Tallinn University of Technology

Faculty of Information Technology

Department of Informatics

E-Governance Technologies and Services

Modern governments need No Legacy Policy to keep ICT cost under control

Master's thesis

Student: Aet Rahe

Student code: 143933IVGM

Supervisor: Taavi Kotka

Co-Supervisor: -

Tallinn

2015

Author's declaration

I confirm that I have constructed this Master's thesis individually and that the current paper has not been presented by anyone before. All resources, viewpoints, citations, and other materials from other authors that have been used in this thesis have been referred to.

Kinnitan, et olen koostanud antud magistritöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

---------- ----------

(kuupäev / date) (allkiri / signature)

Juhendaja / supervisor PhD candidate Taavi Kotka:

Kaitsmiskomisjoni esimees / Chairman of the defence committee:

Annotation

Süstemaatiline lähenemine IKT investeeringute juhtimisel ja vananeva tehnoloogiaga *(IT legacy)* toimetulek on muutumas üha olulisemaks, seda ilmestab nii Eestis kui ka teiste edukate e-riigi võimaluste rakendajate kogemus.

Eesti avaliku sektori olulised äriprotsessid on peale taasiseseisvumist üsna suures osas automatiseeritud ning eesmärgiks on seatud jätkuv IT nutikas rakendamine riigijuhtimise tõhustamiseks. Seega on ühiskonna toimimiseks vajalike protsesside sõltuvus IT süsteemidest järjest suurem. IT infrastruktuur aga vananeb nii nagu igasugune muu infrastruktuur ning seetõttu on vananevate infotehnoloogiliste lahenduste kuhjumise vältimise küsimused muutumas üha tähtsamateks. Tagatud peab olema infosüsteemide turvalisus, järjepidevus ning jätkusuutlikkus.

Täna puuduvad selged poliitikasuunised kriitiliste infosüsteemide investeeringute jätkusuutlikuks planeerimiseks ning vananenud infotehnoloogiliste lahenduste probleemiga tegelemiseks, s.h. taaktehnoloogiatest õigel ajal vabanemiseks.

Käesoleva töö peamine eesmärk on leida vastus kahele põhiküsimusele (MQ): **kuidas õigeaegselt tuvastada, millised infosüsteemid on vananenud,** ning **kuidas tagada avaliku sektori jätkusuutlik sõltumatus taaktehnoloogiatest?** Nendele küsimustele vastuse saamiseks hõlmab uurimustöö täiendavalt 7 alaküsimust (SQ).

Magistritöö uurimisküsimused on:

Uurimuse põhiküsimus 1 (MQ1): **kuidas õigeaegselt tuvastada, millised infosüsteemid on vananenud?**

- SQ 1.1. Millised on peamised põhjused infosüsteemide taasloomiseks olemasolevat lahenduste pideva parandamise asemel?
- SQ 1.2. Millised on peamised kriteeriumid ja riskid, mida infosüsteemide uuesti loomise vajaduse hindamisel tuleks arvesse võtta?
- SQ 1.3. Kas ja millistel juhtudel tuleb kaaluda infosüsteemi uuesti loomist ka siis, kui infosüsteemi käitlemisel ei ole ilmnenud vananenud tehnoloogiale omaseid tunnuseid?

Uurimuse põhiküsimus 2 (MQ2): **kuidas tagada avaliku sektori jätkusuutlik sõltumatus taaktehnoloogiatest?**

- SQ 2.1. Kas avalik sektor vajab poliitikasuuniseid, mis aitavad vältida vananenud infotehnoloogiliste lahenduste kuhjumist?
- SQ 2.2. Juhul, kui sellised poliitikasuunised on vajalikud, siis millisel kujul peaks neid rakendama?
- SQ 2.3. Milliseid IT juhtimise aspekte peaksid taaktehnoloogiast vabanemise poliitikasuunised hõlmama?
- SQ 2.4. Millist mõju omab taaktehnoloogiast vabanemise poliitika avaliku sektori asutuste eelarvele?

