LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Elektrilevi information asset mapping

Hartwig Hiiemäe

2016 Leppävaara

Laurea University of Applied Sciences
NIA13SN

Elektrilevi information asset mapping

Hartwig Hiiemäe
Degree Programme in Business
Information Technology
Bachelor's Thesis
May, 2016

Laurea University of Applied Sciences **Abstract**
NIA13SN
Degree Programme in Business Information Technology

Hiiemäe, Hartwig

Elektrilevi information asset mapping

Year 2016 Pages 32

This thesis project focuses on creating classification table and mapping information assets of the Elektrilevi. The project aim was to map all the information assets within the Elektrilevi. The research dives methods that were used to classify and assess the information assets.

The thesis project was commissioned by the upper management of the Elektrilevi, which is the provider and maintainer of the power grid within the Estonia. The project was conducted under CISO supervision.

This thesis delivers detailed study of knowledge base built up for the project. It covers what classifications were used to rate the information assets. The result of the project is a document containing all the information assets with ratings, within the Elektrilevi.

Information assets, Information lifecycle, Information classification, Analysis

Table of contents

Terms and abbreviations

SCADA	Supervisory Control and Data Acquisition
CIA triad	Confidentiality, integrity and availability guideline
CRUD model	create, read, update and delete model
OneNote	Microsoft OneNote, note taking software
IBM notes	Collaborative software, Personal information manager, Email
ILM	Information lifecycle management
ITAM	IT asset management
ELV	Elektrilevi
EE	Eesti Energia AS

1 Introduction

As electricity is essential for life, the need for ensuring its availability is crucial. Electricity powers hospitals, communication centres, water stations, gas stations which are vital for continuous life. There are numerous threats that power grids face: electromagnetic pulse, direct physical attacks, and cyber warfare. This thesis will focus on the last part of it, with the focus of securing information asset.

Information technology growth has been exponential within the past few decades. Development of information technology has given us: e-mail, e-business, the internet, business software and financial software etc. allowing different areas to achieve goals far faster and at a lower cost. However, modern solutions also bring new risks. In addition to protecting material values, the need for information protection and intellectual property protection has arisen. Information technology has become one of the fastest growing areas and area most involved with humans, thus it's quick and thought-out development is extremely important to each enterprise. Nowadays, it is unthinkable for organizations to operate without automated information processing, which entails the need of information lifecycle management.

With information growth, its lifecycle needs to be managed simultaneously. Managing the cycle is challenging to begin with, difficult to map information assets, scarcity of operational guidelines for the wider audience, since the subject is sensitive it is difficult to find conducted information lifecycle process. Thus the methods are indirect and finding a suitable method is hard. Formalized methods are at a nascent.

To begin managing information lifecycle a knowledge on information assets is needed. An information asset is a knowledge of information which is managed and grouped into single unit, thus it can be better understood and make use of. Information assets have lifecycles, content, value and risk which are managed (Identifying Information Assets and Business Requirements 2011). This thesis project covers information asset mapping within the company called Elektrilevi. The project consisted of two phases, the first phase consisted of building theory base and the second phase was conducting interviews to map information assets.

This thesis is divided into four main segments, the introduction which will present the company, the project background and reasons. Methodology, how this project was implemented and what were the research topics. Project start-up and Theoretical background focus on explaining how the project was approached and clarifying key theoretical concepts. Interviews and conclusion that discusses the process of mapping information assets and results of the process.

1.1 Company background

Elektrilevi is a subsidiary company of Eesti Energia and is the supplier of electricity to 92% of households and companies in Estonia, based on their website the claim that they manage and adjust about 61,000 kilometers of power cables and more than 22,000 substations. They have about 475,000 clients across Estonia. Electricity is supplied by alternative network operators in following areas: Lääne County, Viimsi, Narva and its surrounding areas. Following Figure 1: Elektrilevi network regions shows Elektrilevi operation regions in Estonia.

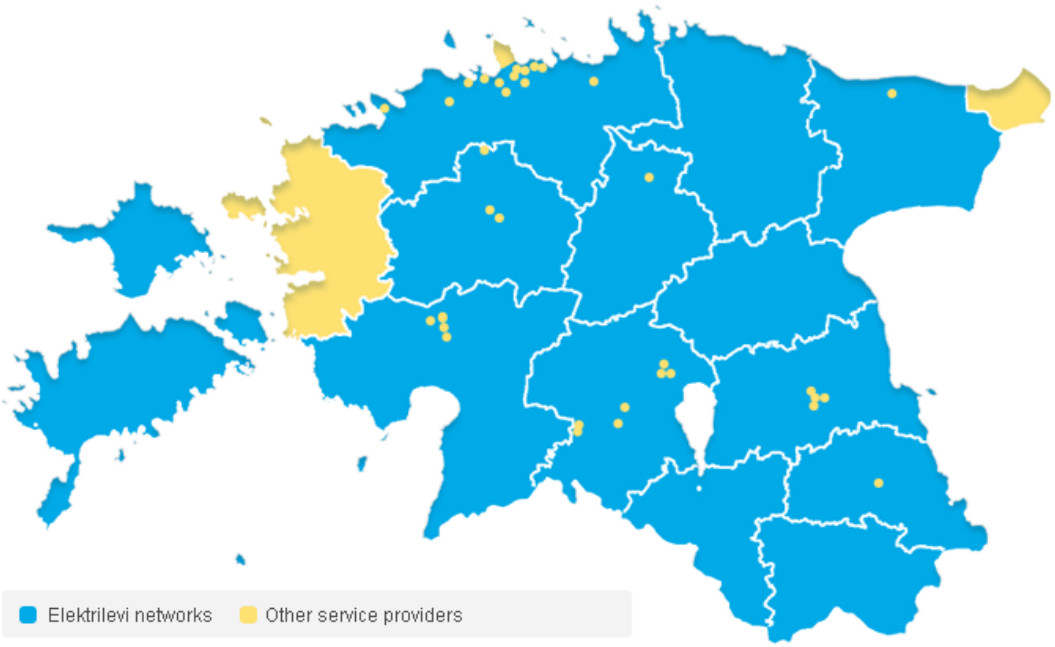

Figure 1: Elektrilevi network regions

I as a full-time employee of Elektrilevi approached my supervisors to conduct a project that would be beneficial to the company and would suit for bachelor thesis project, thus project "Information asset mapping" was started.

