and have plans to achieve ISO/IEC 27001 certification, are recommended to use ISO/IEC 27002 and ISO/IEC 27005 in the process. ISO/IEC 27005 standard concentrates on information risk

management and it is also possible to achieve *ISO 27005 Risk Manager certification* for personnel. [46.] Chapter 5 and Chapter 6 offer a closer look how ISO/IEC 27001 standard can be used to improve cybersecurity of SMEs, and what needs to be taken account in a certification process. [45.]

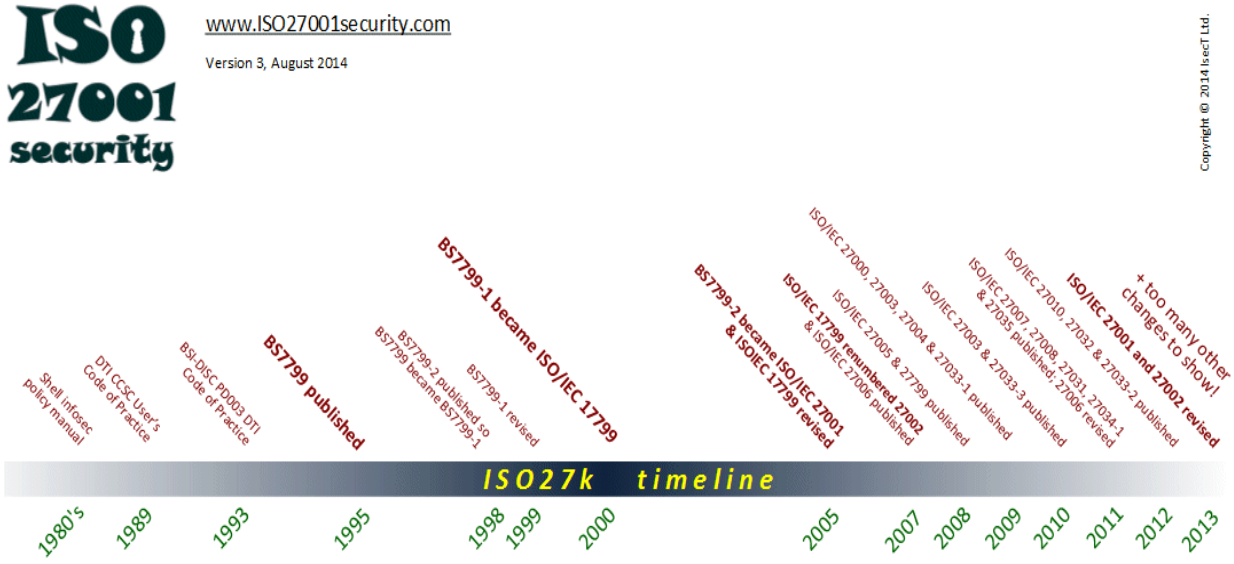

Figure 13. ISO 27k timeline. [45.]

4.4 Structure of ISO/IEC 27001 information security standard

ISO/IEC 27001:2013 standard's latest version's title is *Information technology - Security techniques - Information security management systems - Requirements.* History of ISO 27001 starts 1999, when *British Standards Institutes BS 7799 Part 2 - Information Security Management Systems - Specification with guidance for use* was published. In 2005 standard was renamed for ISO/IEC 27001:2005 with multiple changes in its structure. In 2013 ISO/IEC 27001:2005 was revised to its latest version ISO/IEC 27001:2013. In this revision lots changes were made as well, probably the most notable one was dropping central idea *Plan-Do-Check-Act (PDCA) cycle* out from the contents. Idea of PDCA still exists in 27001:2013 version but it is merged on the clauses. Next two subtitles present topics of the ISO/IEC 27001 clauses and Annex A. [47.]

4.4.1 Clauses and topics

ISO/IEC 27001 includes ten clauses. Each section has own topic, but all the chapters are attached to each other in the big picture and define requirements for ISMS. Structure is easy to follow and SMEs can study the standard without large investments and pick separate parts to improve cybersecurity. Companies that want to build best possible ISMS and certify it, should follow carefully every step. Contents of the clauses are:

"

- **0 Introduction** - the standard describes a process for systematically managing information risks.
- **1 Scope** - it specifies generic ISMS requirements suitable for organizations of any type, size or nature.
- **2 Normative references** - only ISO/IEC 27000 is considered absolutely essential to users of '27001: the remaining ISO27k standards are optional.
- **3 Terms and definitions** - see ISO/IEC 27000.
- **4 Context of the organization** - understanding the organizational context, the needs and expectations of 'interested parties' and defining the scope of the ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" the ISMS.
- **5 Leadership** - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.
- **6 Planning** - outlines the process to identify, analyse and plan to treat information risks, and clarify the objectives of information security.
- **7 Support** - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
- **8 Operation** - a bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).
- **9 Performance evaluation** - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.
- **10 Improvement** - address the findings of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS." [47.]

4.4.2 Annex A and topics

ISO/IEC 27001 includes comprehensive list of security controls and objectives called Annex A. Annex A consists from 14 clauses that include 35 controls categories and 114 controls. The most important change in the latest version of ISO/IEC 27001 is how Annex A's controls are not anymore a requirement to manage risks that are identified in a risk assessment. Use of the security controls are optional and companies can choose suitable controls for own needs. Controls have also been updated to correlate technology such as cloud computing. Freedom with the control use can be seen as companies are

receiving ISO/IEC 27001 certification, even Annex A's controls are not used at all. Though Annex A control set is quite comprehensive and companies find many of them useful. Annex A have the same security controls that appear in ISO/IEC 27002 standard. Difference is that controls are explained much more detailed in ISO/IEC 27002. ISO/IEC 27001 and 27002 together are powerful tool for managing security of information. In following list, there are expressed the topics of each 14 sections from Annex A:

"

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resources security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operational security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance." [48.]

4.5 VAHTI

There are information security standards developed inside Finland's borders for Finnish organizations and companies as well. *The Ministry of Finance* has created steering group and security framework guidance called *the Government Information Security Management Board, VAHTI*. The goal of the framework is develop and enhance information security in central government. VAHTI has very comprehensive instructions to compare to any set of information security instructions in the world. These instructions are available for everybody on Ministry of Finance website. The oldest instructions are from end of the 90's and VAHTI has been under development ever since. Today VAHTI concentrates on providing guidelines and policies for government's organizations in cybersecurity and information security. Main focus is on digitalization, artificial intelligence, robotics and on digital personal data, which is strongly attached to new data protection legislation the General Data Protection Regulation 2016/679 (GDPR). [49.]

VAHTI has been gathered from various global security standards such as ISO/IEC 27000, PCI-DSS, ISG-SOGP and several Finnish laws and regulations. New period for VAHTI has been set for 2017 - 2019 by Ministry of Finance. It is mainly intended for

governmental use, but can be helpful for SMEs as well. Challenge for SMEs might be complexity, as VAHTI is carefully detailed from governmental point of view. [49.]

4.6 KATAKRI

KATAKRI like VAHTI, is a collection of information security instructions from several sources. KATAKRI is planned to use for national security purposes in Finland. It performs more as an auditing tool for authorities than information security standard. KATAKRI is led by the Ministry of Finance in cooperation with authorities and the business community. First version was published in 2009 and has been approved by collaboration of NSA's workgroup in 2015. Main use for KATAKRI is to assess the target organization's ability to protect classified information of authorities and evaluate security of the authorities information systems. It is also helpful for organizations and companies for assessing security arrangements and developing security policies. [50.]

KATAKRI does not demand any exact requirements for information security. Guidance is based on a collection of Finnish national legislation and international obligations for information security bound to Finland. KATAKRI has three main subdivisions, *Security management, Physical security* and *Information Assurance*, which all have several subdivisions of more detailed instructions. [50.]