Käesolev töö on kirjutatud inglise keeles ning sisaldab teksti 72 leheküljel. Töös on 7 sisulist peatükki, 3 tabelit, 22 joonist ja 4 lisa.

Abstract

Systematic approach in ICT investment management process, including dealing with IT legacy problem, is becoming increasingly important as shows the experiences of Estonia and other governments who have been successful in implementing e-government solutions.

A considerable part of important business processes of the public sector of Estonia have been automated after Estonia regained its independence. In addition, one of the major IT-policy objectives of Estonia is smart implementation of IT solutions for better governance. Thus, processes that are necessary for the functioning of the society are becoming increasingly dependent on IT systems. However, IT infrastructure becomes outdated just like any other infrastructure and the questions of how to avoid the excessive build-up of IT legacy are becoming increasingly important. Cyber security, continuity and sustainability of IT systems must be ensured.

There are currently no policy guidelines to support sustainable investment planning process of critical IT systems and to deal with the problem of outdated IT solutions, including timely elimination of legacy technologies.

The objective of the current thesis is to find answers to the two main questions (MQ), **how to find out which IT systems are becoming outdated in the right time** and **how to sustainably ensure that the public sector is free of IT legacy?** In order to answer these questions, the study contains additionally 7 sub-questions (SQ).

The research questions of the thesis are the following:

Main question 1 (MQ1): **How to find out which IT systems are becoming outdated in the right time?**

- SQ1.1. What are the main reasons why rewrites should be considered, instead of endlessly continuing to fix legacy system?
- SQ 1.2. What are the key criteria and risks to be considered when planning a re-write project?
- SQ 1.3. In which cases should rewrites be considered even if there are no symptoms of outdated technologies present?

Main question 2 (MQ2): **how to sustainably ensure that the public sector is IT legacy free?**

- SQ 2.1. Is there a need for No Legacy Policy guidelines in the public sector to avoid the build-up of IT legacy?
- SQ 2.2. In case such guidelines are needed, how should they be implemented?
- SQ 2.3. What kind of IT management aspects should the No Legacy Policy guidelines include?
- SQ 2.4. What kind of effect the No Legacy Policy might have on IT budgets of public sector organisations?

This thesis is written in English and it contains 72 pages of text. It includes 7 substantive chapters, 3 tables, 22 figures, and 4 appendices.

Abbreviations and concepts

- EU – the European Union is an organisation that connects European countries and is built on economic and political partnership. There are currently 28 member states in the EU (European Union, n.d.).
- Important (mission critical) IT systems – in this study, a mission critical information system is a system that is vital for operating the main business processes of a public sector organisation. If the information system would stop working for longer time, this would paralyze the main functions of that organization. The key processes of the organisation would not be manageable at all or would be manageable with great difficulties (include unreasonable alternative costs etc.) without the support of the IT system. The replacement of critical IT systems by manual work is riskier (e.g. less secure) or much more expensive than the creation of a new IT system or going back to manual labour would significantly decrease the transparency of the organisation.
- Legacy systems (also: legacy) – in this study legacy systems (or legacy) means software that has become outdated and no longer meets business needs. Legacy system may or may not reveal symptoms that are typically the indicators that the IT solution is becoming technically outdated (legacy symptoms). Thus, an IT solution can become legacy even before the technological platform becomes outdated.
- Legacy symptoms – e.g. increase in bugs, spaghetti architecture, increasing maintenance costs, and other problems that emerge as a result of using outdated technology.
- NoLP – No Legacy Policy – a set of guidelines that aim to support getting rid of existing IT legacy and help to avoid the build-up of legacy systems in the long run. One of the core principal suggested by Estonian government CIO Taavi Kotka is that there should not be any important IT systems in use in the public sector that are older than 13 years.
- OECD - Organisation for Economic Co-operation and Development with the mission of organising best practices sharing. OECD has many IT and digital economy oriented working groups. Currently the organisation has 34 member-countries (OECD, n.d.).
- SCADA systems - Supervisory Control and Data Acquisition systems are real-time process control systems that monitor and control local or geographically remote devices (Tsang and Smith, 2008).