1.2 Project background

Elektrilevi is in a constant volatile state, structure's change, constant new information, processes change along with enterprise strategy. Need for sustainable information lifecycle is required. Elektrilevi has an information lifecycle management in use, however knowledge on information assets was outdated.

Management main interests were for risk analysis and business critical information components, concern for information assets that are not in accordance with Estonian and European law was also very actual. To conduct given researches, information assets needed to be mapped properly beforehand. Not only the name of the information asset was to be mapped,

but also who is the responsible person for it, which business processes it is used in, what are the user access rights to it, thus I was assigned as a project manager for information asset mapping.

1.3 Objectives

The purpose of this project is to map information assets along with mapping their business criticality, responsible owner and access rights, within the Elektrilevi. The project had multiple mini-objectives, and was divided into two main phases.

Two key objectives were formed for the project, the first objective is the first phase of the project and the second objective is the second phase of the project.

- Building theoretical knowledge for creating base document
- Conducting interviews to map assets

The outcome of this project aims to provide value to the company from information security perspective, a document containing information assets is the deliverable and it will be used in upcoming risk analysis project. As power grid is critical infrastructure for life and securing it from uprising threats from cyber worlds is a must.

1.4 Limitations

Estimating time for tasks is difficult and it becomes much more challenging when other people are involved. The project should be completed by the end of 2016, with the deliverable of mapped information assets in one document. A broad schedule was created, however in the first month, it was obvious that tasks will take longer than expected. Booking a meeting that suits the managers is doable, but there is always a possibility of delays or other complications to come.

Due to high confidentiality and business secrets, it was not allowed to publish or elaborate about any sensitive information revolving the project. It was allowed to write about project theoretical build up and bring few examples of information assets where the information has been changed.

2 Knowledge base

The project's first phase contained several research topics and in the second phase, qualitative method was used. It aims to explain how research topics were approached and how the decisions were made. There is limited and broad information online about information assets, thus the project leaned towards management's needs and interests. This project focused on critical infrastructure viewpoint, thus critical law requirements were also looked upon.

2.1 Threats for critical infrastructure

Securing critical infrastructure is a very challenging task. There are long discussed nightmare scenarios caused by cyber-attack against critical infrastructures, unfortunately those scenarios are more likely nowadays. It is now being approached as "the when, rather than if". (CYBER ATTACKS AGAINST CRITICAL INFRASTRUCTURE ARE NO LONGER JUST THEORIES 2016)

In 2015 we already saw cyber-attack on Ukraine's power grid, which left 700 000 people without electricity for a couple of hours. Which had CERT organizations around the world alerted.

This thesis project aimed to produce value to the overall security of the company. While during the interviews many recent cyber security threats, news and their impacts were discussed with managers.

2.1.1 Industrial control systems

Industrial control systems (ICS) are in use every day, even when civilians do not know of their existence or use. The automated control systems are beneficial to the enterprise, for its economic advantages and profitable efficiency. Smart home control and nuclear power plant monitoring are the modern and different uses of ICS. The use of ICS in smart homes similar to those used in industrial plants has risen. Modern energy control systems have begun extending to households and apartments. With the increase of such technologies, security of those devices has fallen. See Figure 2.

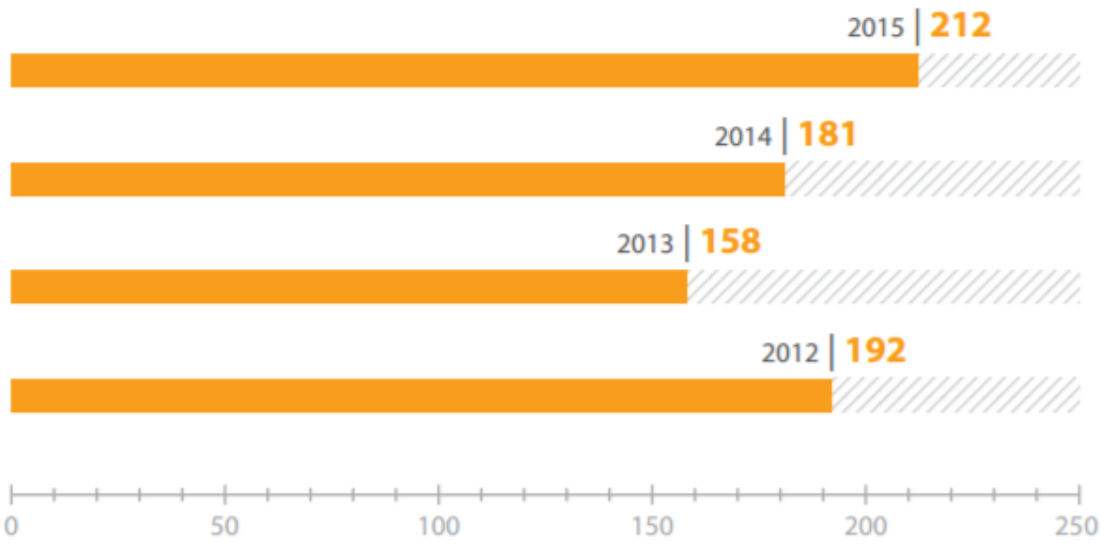

Figure 2: Threats found in ICS devices.