4.7 PCI DSS

Information security standard sector has security standards targeted only for payment card industry. *The Payment Card Industry Security Standards Council* is a global open body independent council, managing *Payment Card Industry Data Security Standards* for manufactures, software developers and service providers. Council was founded in 2006 by *JCB International, American Express, Discover Financial Services* and *Visa Inc*. Council's main tasks are promote, evolve and maintain PCI standards. Tasks aim to protect card holders data and guarantee safe use of payment cards for card holders and service providers. Council also provides help for vendors and merchants with technology, penetration testing, education and implementing standards and security policies. [51.]

Council's leading standard is the *Payment Card Industry Data Security Standard (PCI DSS)*, which is used widely around the world with merchants and service providers. Regular people may not even have heard about the standard, still it is attached to hundreds of millions of people every day. International payment card companies are setting year by year more strict requirements for merchants, how to handle credit card payments and card holders information. Companies need to be compliance with PCI DSS if they are storing, accepting or transmitting credit card information. PCI DSS includes wide set of requirements and control objectives as ISO/IEC 27001 does as well. Requirements that need to be fulfilled by merchants and service providers depend on processing volume of the payment cards. Even PCI DSS is comprehensive information security standard, companies are using ISO/IEC 27001 along with it, for gaining the best possible level of information security. [52.]

4.8 NIST CFS

Another popular information security standard for private sector organizations and individual businesses is the voluntary *NIST Cybersecurity Framework (NIST CFS)*. Standard is provided by *National Institute of Standards and Technologies* and operates under *United States Department of Commerce*. First version was published in 2014 and the latest 1.1. version on April 16th 2018. NIST CFS targets reliable function of critical infrastructure and assesses information security risks companies may face. Framework has been divided to three parts which are *Core, Profile* and *Framework Core*. Under Framework Core are the five main functions:

- Identify
- Protect
- Detect
- Respond
- Recover. [53.]

These five functions have 22 categories and 98 subcategories, which include wide variety of cybersecurity related activities. References have been made to several information security standards, including ISO/IEC 27001. [53.]

4.9 COBIT

International Systems Audit and Control Association (ISACA) established in 1996 IT management framework called *Control Objectives for information and Related Technologies (COBIT).* COBIT's main focus is on areas of IT management and IT governance. Information security add-on was published to the latest version COBIT 5 on December 2012. COBIT 5 was planned to help with organizational IT growth by combining best practises and standards to develop easier management processes. COBIT's perspective to develop IT is on overall risk management and information security. COBIT's Framework is recommend to be used along with other information standards such as ISO/IEC 27000 family or ITIL. Organizations can receive COBIT certification from ISACA. Control Objectives consists from five components:

- Framework
- Process descriptions
- Control objectives
- Management guidelines
- Maturity models. [54.]

COBIT's main goals are:

- Streamline information sharing across an organization
- Reach corporate goals by incorporating IT into the strategy
- Minimize and control information security and risk management
- Optimize the cost surrounding IT and technology
- Better integrate ISACA research and the COBIT framework. [54.]

4.10 NERC

The North American Electric Reliability Corporation (NERC) is an international not-for-profit corporation founded in 2006. NERC's main responsibility is to reduce risks and raise security of the grid. NERC develops *Reliability Standards* for operating and monitoring the bulk power systems. It also provides education, certification and enforce compliance of the standards use. NERC's most popular standard is NERC 1300, which is called *CIP-002-3 (Critical Infrastructure Protection).* Standard includes risk management and administration from information security point of view in the networks. [54.]

4.11 ITIL

Information Technology Infrastructure Library (ITIL) is a best practice framework for managing and leading IT services. ITIL was developed by *British government's Central Computer and Telecommunications Agency (CTA)* in the 1980's. From early days it has been developed through many forms to its latest one, *ITIL 2011*. ITIL underpins I*SO/IEC 20000 IT service management*. They complement each other but have differences as well. Other information security standards such as COBIT, can be used along with ITIL for achieving high level of information security and IT management. ITIL aligns IT services working more seamless with the needs of business. Framework concentrates on many areas attached to business, including customer relations, cost-effectiveness, improving risk management and IT environment. ITIL is not information security standard, but it is comprehensive set of best practices and has strong bridge to information security. ITIL has a covered process called *Security Management,* which is based on ISMS and security controls on ISO/IEC 27002 information security standard. [56.]

ITIL Certification includes five levels. Every level indicates deeper skills and understanding of the framework. Taking ITIL courses are popular in the companies to make personnel understand IT management, even certification tests are not taken. Levels for the ITIL certification are:

- Foundation
- Practitioner
- Intermediate
- Expert
- Master. [56.]

ITIL framework has been divided to five broad categories, which have various subcategories. Main categories are:

- ITIL Service Strategy
- ITIL Service Design
- ITIL Service Transition
- ITIL Service Operation
- ITIL Continual Service Improvement. [56.]

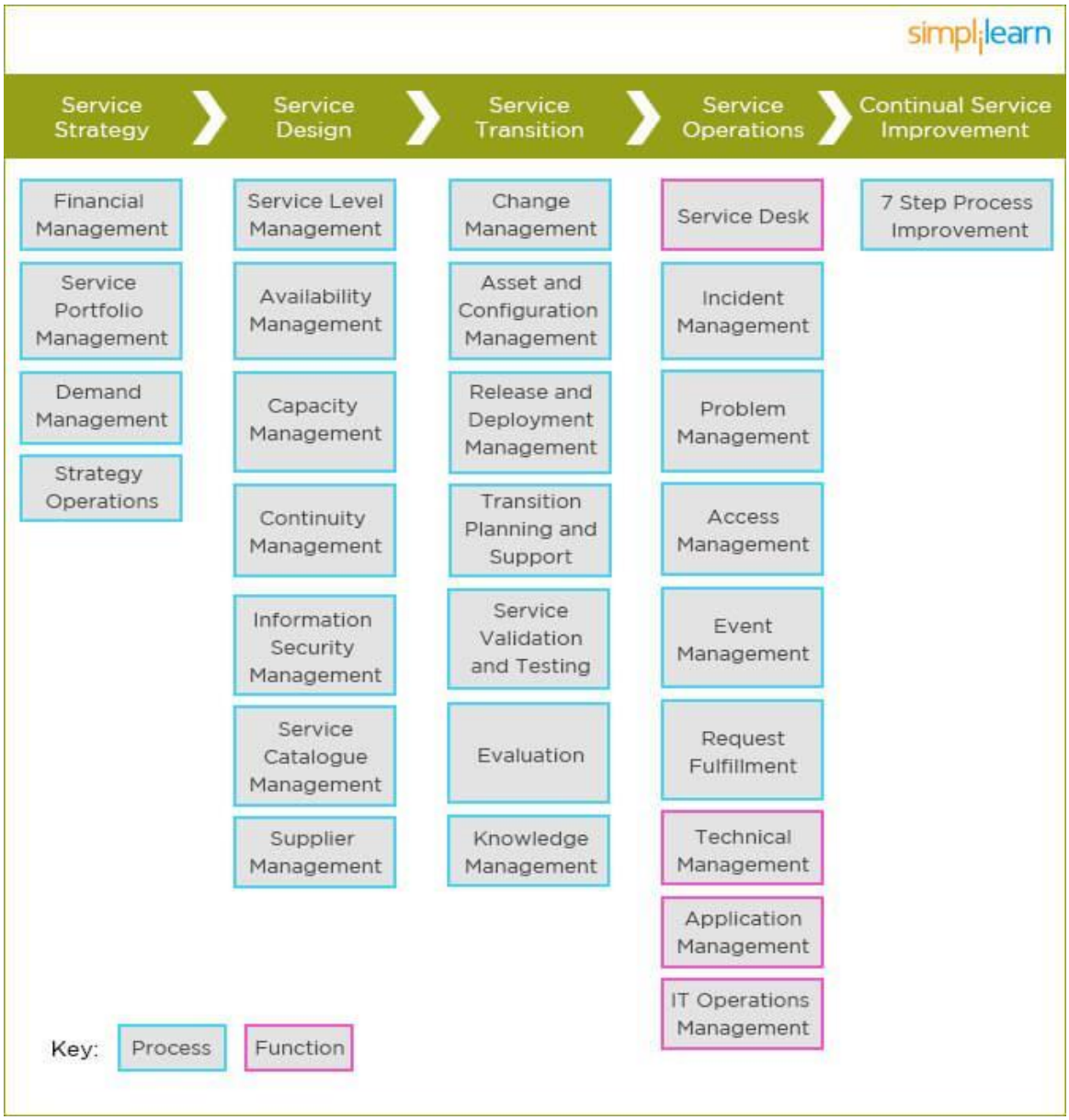

Figure 14. ITIL Broad and subcategories. [57.]