List of Tables

List of Figures

Table of Content

Acknowledgements

I would like to express my sincere gratitude to my mentor, a long-time friend and a visionary – Estonian government CIO Taavi Kotka, whose idea it was to start investigating the issues related to IT legacy in the public sector. I also want to thank him for being my partner in crime in conducting the research and supporting me with his ideas throughout the whole process, but also for giving me well-needed kick in the back to keep going!

My special thanks go to Estonian government IT architect Andres Kütt for his insightful comments and criticism, to Karin Rits for being a good pair of objective eyes to review my work and for being a patient audience, always willing to listen to me talking out loud to clear my thoughts. I also want to thank Maili Mahlapuu for being a partner in the Estonian ICT investment management processes and supporting the implementation of first steps of No Legacy Policy in Estonian government.

I also want to express my gratitude to Urmo Pärg, Innar Liiv, Karin Oolu and Regina Sirendi for their comments and suggestions on how to improve the thesis, as well as to all of the experts who found time to share their thoughts and experiences with me during the study.

And last but not least, I would also like to thank my dear daughter Age-Iiris for being ever so patient. I can never repay her the time I have spent doing this study on her expense.

1. Introduction

The main motivation to investigate the problem related to the build-up of IT legacy in the public sector comes from practical needs. The Estonian government ICT policy makers have realised that unless conscious steps will be taken against legacy build-up, the problem remains and deepens. First, comprehensive studies in the field are needed to understand the dynamics happening in the public sector that stop from actively dealing with the issue. This study is planned to be one of the first steps in the attempt to achieve in-depth knowledge about these dynamics and to plan further steps to eliminate legacy.

To provide a better justification about the motivation of this study, some important technology and public administration trends need to be explained.

Governments all over the world are facing growing pressure to **control their IT budgets**. The UK has established an objective to decrease the government's IT budget 1 billion pounds per year, from a yearly budget of 20 billion pound to 16 billion pounds (Maxwell, 2013). At the same time, a survey done by Gartner (Moore, 2013) revealed that 75% of government CIOs estimated that IT budgets will remain the same or increase in upcoming years. Thus, unless changes will be introduced to IT investment management in the public sector, the majority of governments will be facing increasing IT costs.

It is common knowledge that when IT systems age, the **knowledge about the IT system** (how the system operates and what is the exact business logic behind every function) **tends to fade away** as team members change over time. It is impossible to ensure perfect documentation about an IT system and it is even harder to keep it so over the years. This can lead to a situation where at some point it is easier to **avoid making changes** because of not having anyone available who knows the system inside out and can help to estimate all the side-effects that the planned changes are going to cause. All changes become more and more **risky and expensive** due to lack of knowledge about the IT solution and the related business processes.

According to the study by Erlikh (2000) the **proportion of maintenance cost can be up to 90%** of the total software cost when legacy systems are in use. Seacord et al. (2003) have called this phenomenon the *legacy crisis*.

Thus, one can argue that unless governments start making conscious efforts to eliminate legacy, they will **lose the ability to invest into innovation** due to ever-increasing maintenance costs.

There are many international organisations and co-operation networks dealing with the exchange of best practices and providing policy guidance on IT co-ordination in the government: OECD[1], EU, ICA[2], D5[3] workgroups and many others. Those bodies involve government CIOs, cyber security experts, IT policy makers and public sector IT managers. Even though these formats exist, **there is no comprehensive collection of concrete recommendations for governments that government CIOs and policy makers can take as guidelines in making decisions on whether to fix or rewrite mission critical government IT systems.**

The lack of guidelines has resulted in having many old information systems and technologies still being in use in governments. During consultations carried out in the framework of current study, all Nordic countries[4] government policy makers admitted without hesitation that there are many legacy systems in their government. Nordic countries started developing their government IT systems more than 20 years before Estonia and they are still actively running IT systems that are 20, 30, or sometimes even 40 years old (Nordic countries IT policy coordinators, 2015). At the same time they admit having no specific policies or guidelines in government-wide use, which would help to fight against the build-up of IT legacy. Similar trends are also reflected by other successful e-governments like New Zealand (Occleshaw, 2015), Singapore (Poh, 2015), UK (Maxwell, 2013) and many others.