Vulnerabilities in various devices are also considerably high. See Figure 3 which shows most vulnerabilities found are in SCADA, HMI and PLC/RTU components, the research conducted during 2012 had about the same amount of vulnerabilities according to .pdf

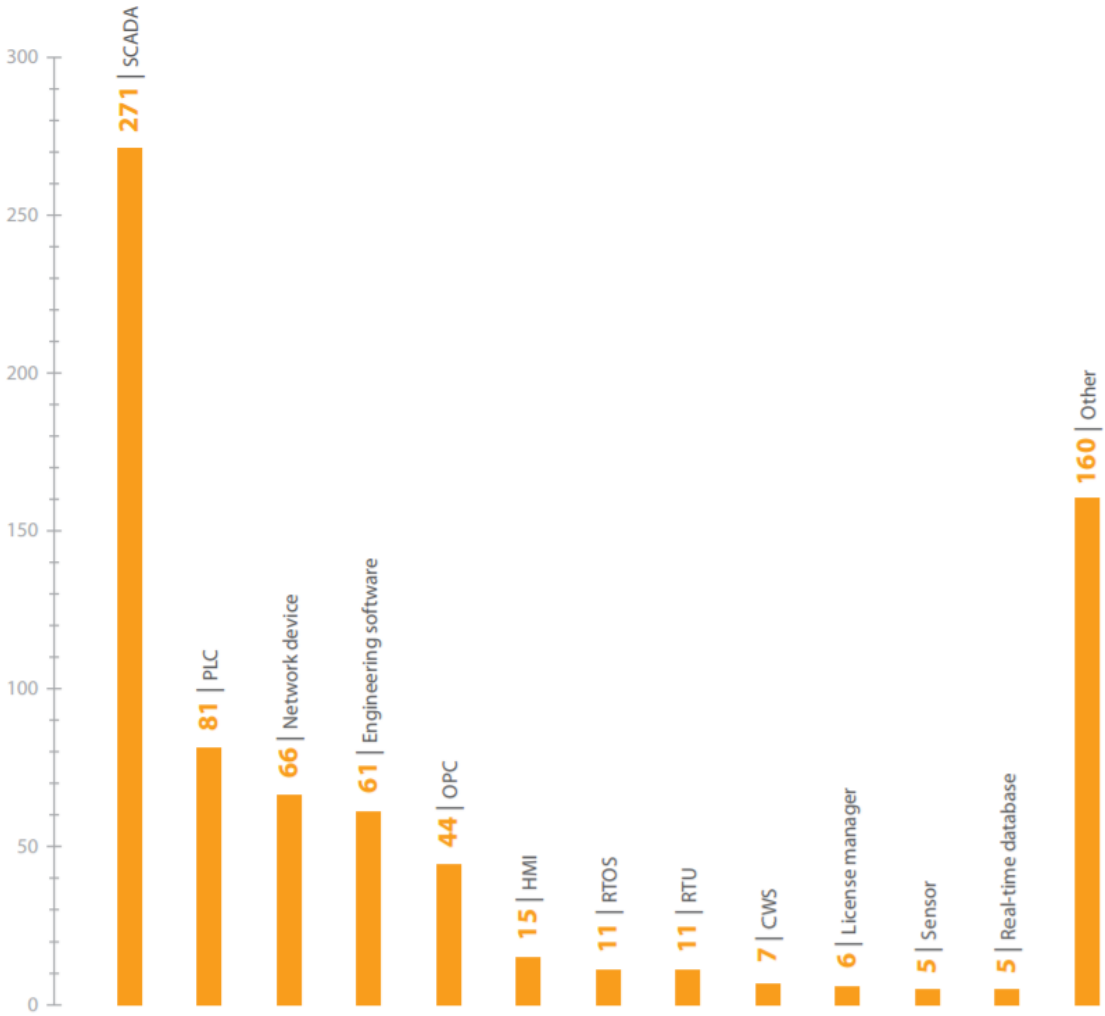

Figure 3: Vulnerabilities found in devices.

The trend of ICS components security is stagnated. The identified vulnerabilities are high-risk and they are not reducing from year to year. The bulk of vulnerabilities are from popular product vendors. This is only a single factor for security, within the enterprises. (Industrial Control Systems 2016 Report: Connected and Vulnerable 2016)

2.2 Laws and regulations

This part had several key research areas, first gathering knowledge on managing information lifecycles and information assets. The aim was to be able to group assets and know differences of them. However knowing only the information assets name is not enough for it to provide any value, thus upper management's guidance was followed and three main purposes were given for the project. They were following "What is the criticality of the information asset in business processes", "Who is the responsible person for managing it", "and how the access rights are regulated" all of them were approached with different research methods.

I also had to get familiar with three laws which were following. “The Emergency law” regulation 43, “Electricity Marketing Act” and “Personal Data Protection Act”. The reason for this was to be able to see information assets from a higher level and sought out potential cases where information assets might not in accordance with laws. See Figure 4

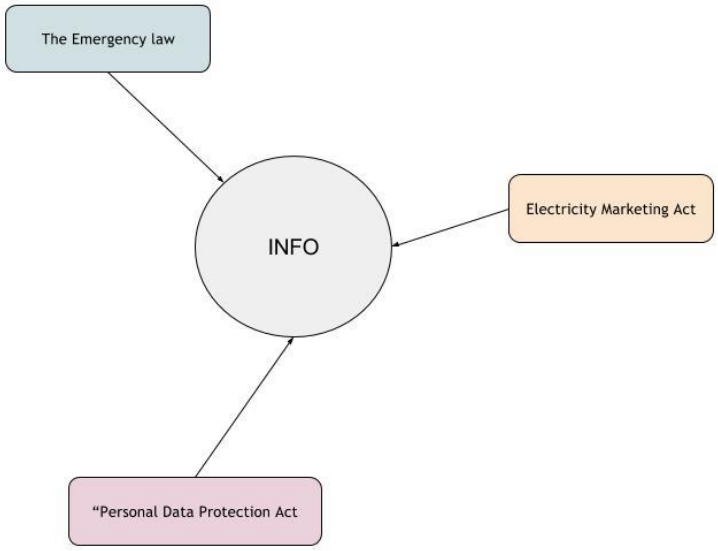

Figure 4: Three laws that regulate information use

2.3 Estonian laws

Elektrilevi is state-regulated company and they follow all laws that apply to them thoroughly. When it comes to information there are three major laws that need to be followed. “The Emergency law” regulation 43, “Electricity Marketing Act” and “Personal Data Protection Act”. They all contain paragraphs which affect information assets. To view the company broadly, there are two main divisions which contain most of the information assets, they are “Assets management” and “Customer management”. In Figure 11 there is shown how two laws fall into “Customer management” division responsibility and other into asset management.