5 Improving cybersecurity through ISO/IEC 27001 standard

5.1 ISO/IEC 27001 for SMEs

At present-day main part of the business takes place digitally and is handled electrically. Still information in physical form should not be totally forgotten. Knowledge and effort are demands when covering carefully SMEs security policies. Basic assumption among the customers is that information is in safe from any unauthorized use. Development and maintain of information security policy is much easier with organized approach with information security standards. ISO/IEC 27001 information security standard is proved to be very functional and useful standard by numerous of SMEs worldwide. ISO/IEC 27001's flexibility makes it popular between all kind of companies. That flexibility makes it possible for small SMEs to pick up some useful information without costs, and at the same time standard supports enterprises to build large-scale ISMS.

SMEs practise increasingly business globally. When companies want to make sure that information is in safe, several frameworks are recommended to use simultaneously. For example ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and GDPR instructions together is a comprehensive combination. In this chapter, research focuses on main points where SMEs should concentrate when starting to plan improvements for cybersecurity. Chapter demonstrates steps when implementing ISMS from ISO/IEC 27001 point of view. In Chapter 4 presented structure of ISO/IEC 27001 and topics of the 10 clauses include all the steps that are used in this section of the research. Chapter presents the big picture about the process of implementing and meaning of the risk management for SMEs. [28.]

5.1.1 ISO 27001's relation to ISO 27005 and ISO 31000

There is own ISO guideline purposed for any type of risk management, *ISO 31000:2018, Risk management - Guidelines* provides process just for risk management. ISO 31000 guideline includes principles, glossary, terms, PDCA (plan-do-check-act) cycle and other best practises. PDCA cycle was long time central element and commonly used procedure for risk management. It was used to help controlling business continual with companies on every area. PDCA cycle was still visible part of ISO 27001:2005 standard but it is not anymore displayed expressly in ISO 27001:2013 standard. In the latest version its functionalities still exist, but are merged into clauses. ISO 27001 suggests that ISO

31000 is useful on external and internal contexts when implementing risk management, but use of it is not mandatory for ISMS. [58.]

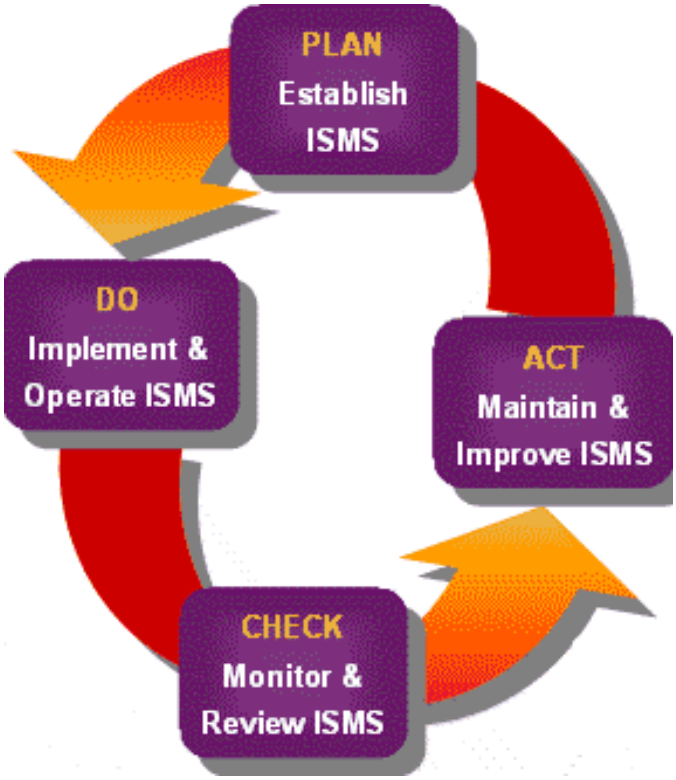

Figure 15. PDCA cycle. [59.]

ISO 31000 does not give specifically instructions for information security risk assessment, as it is designed framework for risk management in all areas. Instead ISO 27005 is perfect add-on to use with ISO 27001 for maximizing information risk management abilities. ISO 27005 is tailored for information security risk management from assessing and treating point of views. It provides help for identifying threats and assets, but also assessing probabilities and consequences of the risks. ISO 27001 requirements and ISO 27005 are both compliant with ISO 31000. Benefit from using ISO 31000 with ISO 27001 and ISO 27005 is, as mentioned previously, to identify external and internal contexts more deeply in risk management. With combination of these three ISO standards, corporation level risk management comes easier to understand and handle. It also indicates for customers and potential customers that risk management is well planned and on comprehensive level. When processes are all under unified managing, the framework can be base for *Enterprise Risk Management (ERM)*. ERM covers and leads every area of risk management for whole enterprise. [28.]

5.2 Risk management as a base of ISO/IEC 27001 ISMS

Risks, threats and incidents occur all the time and everywhere in cybersecurity environments, even against the strongest possible information security policies. Though it is possible to reduce some of the risks and threats becoming incidents, if the risk management is performed in the right way. The best way to operate it, is unquestionably comprehensive ISMS. Stated in a simply way, risks found in risk assessment need to be treated with suitable information security controls. Each SME has individual implementing process, even the framework with ISO/IEC 27001 information security standard is always the same. Everything starts with understanding and assessing the risks. To do so, there need to be a broad-minded management behind cybersecurity related decisions. Good management should understand importance of security policy from every angle, and that there need to be responsible for ISMS or for different parts of ISMS. Practical ISMS is in receptive and evolving continuously due to changes with the markets, technics and risks. Next subtitles address general steps when defining ISMS.

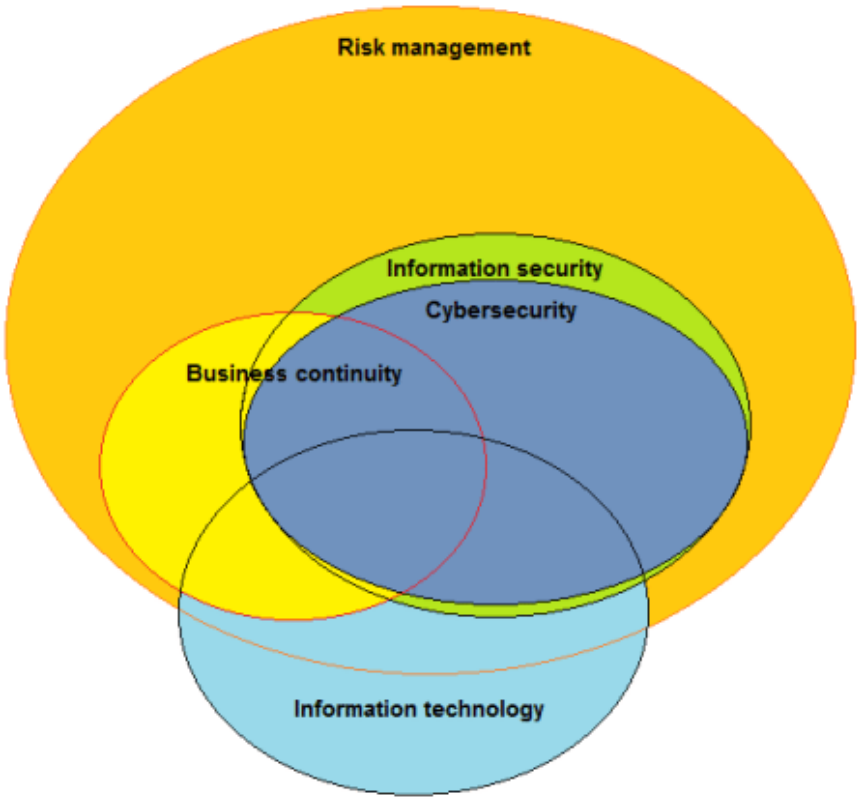

Figure 16. Risk management's relations. [60.]