It is also remarkable that the IT budgets of these countries tend to be 30-40 (or more) times bigger than the IT-budget of the Estonian government (Kotka, 2014; Nordic countries IT policy coordinators, 2015). This cannot be justified by the size of the population because that does not add additional functional requirements to the government IT system – small countries need to provide the same kind of services to citizens as larger countries. The size of the population affects the number of rows in the tables and this cannot be the root-cause of such a huge difference in government IT budgets (Kotka, 2014).

The budget difference also applies to the private sector. IT managers with previous experience from the finance sector admitted that IT projects with similar functional scope, undertaken in different countries had a budget difference of at least 10 times. They illustrated this by adding an

[1] OECD - Organisation for Economic Co-operation and Development – on organisation with the mission of organising best practices sharing. OECD has many IT and digital economy oriented working groups. OECD has 34 member-countries.

[2] ICA – International Council for IT in Government Administrations. Non-profit organisation with the goal of informal exchange of ideas, knowledge and experiences on management and the use of Information and Communications Technologies (ICT) in central government administration.

[3] D5 – leading digital governments network initiated by UK in 2014, involves 5 member states: Estonia, UK, Israel, New Zealand and South Korea. The goal is to exchange best practices among leading e-governments.

[4] Nordic countries: Finland, Sweden, Denmark, Norway

example that the budgets for IT projects in Estonia were typically around 10 times smaller than in Sweden. And the main reason for that was over 20 year's old legacy back-end systems in Nordic countries (Anon., 2015).

Another symptom of legacy problem is the active use of old programming languages. For example a programming language COBOL, designed in 1959[5], is still widely used in US companies based on survey done by Computerworld (Mitchell, 2006). According to that survey 62% of US IT managers admitted having COBOL systems still in use, 36% of them said that they gradually plan to migrate off from COBOL systems and 25% of them said that they would like to do so if the rewrites would not be so expensive (Mitchell, 2006). The same study states that 55% of those who do not use COBOL as a programming language say that the main reason for not using it is that it is an outdated language. In addition Konkel (2012, 2013) emphasizes that one of the reasons why the US government is spending 70% of its IT budgets on maintenance is because of legacy systems. He too points out that the US government is still heavily using outdated COBOL systems.

According to Wagner (2015), many EU agricultural payment agencies are still using old COBOL systems. Some of them were built in the early and mid-80's, making the core systems now 30 years old. Since the systems are very complex and have a lot of built-in business logic that now has to be revised and reinvented, the rewrite projects are estimated to last around 5-7 years. Showcasing that in case systems get too old, the rewrite projects tend to get enormous in terms of budget and implementation timeline.

New Zealand (Occleshaw, 2015) has a similar example of rewriting an outdated social affairs system. Because the existing IT system was over 20 years old, there was no one left in the public sector authority, who knew the processes and the legacy IT system inside out. Thus, once the rewrite project was initiated, it was decided that the rewrite will only be about changing the technological platform and no business processes will be redesigned because of the fear of project becoming unmanageable and fail because of involving too many changes at the same time. This is another good example of dealing with legacy too late and thus, making it impossible to find positive business case to justify the cost of the rewrite project. Usually the financial justification for a rewrite comes from optimizing the processes – automating manual work, getting rid of paper-based processes etc. Thus, dealing with legacy systems too late, in a stage where the main goal is to get rid of the platform that is technologically obsolete, may make it very difficult to harvest those benefits due to the fact that the main purpose is not to review and optimize related processes, but to get off the platform that is just not functional any more. As a result, the overall process

[5] COBOL history: http://en.wikipedia.org/wiki/COBOL

related costs will stay the same making it difficult to get funding to initiate the rewrite project. IT projects tend to be complicated because it is difficult to keep track and know that you are on the correct path until you finally start using the system in production environment. Therefore, the more unknown variables are in play, the more difficult is to complete the project successfully. The older the system, the more unknown variables are on the table because of the loss of knowledge that has happened over the years. As a consequence – the project becomes more expensive and risky to manage. One of the ways to lower the risks is to avoid too many changes in the processes during the rewrite project. Thus, one could argue that the later the rewrite project is initiated, the more controversial might be the situation due to the fact that managing too many changes that are needed to justify the investment, make it harder to successfully complete the project, thus making the rewrite of a system financially unprofitable.