2.3.1 The Emergency law

This law regulates crisis management, including emergency planning and solving emergency situation along with controlling vital service providers legal guarantee basis. In the law section § 40 paragraph 2 there is regulation *Vital service information systems and related information assets security measures*" act § 43. It is referenced in law "that companies that are involved with providing vital services need to have an information system risk analysis and system reliability assessment conducted" under, act § 37 paragraph 3, point 1. Act § 43 paragraph 4, point 3 highly recommends usage of EVS-ISO/IEC 27001:2006 standard, which helps to ensure information security.

To understand the effects and complexity of this law, an example situation will be explained. We have an information asset called SCADA (supervisory control and data acquisition) which allow dispatchers to control the power grid. It works on IP protocols, but what if the IP network crashes or is down due to service provider failure and at the same time an there is a short circuit somewhere, physical assets might be damaged, potential loss of life, loss of customer satisfaction due to the power outage. All that because dispatcher was not able to control the power grid since the SCADA which has that functionality was halted. From the government's point of view, Elektrilevi is the vital service provider who broke the law, yet it was caused by the third party. Thus it often depends on the political view when it comes to solving complex situations.

2.3.2 Electricity Marketing Act

Elektrilevi is a natural monopoly, it is simply not wise to build secondary power cables to clients, just to sell them electricity. Thus Elektrilevi is state regulated and has to be market neutral. Eesti Energia is power seller and Elektrilevi is a supplier of the electricity. Even though Elektrilevi belongs in same concern as Eesti Energia, we need to have separation of the data controlled, so that Eesti Energia would not gain any market advantages compared to others. This means that Elektrilevi needs to own network preservation and development of the necessary resources, including technical, physical, financial, and human resources. According to act §18 point 5 of the Electricity Marketing Act.

Information assets that preserve data that could lead to market advantage need to be controlled and user access rights should be monitored. This is a law that has a conflict of interests and different philosophical views.

2.3.3 Personal Data Protection Act

Elektrilevi collects and manages customer data which falls under “Personal Data Protection” law and in act §25 paragraph 2 point 1 reads-out that party that uses personal data must ensure that unauthorized persons are not allowed to access devices that contain personal data. Thus all information assets that contain any data about customers need to be well protected and kept confidential. The data protection Inspectorate do compliances on how the data is managed within the company, thus this law needs to be followed delicately.

European legislation has updated personal data protection act on 27. April 2016. It is an 80-page document and has very strict laws. For example article 83 point four reads out following: “*Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*” Official Journal of the European Union (2016, 82) this means that more strict measures are in need, for the consequences are immense.

Having a classification about user access and CIA triad is essential for protection personal data when it comes to information assets.

2.3.4 Criticality of the information asset in business processes

Each business owns a strategy and often business tasks are divided into processes, larger the company, the more processes there are. In Elektrilevi there are seven major processes, with eight supporting processes. To be able to conduct business processed an assets are required, they may be physical assets, service assets and information assets. This project focuses information assets which are involved with business processes. Processes can use many information assets while information assets can belong to many processes. If information were destroyed and lost, what would be the impact of it on a business process? What is the cost of reinstatement? What will be the media’s and public response? Could you classify assessment of the effects of weight? To get a rough estimate and answers, key personnel were identified.

According to CISO of the company information technology could be looked from this perspective, there are about seven different layers to it, see Figure 5: Information layers. There are shown that Processes block is managed by process managers, Data block is managed by Branch managers and IS block has Admin users.

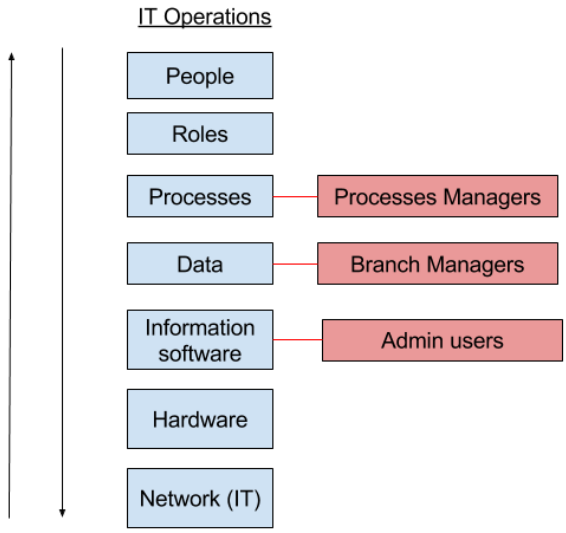

Figure 5: Information layers

Process managers have a broader view on information assets and are often responsible personnel for them. While Admin users have better insights on information assets and user access controls. There were two ways to approach it, from bottom-up or from top-down. It was decided to interview process managers first, to get an overview of information assets and later on interview Admin users to gather insights.
Key personnel mapping was done using an inner database which contains all of the workers within the company, they were mapped with their job titles and their divisions. The lead process manager was also able to provide a list of key personnel to have a meeting with.

2.3.5 Responsible person for information asset

Process managers were identified to be the key owners of information assets, however it was not that simple. Complications arose when it was reviled that in some cases third party, was for example, storing the information and if a problem occurred from their side then person responsible for information asset would not be able to take responsibility for it. Thus the conflict of interests was very actual.

2.3.6 User access rights regulation

To gather information about user access rights regulation we interviewed process managers and administrator users. Process managers were able to give insights of what should be while admin users told us what is.

Classification methods for this were researched from online. TLP and CRUD model were two considered use-cases for it, however due to being more specific CRUD model was chosen. It gave a more detailed view of user access rights.

2.4 Information lifecycle management

The first research topic was clarifying the philosophy behind information lifecycle management. To manage information through its lifecycle, from creation to disposal in a manner of controlled way a need for information lifecycle management (ILM) is needed.

ILM includes processes and policies to manage information along with hardware or software. Its core idea is that information at different points in their lifecycle have distinct values. Controlling user access and prediction various costs can be especially challenging as the data grows (Information Lifecycle Management Best Practices Guide 2007).

Effective ILM implementation requires understanding how information is built, ages over time, is modified, and whether if it can be deleted. See Figure 6.