5.3 Identifying risks and opportunities while creating ISMS

In the beginning of ISMS planning process, the key is to realize organizational needs for information security. Needs come more clear when risk levels, opportunities and treating options are recognized. One of the most necessary fact is that companies must be able to define realistic scope for ISMS, before implementing process. With the scope it is easier to understand if company can manage and maintain ISMS in the future. Costs are usually more than originally planned, so important is that company's management is all the time aware phases and features of the building process.

Usually one of the first things is to address or hire information security specialist. Specialist or specialists who are in charge of the different parts and phases of the whole operation. Sometimes knowledge and operating actions are bought from external experts or consultants. This is a good opportunity to grow knowledge of cybersecurity between the personnel. Following experts and sharing information inside the company is efficient way to learn. When personnel is educated regularly, at some point continuous learning becomes a process itself and is valuable asset for the company.

Opportunities and risks occur usually in the same things. When there is a chance to grow business, it is an opportunity but brings several risks. Risks depend on different factors with each company and may be any event that have effects on information security. Risk management implementation is slow but major part of the ISMS. When ISMS is on its final stage, risks will be addressed easier and several solutions options for incidents are ready. Functional ISMS is a great opportunity to improve everything inside the company, defective ISMS instead turns risks easier to incidents or even creates risks.

ISO 27001 based ISMS is possible to implement in many ways and security controls can be also taken outside of ISO/IEC 27001 Annex A and ISO/IEC 27005. In this chapter, risk management implementation is explained as ISO Expert Dejan Kosutic's explains it in a book *ISO 27001 Risk Management in Plain English* (Dejan Kosutic 2016). This research viewpoint was chosen because it is simple but comprehensive approach for SMEs to get familiar with ISO/IEC 27001 risk management implementation. Specially Kosutic's concept of *Five steps in the risk management process* is the central idea in this chapter. [28.]

Figure 17. Five steps in the risk management process. [28.]

5.3.1 Risk assessment methodology

Creating a methodology for SMEs risk management is the first step of the five step process. Particularly important is that all the steps are covered and in right order. In the beginning funds, scope, depth and available time are defined. Even before the first step, there need to be understanding that every company is unique. As well as that when project will be in the end, results must be manageable. On the other words, company needs to define risk level before implementing steps. At least actions below are recommended to define in the first step of risk management process:

- Identifying risks - Methods how to identify risks in forms of threats, vulnerabilities, nature related, personnel roles, human errors etc.
- Owners of the risks - There need to be authorized persons, who are responsible of the risk treatment through lifecycle of each risk.
- Consequences and probabilities – Scales/criteria need to be assessed for both of them, for example low-medium-high, 1-10 etc.
- Risk calculation - How to calculate risk values from combination of consequences and probabilities.
- Risk criteria - Value criteria for the risks that need to be treated and making decision with each risk if it will be treated.
- At least annual review and reviews when large changes have been performed.
- Mandatory and comprehensive documentation of risks, assets, changes and acts that have been done. [28.]

Management and responsible persons need to be careful from the beginning. Risks must first be recognized, only then it is possible to choose right security controls. Methodology should not be too large or complicated comparing to resources. In some cases, regulations and laws define considerably what kind of methodology must be chosen. Most important thing is that once rules are created, they must be followed correctly by entire

company. Performing ISMS policy differently between the people or departments causes confusion and creates more risks. Large enterprises may already have enterprise level risk management in use. When information security risk management is wanted to develop to deeper level, it must be compliant with existing ERM. [28.]

5.3.2 Risk assessment implementation

Once a risk assessment methodology has been created, next step is a risk assessment implementation. In this phase, company prepares to face potential problems. Documentation of all assets and possible targets of the risks and threats must be done carefully. After documentation, everything that could cause harm for information related to CIA model, should be able to point out in advance. Also likelihoods, possible outcomes and risk levels for each harm in risks, must be pointed out in risk evaluation and risk analysis. [28.]

Possible difficulties on this step, often require consultancy from external experts, experienced security managers or CISO. This is depending on the size, resources and construction of the company. Even if the methodology and policies are ready, most of the personnel do not internalize importance of them immediately. This why on early stage, companies must organize interviews for those who possess responsibilities and visions of company's infrastructure, roles, subcontractors, hardware, software, services, servers etc. In interviews, consultant, security manager or CISO explains importance and purposes of the risk management. [28.]

After preparing, documentation of the risks of company or every department should exist. The decision what risk level on each part of the company will be, is usually done by responsible of that certain part. Responsible often knows own department deeper than management or CISO. Still management need to be aware risk levels of each department. In smaller SMEs, responsibility is with the management and often external help is needed. With bigger companies, risk level is sometimes chosen in cooperation of executives, depending on organizational matters. Once risk levels are decided, workshops and trainings should be organized for management and personnel about the processes, tools, and policies. This activity is continuous as technics evolve and cyber threat hunting becomes active on daily bases. Process for reporting is highly important to establish, also documentation is mandatory and need to be performed even with the smallest actions and changes. [28.]

Asset	Threat	Vulnerability	Risk owner	Conse-quence	Likeli-hood	Risk
Server	Electricity outage	No UPS	Head of IT	4	2	6
	Fire	No fire extinguisher	Health & safety coordinator	5	3	8
Laptop	Access by unauthorized persons	Inadequate password	User of the laptop	4	4	8
	Loss of data	Backup is not made regularly	User of the laptop	4	3	7
System administrator	Leaving the company	No replacement	Head of HR	5	3	8

Figure 18. Example of risk assessment table. [28.]

5.3.3 Risk treatment implementation

Risk mitigation should be easy step comparing to risk methodology and risk assessment, if those two have been implemented in the right way. Risk level can be lowered, for example if probability of incidents or effect on assets are reduced. There are lots of risks that need to be treated and general guidelines may not offer enough specific help. That is why recognized risks must be all checked through and risk criteria need to be defined in advance, based on recognized risks. After the incidents, comprehensive walk-throughs are also important to perform for learning purposes. [28.]

For the risks that need to be noticed, there are few risk treatment options to use for closer examination. Decreasing the risks with planned activities is the best case scenario. Another option in some cases is to use *decrease, avoid* and *share* activities simultaneously. *Retaining* the risk is the option that should not be used, unless it is absolutely must. Risk treatment options are:

- Decrease - Decreasing the risks using suitable security controls as implementation process normally does.
- Avoid - Avoiding the risks by banning, limiting or stopping actions which are causing possibly too high risks.

- Share - Sharing the risks with external party, such as cooperation with another company and taking assurances from insurance company.
- Retain - Retaining the risks and not performing mitigating actions in advance. [28.]

Management need to be aware about the budget all the time. When implementing treatment process, there always should be some extra funds. Surprising things often occur when not expected, also changes require money. It is also not extraordinary that some security controls extend deeper when they are under closer look. With ISMS implementation process, the attempt is to decrease the risks with chosen security controls. There are totally 114 controls in ISO 27001 Annex A. Specially three of them are always current and important according Kosutics. These three controls are the most meaningful in continuous development covering basically everything:

- Definition of new rules - Strict documentation through all processes, policies, instructions and guidelines.
- Implementation of new technology - Fitting them to existing infrastructure, noticing also backup systems, duplication systems, disaster recovery locations etc.
- Structure changes of company - New job roles and functions, changes with responsibilities etc. [28.]

Some risks and incidents are complex and reach multiple different interfaces, areas, regulations and departments. These events need brainstorming with management, specialists, legal specialists and CISO. Without meetings, solutions may lack some details or treatment will become unexpecting expensive. New technology and external services offer often possibilities but spend unnecessary funds as well. Solution options may found sometimes from own resources. This is recommended to investigate first, as it would be cost-effective, may develop creativity and increase skills of personnel. Documentation of risk treatment can be done on similar way than in risk assessment and is mandatory. [28.]