Even though majority of people dealing with IT systems are aware of problems related to legacy IT systems, the experience of many other successful e-governments shows that **timely elimination of IT legacy does not happen organically.** It is difficult to take steps to fight against legacy, especially in the public sector, where investments are funded using public money. Improving processes will not, in most cases, help the government to earn more money, which is an important difference compared to the private sector. Thus, it is more complicated to justify the business case of a rewrite project in the public sector. This, in turn, makes it emotionally difficult to make the decision to rewrite an important and expensive information system, especially if seemingly there is nothing wrong yet (the services work most of the time for the citizens etc.). In case an important IT system fails or serious cyber incident happens, it is of course much easier to find funding, but governments should not wait that long, especially in dealing with mission critical government information systems.

By investing more and more into IT, **countries are becoming increasingly dependent on IT solutions**. Estonia already has a critical dependency on IT systems. Information System Authority conducted a study[6] in 2014 among vital services providers. The study showed that over 80% of vital service providers estimated that their dependency on IT systems is high or very high. Beidleman (2009) states that computers control a large part of Americas' critical infrastructure and many essential processes in manufacturing, utilities, banking and communications.

[6] Survey done by Information System Authority in 2014 - 41 vital services owners IT managers and information security managers participated in the survey. Survey results are not publicly available because this information is a matter of state defence.

So the need for systematic approach to IT systems lifecycle management is becoming more crucial than ever.

As a conclusion – the main motivation behind this study is to investigate the problems related to legacy systems and the obstacles governments face in dealing with legacy. The aim is to find out whether more concrete NoLP guidelines are needed. In case it is so, the long term goal is to work out No Legacy Policy guidelines for the Estonian government to sustainably ensure that the public sector is IT legacy free.

Main research question

The objective of the this study is to find answers to two main questions (MQ), **how to find out which IT systems are becoming outdated in the right time** and **how to sustainably ensure that the public sector is IT legacy free?** In order to answer these questions, the study includes additionally 7 sub-questions (SQ).

The research questions of current thesis are:

Main question 1 (MQ1): **How to find out which IT systems are becoming outdated in the right time?**

- SQ1.1. What are the main reasons why rewrites should be considered, instead of endlessly continuing to fix legacy system?
- SQ 1.2. What are the key criteria and risks to be considered when planning a re-write project?
- SQ 1.3. In which cases should rewrites be considered even if there are no symptoms of outdated technologies present?

Main question 2 (MQ2): **how to sustainably ensure that the public sector is IT legacy free?**

- SQ 2.1. Is there a need for No Legacy Policy guidelines in the public sector to avoid the build-up of IT legacy?
- SQ 2.2. In case such guidelines are needed, how should they be implemented?
- SQ 2.3. What kind of IT management aspects should the No Legacy Policy guidelines include?

- SQ 2.4. What kind of effect the No Legacy Policy might have on IT budgets of public sector organisations?

This study will only focus on important (mission critical) information systems. A **mission critical information system** is a system that is vital for operating the main business processes of the public sector organisation. If the information system would stop working for a longer period of time, then this would paralyze the main functions of that organization. The key processes of that organisation would not be manageable at all or would be manageable with great difficulties (include unreasonable alternative costs etc.) without the support of the IT system. The replacement of critical IT systems with manual work is riskier (e.g. less secure) or much more expensive then it would be to create a new IT system, or going back to manual labour would significantly decrease the transparency of the organisation.

IT systems outdate similarly like other infrastructures and, thus, it is not the question IF IT systems need to be rewritten or not, but about how to decide WHEN is the right time to plan the rewrite project.