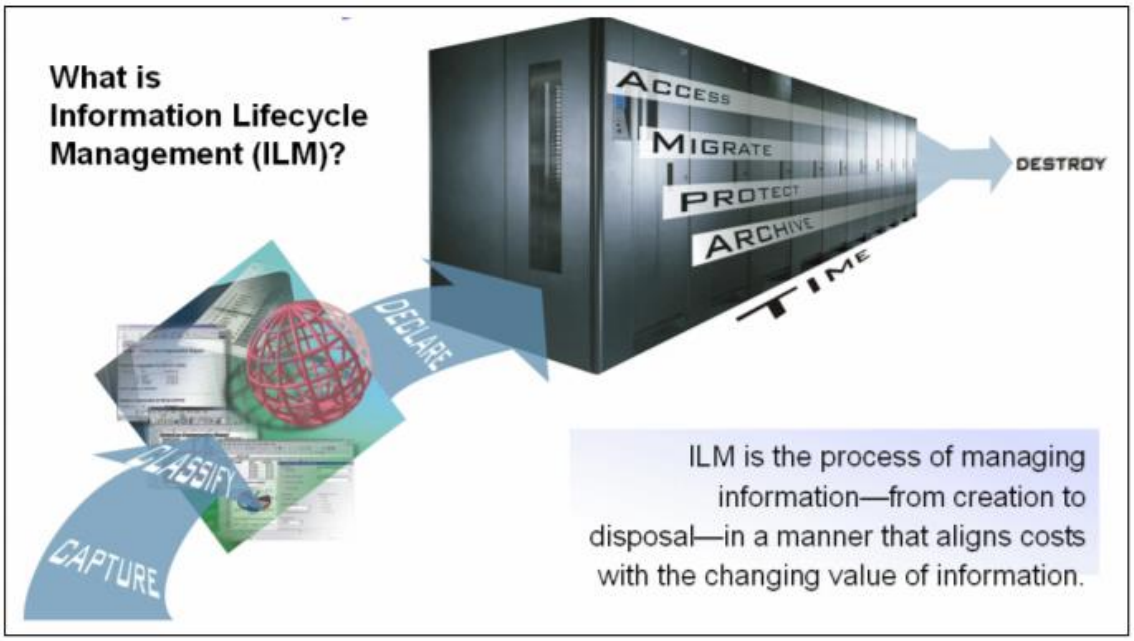

Figure 6: Information lifecycle management process

Starting ILM requires knowledge on information assets, to do that you need to map out and classify them.

2.4.1 Information assets

To manage ILM process you need to know what your information assets are, identifying them is a less glamorous aspect of it. To know what amount of time, effort or money you need to secure your assets along with managing them you need to know their locations and value. (Identifying and classifying assets 2002)

Asset classification and control have major following steps:

- Identification of the assets
- Accountability of the assets
- Information classification
- Replacement value
- Business criticality

There are several types of assets: Information -, Software – and Physical assets. This thesis project target was mapping Information assets.

While identifying information assets is time costly but doable, finding accountable personnel for it is much more difficult, which is understandable. If a business critical component would be destroyed, crippled or disabled, a financial loss could be significant furthermore a loss of life could be involved. Taking responsibility for such consequence could mean a loss of freedom or/and financial fine and more complication arises when assets are stored by the third party. Thus it is difficult to define responsible personnel within the company.

Excluding the idea of taking responsibility, establishing ownership of asset is still mandatory, because the person who is asset owner is liable for information accuracy. Modifications and additions to the information assets need to be approved by the asset owner. (Identifying and classifying assets 2002)

Asset owner is the one that defines access rights for individuals as well as groups. Confidential information needs to be managed and controlled. This is difficult to define for classification may vary from point of view, for example, CEO probably deals with “Highly Sensitive” information while sales manager deals with “Sensitive” label, but they might want to classify

outgoing deal as “Highly Sensitive”, thus the problem becomes even harder when company is in collaboration with other companies. Different methods need to be used when dealing with classified information, having an agreement with collaborative companies is a must for information handling.

2.5 ELV and EE internal regulations and documents

Elektrilevi is a large company and it has its own internal regulations and documents. Gathering knowledge on ELV’s business processes was essential for understanding relationships between them. ELV has seven main processes and eight supporting processes, see Figure 7.

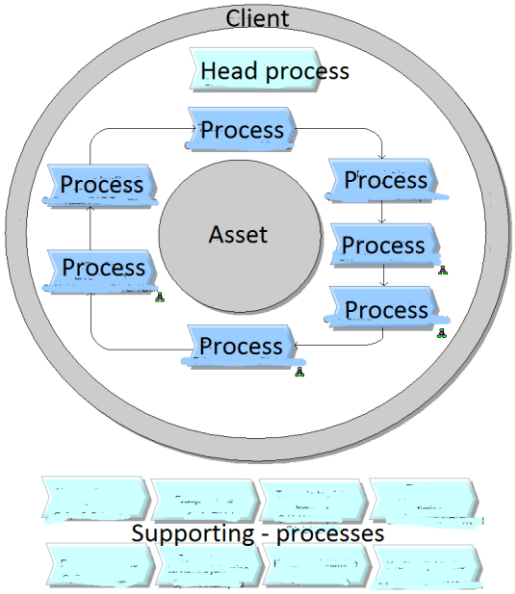

Figure 7: ELV process map

“Information assets and access rights management” was document that was followed during the project. It regulates how the information assets should be mapped and how user access rights should be managed, the document was created by Eesti Energia.

Due to business secrets, this thesis will not explain nor dwell into researching company’s internal documents. However when a decision was made it will point to internal documents, for example, if some method was chosen over another, and the reason is that it’s regulated by an internal policy it will be mentioned.

2.6 CRUD model

To better understand user access to information assets a security model was needed, a classification for users. Its aim should be to prevent and deny access for wrong personnel to have an access to information. CRUD model was chosen due to the need of more detailed method was needed and company's internal document highly encourages the usage of it.

2.6.1 CRUD model

Figure 8: CRUD model

CRUD model stands for create, read, update and delete. Its purpose is to clarify which user groups have what types of permissions to a file, document or a database. It is best to implement this method when you have multiple users. The same method is well suited to determine software access rights as well.

For example, you have to groups of workers, ones that create and structure data and ones that use that data to do their work. The first group of workers has CRUD rights for the data and second worker groups have only R rights for it.