Asset	Threat	Vulnerability	Treatment option	Means of implementation
Server	Fire	No fire extinguisher	1) Decrease risk + 2) Share risk	Purchase fire extinguisher + buy insurance policy against fire
Laptop	Access by unauthorized persons	Inadequate password	1) Decrease risk	Write Password Policy
System administrator	Leaving the company	No replacement	1) Decrease risk	Hire second system administrator who will learn everything the first one does

Figure 19. Example of risk treatment table. [28.]

5.3.4 Statement of Applicability

Statement of Applicability (SoA) as the central document of ISMS, defines implementation of information security's fundamentals in companies. SoA combines risk assessment, risk treatment and implementation processes together. Risk treatment plays the biggest role in the mix of them, affecting together with legislation, regulations, contracts, customers and almost every part. SoA functions as the key factor when choosing suitable security controls from ISO/IEC 27001 Annex A or in some cases outside of it.

Statement of Applicability is said to be the core of the company's ISMS, it is a document that includes everything. SoA guides certification auditor through the audition process checking listed security controls one by one. In his book Kosutic's also presents details, which are useful to adopt when writing the SoA from ISO/IEC 27001 point of view. Document indicates when and what really have been done to company's information security, and therefore simplifies auditing process for auditor. Aspects that are good to remember on definition phase to help companies to manage SoA in a systematic way are:

- Security objectives are recommended to define for each security control
- Brainstorm how each security control should be implemented
- Description how each security control has been implemented
- Comprehensive documentation is mandatory. [28.].

ID	Control name	Applica-bility	Justification	Control objectives	Implementation method	Status
A.6.2.1	Mobile device policy	Yes	Risks #34, 45, and 66	Decrease the number of security incidents related to mobile devices by 25% during the following year	Bring Your Own Device (BYOD) Policy	Fully implemented
A.6.2.2	Teleworking	No	Employees are working only from the offices	-	-	-

Figure 20. Example of Statement of Applicability. [28.]

5.3.5 Risk Treatment plan

The last step in five step process is creating the treatment plan, which basically means that already planned theory of the risk treatment will be converted to active. Chosen security controls, responsibilities and processes around them need to be moved from planning phase to doing phase. In doing phase, specific policies are written, technical controls are implemented and processes are fulfilled from all angles. SoA's importance emphasizes in this step, as it functions as a help, which security controls are implemented. This is one of the many reasons, why creating comprehensive SoA from the beginning is important for building ISMS successfully. Risk owners approvals and accepted budgets play major role when final plan is getting complete. The risk treatment plan is mandatory document and need to consist minimum following objects when implementing ISO/IEC 27001 based ISMS:

- All security controls that are under implementation processes
- How security controls are implemented
- References to the risks that started implementation of each control
- Responsible persons of each security control
- Deadlines of each implemented security control
- Personnel, external services and financial resources
- Results of each implemented security control
- Timing for reviews
- Risk treatments plan's status and results must be checked at every review. [28.]

Controls to be implemented	Reference to risks	Responsible person	Deadline	Resources	Results
Document a Back-up Policy	Risk no. 16 – Unavailability of electronic information because of accidental loss of the information	Chief Information Security Officer	March 2016	1 man/day	Implemented
Implement the Back-up Policy	Risk no. 16 – Unavailability of electronic information because of accidental loss of the information	System administrator	June 2016	3 man/days; budget for the technical controls	In the process of implementation
Implement a smart card physical entry control	Risk no. 32 – Laptops could be stolen by external people	Technical operations manager	April 2016	3 man/days; budget for the technical controls and the smart cards for all employees	In process of implementation; deadline passed

Figure 21. Example of risk treatment plan. [28.]

5.3.6 Regular reviews

ISO/IEC 27001 standard states that schedule for regular reviews must be planned in advance. New risks are found constantly in complex environments and often with the changes. Technology evolves fast and for example adopting new device brand, cloud services or facing vulnerabilities may require quick actions from the change management. When company's management reviews risk assessment results regularly, is reaction time for new risks lower. Risk assessments may seem to be difficult in the beginning, but personnel usually learn to understand how continuous improvements serve everybody. In the beginning CISO and management play major role with the support for personnel and departments. Depends on the SMEs size, area, environment and risk level, review times can vary from 3 to 12 months. Comprehensive documentation in every step of five step process and planned timing of reviews complete ability to perform reviews regularly. Well performed documentation also helps in situations that demand extra reviews. [28.]

6 ISO/IEC 27001 and certification process

6.1 Certification as an asset

Certification to ISO/IEC 27001 information security standard is respected and beneficial advantage, but not obligatory accomplishment for SME's ISMS. Depends on the situation, there are SMEs, which choose to go through the whole process to achieve certification. Certification shows company's commitment to take the business seriously and keep the customer information as secure as possible. Certification process has several demanding steps, it may take some time and funds, and still there is no guarantee of receiving the certification. Complexity of the process eliminates companies that do not take the certification seriously. This chapter introduces briefly, what main steps need to be taken account to go through the certification process successfully.

6.2 Preparing for certification

Everything starts with the decision. Cybersecurity responsibilities and management of the company must be behind the decision and most of all, must understand what ISO/IEC 27001:2013 certification means and requires. First thing is to get familiar with ISO/IEC 27001 standard for knowing what it offers. This can be done just by studying the standard, taking training courses or purchasing consultancy. Once standard's features are familiar, meetings with ISMS professionals are recommended to arrange. If there are not experienced people in the company, external consultant is the best option. In these appointments, goal is to go through what company needs and how it can be achieved. When prepare phase is done, there should be an idea and commitment from management, what kind of ISMS will be. Persons who are charge of implementation, must be appointed at early stages. [61.]

6.3 Defining the scope, timeframe and resources

Next phase is to define the scope and necessary resources for the certification project. This includes the plan that specifies if ISMS concentrates on certification of certain part or the whole company. Objectives, estimation of the costs and timetable are set, as well as appointments of internal and external resources. Already existing technics, new technics, processes, policies, regulations, stakeholders, subcontractors, employees, laws

etc. must be taken account in a definition phase. Persons in charge have great responsibility to keep the project's workers and milestones in time, and mentor the entire life cycle of the implementation. Timeframe must be planned in advance, also for maintains and reviews. [61.]

6.4 Risk assessment, risk treatment and Statement of Applicability

Risk management can be named as the core function when improving cybersecurity and creating ISMS. Dejan Kostutic's *Five steps in the risk management process* in Chapter 5 of this Master's Thesis introduced how SMEs can simplify the risk management. Assessing risks, creating the risk treatment and the risk implementing plans are strict and slow processes. When all this has been done and SoA is written to its latest version, everything becomes easier and manageable. SoA as already stated in Chapter 5, is the central document of the whole ISMS and guides certification auditor to check implemented security controls. Auditors have faster and easier job with comprehensive SoA to verify if implemented security controls are compliant with ISO/IEC 27001:2013 standard's requirements. [61.]

6.5 Personnel's introduction and training

Going through certification process and work in a company with ISO/IEC 27001 certificate may at first confuse personnel. Specially if there are lack of any communication from management what is going on at different stages. The best option is to inform personnel carefully already since the decision about going to ISO/IEC 27001 certification process is done. Introduction should consist what ISO/IEC 27001 standard is about, what will change, what benefits it brings for the company, staff and clients. Implementation may and normally is changing roles and ways of work during and after certification process. Companies are recommended to arrange staff awareness educations about the cybersecurity regularly and keep the personnel informed on every phase of certification process. Training and staff awareness events should be repetitive procedures, also after successful implementation. [62.]