Estonia has started dealing with the IT legacy very actively and is already implementing No Legacy Policy principles (i.e. consciously taking actions to rewrite important systems that are becoming legacy). So far the implementation has been based on soft activities like awareness raising and knowledge sharing among Estonian government IT managers. The principle of NoLP is also kept in mind during the ICT investment management processes governed by the Estonian Ministry of Economic Affairs and Communications. These recommendations and information exchange activities have brought along many initiatives to get rid of existing legacy systems, but one of the aims of the study is to understand if more concrete requirements should be implemented to move forward. The experience of implementing NoLP principles so far shows that organisations with higher ICT management maturity tend to have lower need for more strict guidelines than the organisations that have lower ICT management maturity.

Main contributions of the thesis

The main contributions of the thesis are:

- Achieving a comprehensive overview of problems that impede getting rid of IT legacy in the government.

- Based on study results, working out recommended rules and implementation mechanisms that help to sustainably keep governments IT legacy free.

This masters' thesis will have a practical impact – it will be taken into account in the process of clarifying the requirements and guidelines in implementing the next steps of No Legacy Policy for the Estonian government.

Outline of the thesis

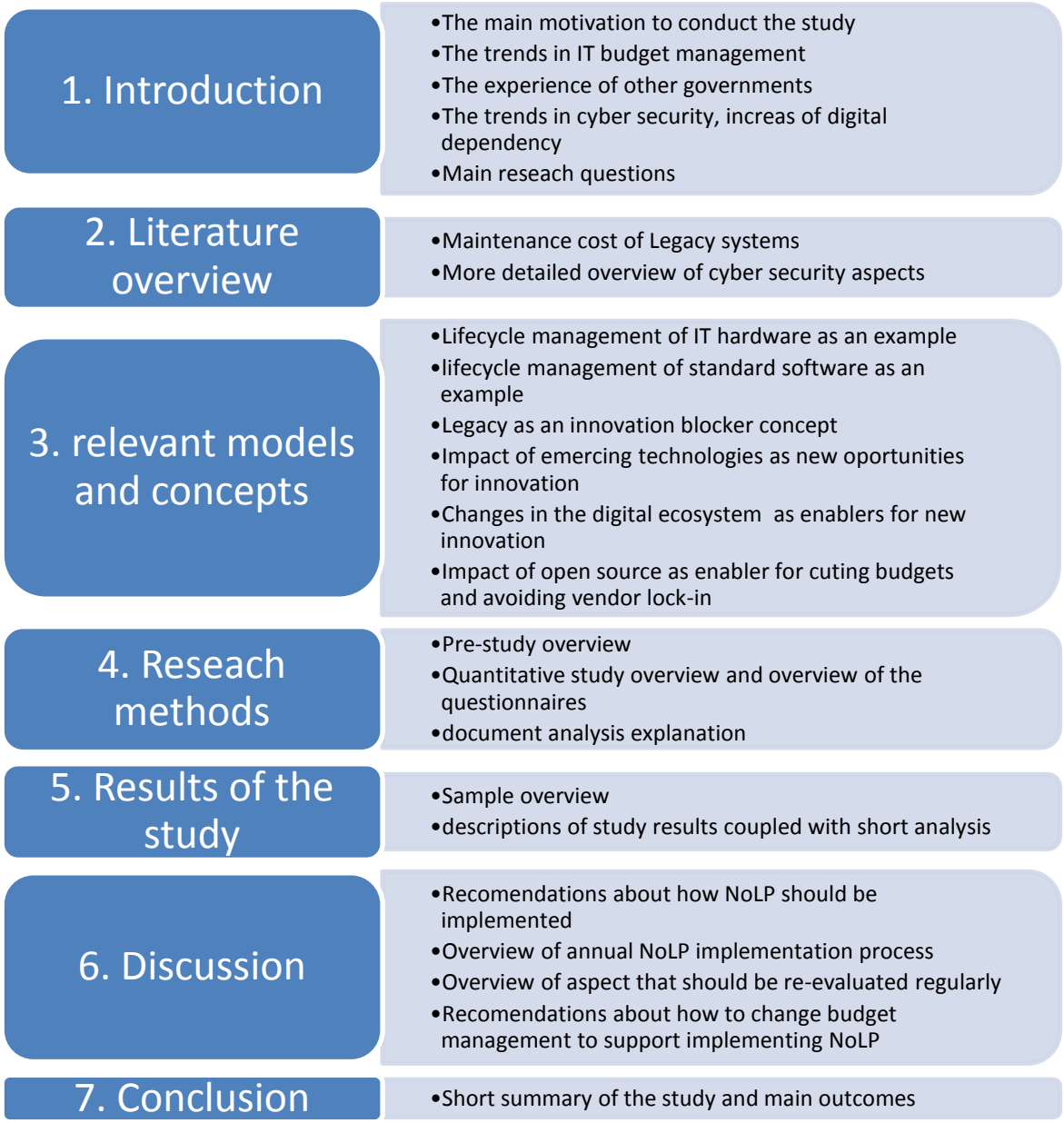

Figure 1. The structure of the thesis

In this chapter, the author introduces the background of the study that explains the **main motivation** to conduct the study.

Chapters 2 and 3 build the necessary background for further research. Chapter 2 will provide **literature review** with the focus on maintenance costs and cyber security aspects. In the 3rd chapter **relevant models and concepts** that should be taken into account while solving the legacy issues are introduced. In that chapter author explains different examples and influencers like lifecycle management of IT hardware and standard software, the idea of legacy as an innovation blocker, the impact of emerging technologies, need to follow and analyse changes in the ecosystem, and the impact of open source software becoming increasingly popular.

The 4th chapter gives an overview of the **study methods**, followed by overview of **study results** that are coupled with short analysis of the results in the 5th chapter.

6th and 7th chapters of the thesis cover the **discussion** about the study results and the main **conclusions** of the study. In the discussion chapter, the author shares **recommendations about how No Legacy Policy should be implemented** explaining the necessary prerequisites, processes and makes suggestions about how to change IT budgeting in the public sector to support the implementation of NoLP. In the conclusion chapter there is a summary of the study and its main results.