Since there can be multiple groups that need to work with information a CRUD model implementation is critical for information assets, thus to get a good overview of user access rights for different assets a CRUD was used. Eesti Energia's internal documents also regulated that this model needs to be used when classifying user access permissions.

2.7 CIA triad

Begin able to assess the user access rights is not enough, thus a CIA triad method was used. CIA triad stands for confidentiality, integrity, and availability which is also referred as fundamental and central factors of security. To shortly disclose, confidentiality is meant to limit access to information, integrity is to ensure that information is trustworthy and accurate, and availability is a guarantee of access to information for authorized people. See Figure 9

Figure 9: CIA triad model

- **Confidentiality**
  Confidentiality is practically equal to privacy. To ensure that sensitive information does not reach the wrong people and at the same time reaches the right. It is also common to classify and categorize information according to an amount of the damage it could do if it were inappropriately handled.
  A good example of practices to ensure confidentiality is a Data encryption, Passwords, authentication and other similar methods that validate the person trying to access information.

- **Integrity**
  Integrity revolves around data consistency and truthfulness over its entire lifecycle. Data should not be modified by unauthorized people or may not be changed during transit. Measures to ensure this, revolve around access controls, version control is also part of it due to accidental changes or deletion by authorized users.
  Also, physical countermeasures need to be in used as an outcome of non-human-caused events such as a backup failure, server crash, and electromagnetic pulse.

- **Availability**
  Availability assures that information always available when it is needed. This means that computer systems that store information must be protected and the communication channels must function correctly. High availability systems that need to remain available at all times, need to have backup power in case power outages as well as right network routing in case of denial-of-service attack, which is a flood of incoming messages to a target system which will bring it down due to high workload and latency.

CIA triad was taken into use for information asset mapping since CIA triad offers good overview from the security point of view and Eesti Energia's internal documents regulate that it need to be used when mapping information assets. Also, Republic of Estonia Information System Authority has ISKE guidelines which rely on IT- Grundschutz material and has CIA triad implementation instructions. (Information System Authority 2016)

2.8 ISKE

The security level tolerable for the data processes in IT systems is the aim of implementing ISKE. Enforcing the standard is the fundamental security level and accomplishing measures of organizational, infrastructural/physical and technical security measures.

ISKE is developed by Republic of Estonia Information System Authority, for the Estonian civil part. On their website, they claim that ISKE is compulsory for state and local government organizations who handle databases or registers, by the government regulation no. 273. Fortunately, Elektrilevi is private company, thus applying ISKE is not mandatory however it is recommended.

ISKE is adapted to suit Estonia's needs and it is based on a German information security standard called IT-Grundschutz. IT-Grundschutz offers an extensive set of safeguards, regularly updated, suitable granularity, Enables development to a common understanding about the security levels needed for public sector IT systems.

ISKE can be thought of baseline system with three different sets of security measures, with separate security requirements developed. It is accurate however it is inaccurate compared to detailed risk analysis. Another lack of ISKE is that it has not been translated into English.

2.8.1 ISKE consequence rating guide

ISKE also has a four level guide for rating consequences. It was used to measure information assets criticality, in case an asset gets destroyed. They guide was adjusted according to companies needs and viewpoint to apply it with the best potential.

3 Research method

The second phase of the project consisted of booking meetings with key personnel and having directed interviews with them.

A qualitative method was used for gaining information during this Project. It involved conducting interviews with process managers within the company, where we would have a guided conversation with them. Semi-structured format was followed, when a meeting was booked a guide was included within the booking notification. Booking was done with IBM Notes software. However, different paths were free to follow during conversations so that over the course of the interview certain topics would clarify and expand themselves. (Methodology 2016)

4 Implementation

This section explains several key concepts used for the project, how it was started and what theoretical background research had to be done. To better understand how the project was conducted to the point of interviews, several topics needed to be explained.

4.1 Project kick-start

In the first project meeting with company CISO, we decided how we are going to approach given task at hand. Project process was divided into two phases see Figure 10: Project process.

In the first phase, our aim was to find out exactly what details our information asset classification mapping would need. We would set meetings and give ourselves action points. In each meeting, we would update and review the findings. Once we had the base table for information assets mapping and a list of personnel to interview, we proceeded to next the phase.

In the second phase, we would set meetings with process managers, bookings were done in IBM notes software. For meetings I also developed meeting guidelines for managers to have more effective and managed the interview, it was sent to them with booking notification so they could prepare beforehand.

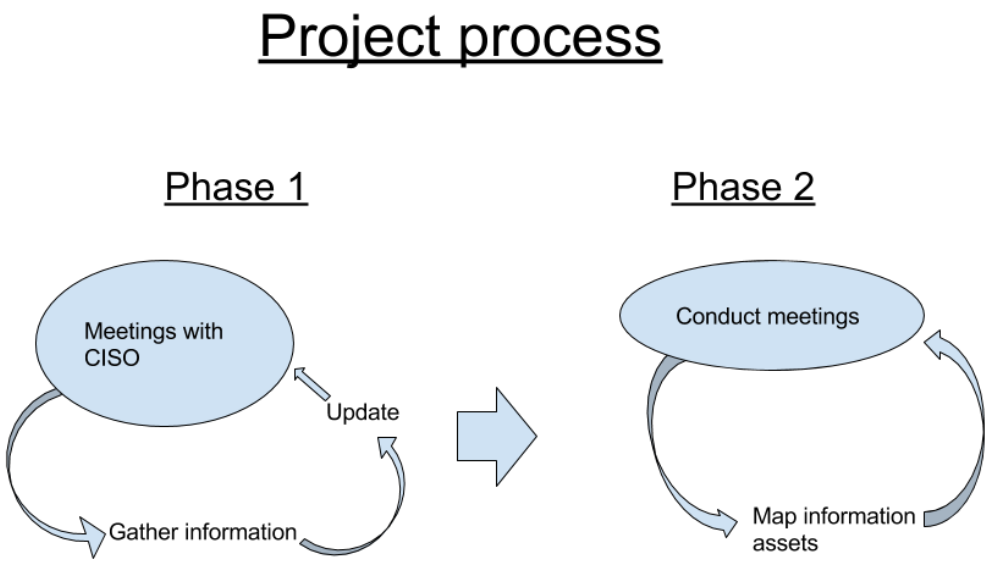

Figure 10: Project process

Since most of the research and ideas were gathered from the internet a system was needed to sort out relevant findings. OneNote was the software used to document useful quotes and remarks as well as links to web pages that contained relevant information for the project. Documents and laws that were lengthier and contained highly relevant information were printed out and important parts marked with a highlighter.