6.6 Comprehensive documentation

Risk management itself requires extensive documentation and when planning to go to certification process, documentation needs to be even more strict. All security controls under implementation, with exact milestones need to be documented with policies, standards and procedures. Everything even slightly related to ISMS must be documented for company's own benefit and for the auditor. ISO/IEC 27001 experts have created documentation templates and toolkits, which are helping companies to prepare for certification. Following documentation is needed for certification auditors to check that they are documented and compliant with the standard:

"

- ISMS scope (as per clause 4.3)
- Information security policy (clause 5.2)
- Information risk assessment process (clause 6.1.2)
- Information risk treatment process (clause 6.1.3)
- Information security objectives (clause 6.2)
- Evidence of the competence of the people working in information security (clause 7.2)
- Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)
- Operational planning and control documents (clause 8.1)
- The results of the [information] risk assessments (clause 8.2)
- The decisions regarding [information] risk treatment (clause 8.3)
- Evidence of the monitoring and measurement of information security (clause 9.1)
- The ISMS internal audit program and the results of audits conducted (clause 9.2)
- Evidence of top management reviews of the ISMS (clause 9.3)
- Evidence of nonconformities identified and corrective actions arising (clause 10.1)
- Various others: Annex A mentions but does not fully specify further documentation including the rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, information security incident response procedures, relevant laws, regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures. However, despite Annex A being normative, organizations are not formally required to adopt and comply with Annex A: they can use other structures and approaches to treat their information risks." [47.]

6.7 Execution of the plan

ISO/IEC 27001 standard based ISMS targets improving functionality on every aspect of information security. Improvements are done by security policies that allow monitoring, measuring, analysing and reviewing ISMS on daily bases. Improving aims to expose risks and make security controls more effective by every found risk. In this phase pre assessment, checklists and communication with the personnel is showing if company is

going to right direction. Findings about the problems are important to correct and adjust to become ISO/IEC 27001 compliant, before actual certification audit is taking the place. [62.]

6.8 Internal audit

Internal audit is an important requirement and great learning possibility on the way to certification. With internal audition, implementation stage of ISMS can be defined accurately. Audit forms, reports and checklists must be ready for auditors to complete them with the notes, which improvements are required. An auditor can be an internal or external, as long as experienced audit is going to take place. At some point, companies may decide that own personnel should learn how to lead internal audits. There are many options with the trainings, courses and online courses to gain knowledge. If company possess ability for internal audits, it is huge advantage when preparing for certification audit. In this phase, is also useful to choose audit organization for registration. Auditor company must be independent and need to have authorised accreditation permission from authorities. [62.]

6.9 Certification

Everything what have been done in previous steps is targeting to pass ISO/IEC 27001:2013 information security standard certification process. If all is done by the book and internal audit is performed successfully by experienced auditor, the chance for passing official audit is high. Certification process is divided in two parts. In *Stage 1*, all documentation will be checked carefully if it is compliance with ISO/IEC 27001 requirements. Auditor indicates if there are any lacks of documentation or need for other improvements. When documentation corresponds with ISO/IEC 27001 standard, follows *Stage 2* audit. That is called *certification audit*, when Stage 1 audit is called *documentation review*. In Stage 2 audit, all implemented security controls are checked to be compliant with company's documentation and ISO/IEC 27001 standard by the auditor. [63.]

ISMS must be equivalent with what company's documentation and ISO/IEC 27001 standard are stating. Main focus is on records and implemented security controls, but also employees are sometimes interviewed. Cheating is difficult, because the permission to perform accreditation is granted only by the authorities. This makes auditors high level

specialists and qualified to notice even the smallest deflections. After Stage 2 audit, it is possible to receive certification without any corrections in company's ISMS. Sometimes found corrections must be revised. Normally the auditor allows 90 days for companies to introduce the proofs of solution actions. Depends on the size of the company and scope of the certification target, it takes 6 - 12 months for SMEs to receive certification, including preparation time. Once certification is issued, continual maintaining and improving must be carried on. Certification is valid for three years and is possible to get suspended, if major non-conformities are found under surveillance procedures. [63.]

CERTIFICATE

Sertifikaatti
Nro 1929-11

kiwa

Inspecta Sertifiointi Oy on myöntänyt tämän sertifikaatin, joka varmentaa, että organisaation

Elisa Oyj
Yritysasiakkaiden Kapasiteettipalvelut, Mobiilivarmenne- ja Mobiilitunnistuspalvelu, Dialogi-palvelu ja Elisan Turvallisuusvalvomo
Helsinki

tietoturvallisuusjärjestelmä täyttää seuraavan standardin vaatimukset

ISO/IEC 27001:2013

Sertifiointiin sisältyvä toiminta

Yritysasiakkaiden Kapasiteettipalvelut, Mobiilivarmenne- , Mobiilitunnistus- ja Dialogi-palvelun kehitys-, tuotanto- ja asiakaspalveluprosessit. Elisan turvallisuusvalvonnan toiminnot. Toimisto Helsingissä ja konesalitilat Espoossa, Helsingissä ja Raisiossa. Soveltuvuuslausunnon versio 2.3 (27.8.2018).

Sertifikaatti on myönnetty 2018-10-11
(alkuperäinen myönnetty 2000-04-18).
Sertifikaatti on voimassa 2020-02-15 asti.

Sertifikaatti on voimassa edellyttäen, että organisaation tietoturvallisuusjärjestelmä täyttää jatkuvasti edellä mainitun standardin ja yleisen ohjeen ABC 200 vaatimukset.
Sertifikaatin voimassaolon voi tarkistaa osoitteesta www.inspecta.fi

Inspecta Sertifiointi Oy
P.O. Box 1000,
Sömäistenkatu 2
FI-00581 Helsinki,
Finland
Tel. +358 10 521 600

IQNet MEMBER

kiwa certified ISO/IEC 27001 Inspecta Sertifiointi Oy

FINAS Finnish Accreditation Service S002 (EN ISO/IEC 17021-1)

Figure 22. Elisa's ISO 27001:2013 certificate. [64.]

7 Conclusions

This Master's Thesis has been surprisingly interesting and specially educational for myself. One of the goals were to learn more about information security standards and how they may help improving cybersecurity. This goal became profoundly fulfilled, even in the beginning the research was challenging. When I started the study, I was weighing if the topic is too distant or difficult. At the time, I did not know much about information security standards at all. When I now compare my knowledge towards ISO 27K family and other information security standards, I could teach quite a lot for myself in the beginning. Another goal I hope will actualize is that some SMEs may find this research useful. I hope the thesis will point them to find out more about enhancing cybersecurity through ISO/IEC 27001 information security standard. Some hopefully even end up to get interested about ISO 27001 certification.

I must admit that in the start, proceeding project was slower than I thought it would be. First couple of months passed by just reading about information security standards generally. Day by day I got more familiar with the topic and the wholeness what ISO/IEC 27001 really is, started to open. It was also a bit unrealistic to internalize, how the standard could help so much different size and kind of SMEs with information security. And still I had known it only by the name. At this phase, the Master's Thesis turned to be interesting. It was fascinating to notice that while reading about the ISO/IEC 27001 standard, use and purposes of other information security standards and best practices, also became familiar through the research material.

According to ISO survey in 2017, certification for ISO/IEC 27001 standard has been growing annually in the USA approximately 91% and worldwide 20%. [61.] This increase undoubtedly indicates that companies have been waking to growing cybersecurity era. Companies also seem to understand, how they can impact on level of the information security by themselves. This particular ISO survey measured certification numbers, not ISO/IEC 27001 standard users without certification process. Still conclusion, how the standard is used rapidly more and more without certification process, can be easily drawn. Certification process takes time, resources and funds. So only the most organized SMEs choose that path. Regardless of that, every SME wanting to enhance cybersecurity, can choose to use the standard.

Investigated material during the research showed undoubtedly that there are multiple levels, how companies may use and benefit from ISO/IEC 27001 standard. The world is full of SMEs, each of them have individual information security needs. Situations inside the organized companies are changing over the time. Companies evolve, expand and grow. To be successful in unstable environments and circumstances, demands it careful recognition of every aspect affecting on business. This is where information security standards have major role ensuring classified information. Some of the companies may develop from small SME to large SME or even to large-scale corporation. I learnt that it is rarely too late to invest on cybersecurity improvements, and there will always be the next level to achieve.

Depends on the size and wealth of SMEs, there are needs for very different kind of ISMS implementation. Smaller companies may not need sophisticated ISMS if ISMS at all, but can still benefit from information security standards when facing cybersecurity threats. These SMEs may purchase ISO/IEC 27001 standard guideline as an intention to get familiar how to improve and practice self-study. Even more simple options are available for SMEs that want to cover just basic IT actions. Some companies instead need extremely complex ISMS and larger SMEs may have own departments working only for cybersecurity. Increased demands for cybersecurity have created whole new business around IT security. Markets offer lots of cybersecurity products in form of information security standards, NG firewalls, IDS, IPS, tools, software, systems, services, surveillance etc. Companies can supply these products and build own protection or purchase consultancy, which is now days popular procedure. Consultation companies are offering specialist level help to educate personnel and tailor ISMS for any organizational needs.

Top goal for SMEs with comprehensive ISMS is to achieve ISO/IEC 27001:2013 certification. This research showed how requiring passing certification is and succeeds only with very careful preparing. Even company would already have proper ISMS, they still may choose external consultation to coach them through the actual certification process. Popular is also to put personnel into courses and try to achieve deeper cybersecurity knowledge for the company. With organized management, gained information can be used to lead internal audits and sharp the skills for the future's certification processes.

When studying particularly risk management, I noticed that there are quite many similarities between different information security standards, just like there are between implementation processes. This observation was easily made regardless SMEs size, area or

industry. Once the company has implemented risk management against ISO/IEC 27001 standard, can it also be start for more comprehensive risk management. Specially the wealthier SMEs could have afford and resources to use simultaneously several ISO standards such as ISO 27001, ISO 27005 and ISO 31000. This combination allows expanding of risk management, from already implemented ISO/IEC 27001 to Enterprise Risk Management (ERM) level. Using created ISO/IEC 27001 implementation and procedures as a base for ERM. Even without ERM, several ISO standards used at the same time is globally strong security statement and asset for the company. Reputation creates trust and when customer is purchasing information security related services, SMEs with ISO/IEC 27001 certification may be the choice, if other option is a company without the certificate. Certifiable standards can be used as a negotiation advantage in the business world.

Chapter 2 of the thesis introduced some major threats in the world of cybersecurity. Purpose of that section is to state why systematic approach to protect information within SMEs is essential. While investigating particular incident, threat or vulnerability, I realized that in the big picture other incidents, threats and vulnerabilities are all connected. Just like the information security standards are connected to each other. More I did researching, more these connections appeared. Regardless of that research mainly concentrated on how ISO/IEC 27001 standard can improve cybersecurity of SMEs, I gained more information about all areas of cybersecurity than I ever imagined. Cybersecurity threats and relations to information security standards and risk management are more obvious in my eyes now. In the end of research, my personal knowledge towards cybersecurity had improved enough to understand, how all the matters under cybersecurity somehow affect among each other. I have a strong belief that also SMEs without knowledge of information security or standards, may gain useful information and inspiration for better cybersecurity from this Master's Thesis.

After completing this research, it is crystal clear that ISO/IEC 27001 information security standard is useful for every SME. Even for the smallest ones and if it used only fractionally to improve some of the risk management procedures. Every improvement makes cybersecurity little bit stronger and basically there are no limits, how deep the use of standard can be. Larger companies that want to be as secure as possible, have management, security managers, CIO, CISO, CDO etc. doing co-operation when initializing new technology or developing ISMS. Implementing security controls and building ISMS first time is usually slow and challenging road. Though once ISMS is in use and security

policies have become familiar, managing information evolves more effortless. Risks are found easier, suitable security controls for them are pointed routinely and recovery time from incidents have become faster. When SME adopts itself to ISO/IEC 27001 user successfully, personnel get to use to new procedures and policies around ISMS steadily. After transitional phase under good management, ISMS may become core part of organisational culture.

At first there were some concerns could I find reliable material for this Master's Thesis. This doubt turned out to be totally irrelevant. Internet is full of free or low fare material about information security standards and cybersecurity. Material such as books, articles, researches and blogs were found easily. Additionally companies websites offer wide selection of online courses and trainings. I was also a bit worried, which sources are trustworthy. After studying some time, source criticism towards the topic developed automatically. Interesting point was to notice that there seemed to be more cybersecurity topic publications from last few years than from about ten years period before that. This is a strong indicator for more advanced cybersecurity awareness between the companies, personnel and people. At the same, it was satisfying to realise that it is not only the cybersecurity threats companies have started to understand. Obviously companies recognize that technics behind the attacks are evolving and how they need competence to respond on changing situation.

Before starting this research, I had a belief that cybersecurity playing field around the world is still quite open without clear rules and regulations. This belief became even stronger during the project. Top examples are military and intelligence agencies. Reconnaissance and also defensive type of cyberwarfare seem to be happening between nations continuously. Interesting is also how conversation about that is wide open on daily media. The world does not exactly know, what is allowed or prohibited to do. Clear sanctions are lacking as well. Even the rules for cybersecurity sector are still open, more regulations and laws are adjusted constantly. Information security standards are already sometimes a requirement and an asset in many area of industries and products.

In my opinion there could be more strict international regulations, ruleset and requirements for cybersecurity. At first regulations could be managed by areal body related to industry, government, EU Directive, etc. Later, when in advance defined areas already would have experience, it would be easier to develop more categories for global standards for different purposes and demands. This kind of operating model would make safer

and more stable products and environments for both, companies and customers. Good already existing example is the procedure what companies handling payment card information are using. They need to be PCI DSS compliant if they want to practice business. Another successful example is EU's the General Data Protection Regulation. In May 2018 launched GDPR shows how the world is already changing, what it comes to handling of digital information. Regulation provides comprehensive data privacy for citizens within the EU and the EEA areas. The GDPR made all the companies think and in many cases change their data privacy and data handling procedures. Similar unified functionalities that PCI DSS and GDPR have, could be brought to cybersecurity standardization. Transfer time for new procedures always take time, so new cybersecurity related standardizations could first start as recommendations or with piloting period. In time, there could be a large selection of cybersecurity standards. Selection could consist flexible but essential standards providing more protection for different situations.

Currently worldwide business and technics are both growing rapidly. Same time base of global society structure has been built on money and therefore specially financial information must remain trustful. There probably will be more effort and funds put on information security products from business world than ever before. This development would serve SMEs but also nations and citizens. As a result from matters I learnt during this Master's Thesis, I am confident that in the near future, there will be more comprehensive options for SMEs to enhance cybersecurity. Cyberattacks will be more sophisticated as well, but simultaneously people are developing with defending abilities. Specially growing generation will probably take information technology and skills totally for new level.

References

1 Computer security. 2017. Wikipedia.
Accessed December 2017.
<https://en.wikipedia.org/wiki/Computer_security>

2 The small and medium-sized enterprises. 2017.
Accessed December 2017.
<https://www.yrittajat.fi/en/about-federation-finnish-enterprises/small-and-medium-sized-enterprises-526261>

3 Cyber-attack Volume Doubled in First Half of 2017. 2017.
Accessed December 2017.
<https://www.infosecurity-magazine.com/news/cyberattack-volume-doubled-2017>

4 2016 Presidential Campaign Hacking Fast Facts. 2017.
Accessed December 2017.
<http://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

5 Cyber Attack Landscape of 2017, So Far. 2017.
Accessed December 2017.
<https://business.f-secure.com/report-cyber-attack-landscape-of-2017-so-far>

6 APT life cycle. 2017.
Accessed December 2017.
<https://en.wikipedia.org/wiki/Advanced_persistent_threat>

7 Obama Order Sped Up Wave of Cyberattacks Against Iran. 2012.
Accessed May 2018.
<https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>

8 Vulnerabilities. 2017. Wikipedia.
Accessed September 2017.
<https://en.wikipedia.org/wiki/Vulnerability_(computing)>

9 National Vulnerability Database. 2018.
Accessed March 2018.
<https://nvd.nist.gov>

10 2018 Security Threat Report.
Accessed October 2018.
<https://www.protiviti.com/sites/default/files/infographic-2018-security-threat-report-protiviti.pdf>

11 OWASP Top Ten Project. 2018.
Accessed January 2018.
<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>

12 OWASP Top 10 Application Security Risks – 2017. 2018.
Accessed January 2018.
<https://www.owasp.org/index.php/Top_10-2017_Top_10>