4.2 Project management

No Project management software was used during the project, because of the team size. Using project management software would been excessive for the project this scale. However having tool, where you can manage your tasks and deadlines would have been beneficial, unfortunately it would not have been reasonable due to my nature of work where unanticipated work tasks often appear.

Project workflow was managed with weekly meetings, where I would report on my progress to CISO and ask for mentoring if needed. Documents generated and used during the project were stored on company's local network drive.

There was no project plan in use, however "Plan-as-you-go" method was practiced during the project. Things can change fast and not everybody ought to have a formal plan document written out. The plan is useless, but planning is essential. Thus main focus was on doing practical work rather than creating a plan ahead. (Plan as you go 2008)

4.3 Implementation of laws

During the interviews, we mapped information assets and classified them, along with laws. The aim was to find potential irregularities and problems with information assets that might be in conflict with laws. This mainly revolved around personal views, since each individual on different position will see things from different perspective. It gave a broader view on information assets and overall business operations.

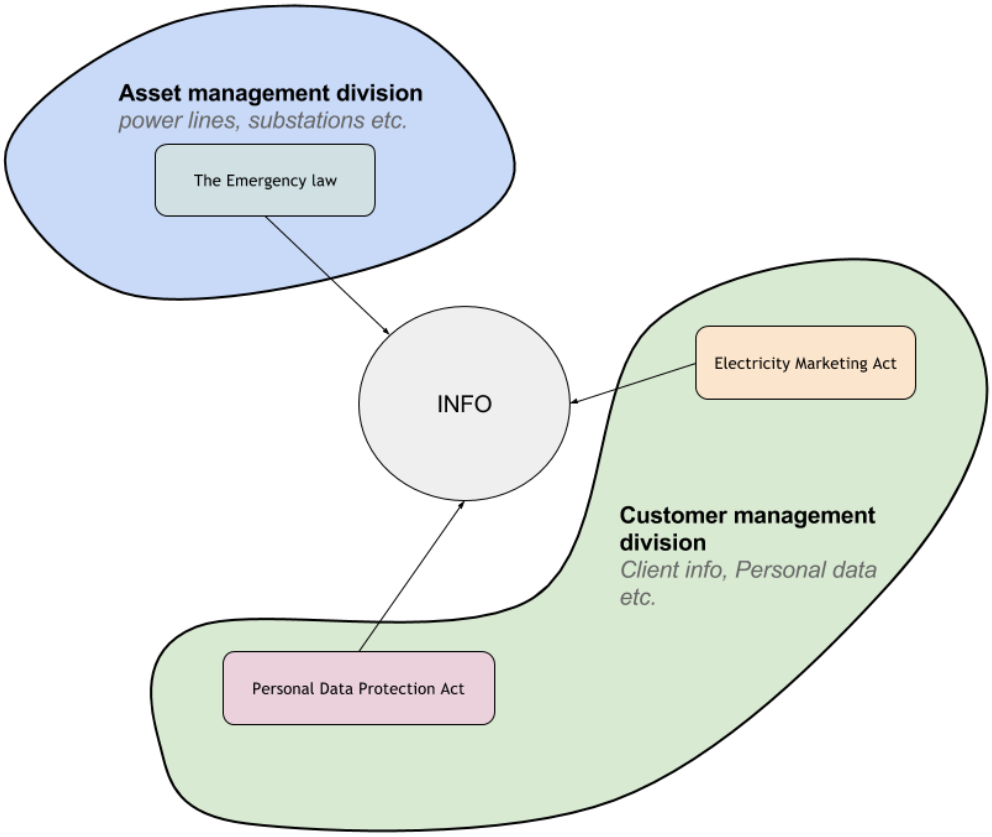

Figure 11: Information assets affected by laws

4.3.1 ISKE implementation in the project

ISKE was used to classify information assets confidentiality, integrity, and availability. ISKE has set of predefined security classes for classifying CIA triad on four point scale. Where the zero is the lowest class and four the highest. ISKE has a security class assignment requirements in place, see Figure 12.

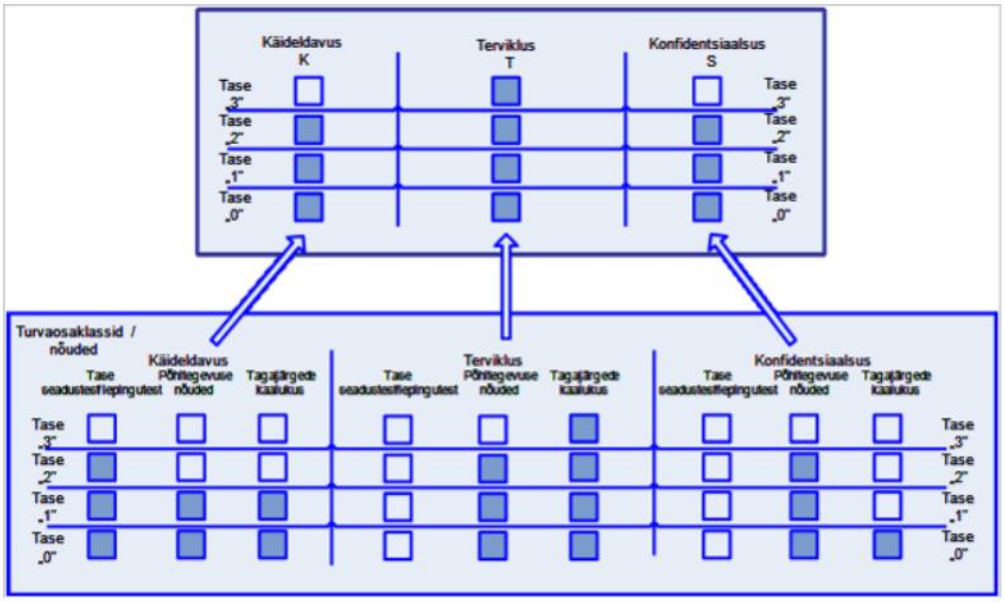

Figure 12: ISKE rating requirements

According to ISKE an information asset could have classification of following: K2T1S2 Where K stands for availability, T for integrity and S for confidentiality. ISKE has an instructions to measure the security level of given data. There are three levels: low -, medium -, high level. Given example would be considered as medium security level according to Figure 13.