13 Must-Know Phishing Statistics 2017. 2017.
Accessed December 2017.
<https://blog.barkly.com/phishing-statistics-2017>

14 SANS Institute InfoSec Reading Room. 2017 Threat Landscape Survey.
Accessed January 2018.
<https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910>

15 The internet sees nearly 30 000 distinct dos attacks each day. 2017.
Accessed March 2018.
<https://www.securityweek.com/internet-sees-nearly-30000-distinct-dos-attacks-each-day-study>

16 Joon Ian Wong. 2016. Largest DDoS attack each year.
Accessed November 2017.
<https://www.theatlas.com/charts/rJ3Y0ynmg>

17 GitHub Survived the Biggest DDoS Attack Ever Recorded. 2018.
Accessed March 2018.
<https://www.wired.com/story/github-ddos-memcached>

18 DDOS ATTACKS. 2018.
Accessed March 2018.
<https://www.incapsula.com/ddos/ddos-attacks>

19 Managing Thumb Drive Security Risks. 2014.
Accessed February 2018.
<https://www.securitymagazine.com/articles/85768-managing-thumb-drive-security-risks>

20 Almost half of dropped USB sticks will get plugged in. 2016.
Accessed August 2018.
<https://nakedsecurity.sophos.com/2016/04/08/almost-half-of-dropped-usb-sticks-will-get-plugged-in/>

21 Rubber ducky you're the one! 2013.
Accessed February 2018.
<https://sramage.wordpress.com/2013/04/01/rubber-ducky-youre-the-one>

22 What is social engineering? How criminals take advantage of human behaviour. 2017.
Accessed March 2018.
<https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html>

23 What is ransomware? How it works and how to remove it. 2017.
Accessed April 2018.
<https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html>

24 10 of the Most Significant Ransomware Attacks of 2017. 2017.
Accessed April 2018.
<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/10-significant-ransomware-attacks-2017/>

25 Popular Tools for Brute-force Attacks. 2018.
Accessed March 2018.
<http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref>

26 What is the darknet? 2017.
Accessed September 2018.
<https://www.darkowl.com/what-is-the-darknet>

27 DDoS Attacks Are $10 per Hour on the Dark Web. 2018.
Accessed August 2018.
<https://www.bleepingcomputer.com/news/security/ddos-attacks-are-10-per-hour-on-the-dark-web/>

28 Dejan Kosutic. ISO 27001 Risk Management in Plain English. 2016.
Accessed multiple times September 2017 – December 2018.

29 Information security. 2018.
Accessed February 2018.
<https://en.wikipedia.org/wiki/Information_security>

30 Committee on National Security Systems: National information Assurance (IA) Glossary, CNSS Instruction No. 4009. 2010.
Accessed February 2018.
<https://en.wikipedia.org/wiki/Information_security#cite_note-22>

31 INFOBASICS-Basic Concept of Information Security. 2016.
Accessed February 2016.
<https://securereading.com/infobasics-basic-concept-information-security>

32 Information Security: A practical approach. 2008.
Accessed March 2018.
<https://dl.acm.org/citation.cfm?id=1571880>

33 Information Security Controls. 2018.
Accessed March 2018.
<https://www.omicsonline.org/open-access/information-security-controls-2168-9695.1000e118.php?aid=23716>

34 Information security is like an onion.
Accessed March 2018.
<http://www.housemarkinnovation.io/news/innovation-insight/thought-leadership/information-security-is-like-an-onion>

35 Network defence methodology. 2018.
Accessed March 2018.
<https://infogram.com/network-defense-methodology-1gvew2vd930d2nj>

36 Information classification according to ISO 27001. 2018.
Accessed March 2018.
<https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001>

37 How to use cryptography according to ISO 27001 control A.10. 2018.
Accessed March 2018.
<https://advisera.com/27001academy/blog/2015/12/14/how-to-use-the-cryptography-according-to-iso-27001-control-a-10/>

38 What is an Information Security Management System (ISMS) according to ISO 27001? 2016.
Accessed May 2018.
<https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/>

39 What is an ISMS and 9 reasons why you should implement one. 2017.
Accessed May 2018.
<https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one/>

40 ISO 27001 Information Security Management System. 2015.
Accessed May 2018.
<http://www.eccinternational.com/consulting/it-process-excellence/iso-27001-information-security-management-system>

41 GDPR Key Changes. 2018.
Accessed March 2018.
<https://www.eugdpr.org/the-regulation.html>

42 How ISO 27001 can help you comply with the GDPR. 2018.
Accessed March 2018.
<https://www.itgovernance.co.uk/gdpr-and-iso-27001>

43 About ISO. 2018.
Accessed February 2018.
<https://www.iso.org/about-us.html>

44 About the IEC. 2018.
Accessed February 2018.
<http://www.iec.ch/about/?ref=menu>

45 ISO 27K timeline. 2018.
Accessed May 2018.
<http://www.iso27001security.com/html/timeline.html>

46 Risk Management: Certified ISO 27005 Risk Manager. 2018.
Accessed September 2018.
<https://www.imfacademy.com/areasofexpertise/security_management/certified_risk_management.php>

47 Information technology - Security techniques - Information security management systems - Requirements. 2017. ISO/IEC 27001.

Accessed September 2017.
<http://www.iso27001security.com/html/27001.html>

48 Dejan Kosutic. 2017. Overview of ISO 27001:2013 Annex A
Accessed November 2017.
<https://advisera.com/27001academy/knowledgebase/overview-of-iso-270012013-annex-a/>

49 VAHTI-instructions. 2016.
Accessed February 2018.
<https://www.vahtiohje.fi/web/guest/home>

50 Information security auditing tool for authorities – Katakri 2015. 2016.
Accessed February 2018.
<http://formin.finland.fi/public/default.aspx?nodeid=49575&culture=en-US&contentlan=2>

51 PCI security. 2018.
Accessed May 2018.
<https://www.pcisecuritystandards.org/pci_security/>

52 PCI-DSS vs. ISO 27001 Part 1 – Similarities and Differences. 2018.
Accessed May 2018.
<https://advisera.com/27001academy/knowledgebase/pci-dss-and-iso-27001-general-description-and-structure/>

53 NIST Cybersecurity Framework. 2018.
Accessed May 2018.
<https://www.nist.gov/cyberframework>

54 What is COBIT? A framework for alignment and governance. 2017.
Accessed May 2018.
<https://www.cio.com/article/3243684/methodology-frameworks/what-is-cobit-a-framework-for-alignment-and-governance.html>

55 Standards, Compliance and Enforcement Bulletin Archive. 2018.
Accessed May 2018.
<https://www.nerc.com/pa/Stand/news/Pages/default.aspx>

56 What is ITIL? Your guide to the IT Infrastructure Library. 2017.
Accessed May 2018.
<https://www.cio.com/article/2439501/itil/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html>

57 ITIL: Key Concepts and Summary. 2018.
Accessed May 2018.
<https://www.simplilearn.com/itil-key-concepts-and-summary-article>

58 Has the PDCA Cycle been removed from the new ISO standards? 2014.
Accessed June 2018.
<https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/>

59 PCDA cycle.
Accessed June 2018.
<http://iso-17799.safemode.org/indexecce.html?page=PDCA_Cycle>

60 ISO 31000 and ISO 27001 – How are they related? 2014.
Accessed May 2018.
<https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/>

61 ISO 27001 registration/certification in 10 easy steps. 2018.
Accessed June 2018.
<https://www.itgovernanceusa.com/blog/iso-27001-registrationcertification-in-ten-easy-steps/>

62 10 Steps to ISO 27001 Certification. 2018.
Accessed June 2018.
<https://www.theagenci.com/iso27001/10-simple-steps-to-iso-27001-certification-html/>

63 Becoming ISO 27001 certified – How to prepare for certification audit. 2018
Accessed June 2018.
<https://advisera.com/27001academy/knowledgebase/becoming-iso-27001-certified-how-to-prepare-for-certification-audit>

64 Elisa's ISO certificate.2018.
Elisa.headquarters