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Figure 13: ISKE rating guide

4.4 Asset classification scheme

A base document was created to map information assets. It was created using previous out-dated document. Software used was Microsoft excel, reason was simplicity and user knowledge. There is no reason to use complex software, it is time-consuming and requires user training. Document consisted of following rows:

- Number
- Information asset name
- Information asset owner
- Usage in business processes
- Security class
- Access rights
    - Role
    - Group
    - Division code
    - CRUD
- Location
    - Primary
    - Secondary
- Financial risk
    - Consequences level
    - Recovery costs

Where higher level list items define category where the sub-classification belongs. Following Figure 14 shows the base document headers.

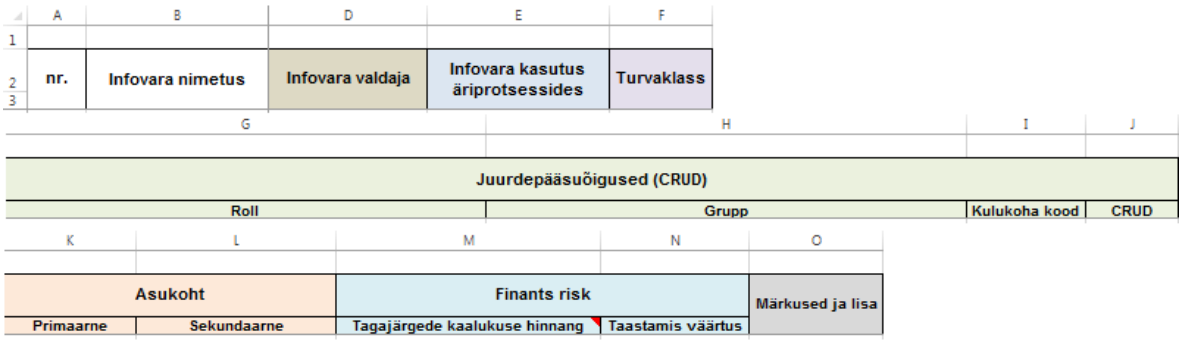

Figure 14: Base document headers

4.5 Preparing for interviews

A list of key personnel was obtained and meetings were booked using IBM notes software. Guidelines were developed to have more productive and constructive meetings with personnel. Information assets were mapped and remarks were made where information assets could not be in accordance with laws.

4.6 Interviews

Conducting interview and mapping the assets was the second phase of the project. The start of this phase was overestimated, research took longer and finding the key personnel to interview was intricate. Thus this phase was postponed to November.

The plan was to interview three key personnel whose work responsibilities are involved with laws mentioned above. This was done before conducting meetings with process managers, the aim for this was to get a broader view on information assets that might have problems with laws and political views. Guidance on how to better gather data about information assets and what other classifications should be used was also gained.

Only two meetings with process managers were conducted at the point of writing this. Few information assets were mapped, from customer management division.

4.7 Mapped information asset example

The following example will explain the information assets that was mapped during conducted interviews. An example information is changed due to confidentiality reasons and some information classifications are left out. Example is divided into three tables - general information, user access rights, and business criticality measures.

Information assets name	**Information asset owner**	**Business process usage**	**CIA triad**
Customer information	Some division code and responsible person	Process 1 Process 2 Process 3	K3T4S4

Table 1: Information asset general classification table

User access rights			
Role	Group	Division code	CRUD
Data creator Data user	Specialists Customer support	Sample code Sample code	CRUD R

Table 2: Information asset user access management

Asset location		Financial risk	
Primary location	Secondary location	Criticality rating	Reclamation costs
Server A	Server B	R3	4 000 000

Table 3: Business criticality rating measures

Given example table's intent is to give an idea of what was and what will be mapped during the information assets project, which will be the outcome of the project.

5 Conclusion

The project itself is going well, yet thesis must be finished beforehand because of the time limitation. The project continues even though the thesis was completed before it. There are already next projects in place once the mapping of assets is done. During the project, time management has been the most difficult part of it. However, it was expected since Elektrilevi is a large company and has lots bureaucracy involved within. Once the project is completed company will gain highly beneficial document which allows further analysis of information assets.

References

Brasso, B. 2016. CYBER ATTACKS AGAINST CRITICAL INFRASTRUCTURE ARE NO LONGER JUST THEORIES. Accessed 14 November 2016.
https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html

Elektrilevi. Accessed 18 October 2016.
https://www.elektrilevi.ee/en/elektrilevi-tutvustus

Haeusser et al. 2007. Information Lifecycle Management Best Practices Guide. Accessed 22 September 2016.
http://www.redbooks.ibm.com/redbooks/pdfs/sg247251.pdf

Identifying Information Assets and Business Requirements. 2011. Accessed 21 September 2016.
http://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

Identifying and classifying assets. 2002. Accessed 25 September 2016.
http://www.networkmagazineindia.com/200212/security2.shtml

Industrial Control Systems 2016 Report: Connected and Vulnerable. 2016. Accessed 29 October 2016.
https://www.ptsecurity.com/upload/iblock/6bd/ics_vulnerability_2016_eng.pdf

Information System Authority. Accessed 5 October 2016.
https://www.ria.ee/en/iske-en.html

Kawasaki, G. 2008. Plan as you go. Accessed 20 September 2016.
http://www.sausd.k12.ca.us/cms/lib5/CA01000471/Centricity/Domain/494/PlanAsYouGo.pdf

Official Journal of the European Union. 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. Accessed 21 October 2016.
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Rouse, M. 2014. Confidentiality, integrity, and availability (CIA triad). Accessed 29 September 2016.
http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Writing your Dissertation: Methodology. Accessed 25 October 2016.
http://www.skillsyouneed.com/learn/dissertation-methodology.html

Figures

Tables