2. Literature review

The author of the study was unable to find comprehensive previous studies about the topic of IT legacy in governments. Rather, the researcher found previous studies that investigated different angles of IT legacy related issues like **maintenance cost** and **cyber security**. Majority of the previous legacy related studies were conducted with private sector samples.

Maintenance cost of legacy systems

Taking into account the fact that all governments are constantly struggling to keep the IT budgets under control (Moore, 2013), reasonable balance between maintenance cost and innovation projects cost is crucial. There are always changes in processes and regulations that the governments have to comply with and need to change the IT systems accordingly. Thus unreasonable increase of maintenance cost is one of the influencers that pushes towards wiping off old IT systems and rebuilding them from scratch. One of the first steps though is to have an overview of what is the proportion of the maintenance cost. Differentiating maintenance cost from development costs[7] can be tricky and the line between them is often blurred due to lacking or conflicting definitions (Buchmann, et al., 2011). Buchmann, et al. (2011) point out lack of standardized contracts that should create a framework for differentiation, as one of the reasons. So, in order to adequately estimate the maintenance costs, clear differentiation methods are needed. Buchmann, et al. (2011) highlight following main drivers of maintenance costs:

1) size of the application;
2) number of components (e.g. modules, databases, programming languages, frameworks);
3) interfaces to surrounding systems;
4) changes (frequency and intensity);
5) developers experience;
6) code quality.

They also state that this categorization is a good first step in forecast the maintenance costs, but there is no generalized approach available to identify those factors. As one of the results of their study Buchmann, et al. (2011) conclude that the average number of reported software defects and

[7] Development costs: the cost of adding new functionalities to the IT system.

the number of programming languages in use are a good indicators of the complexity and maintenance costs.

There are many studies to prove that maintaining legacy systems is extremely costly and that maintenance cost proportion can be up to 90% of the yearly costs (Eastwood, 1993; Erlikh, 2000; Seacord et al, 2003). In case maintenance costs proportion is hidden, there is a lack of clear understanding of how much is paid for maintenance and how much is spent on implementing new innovative ideas. This can be one of the reasons why concrete steps to get rid of the outdated systems are not done at the right time. So it is one of the factors that should be investigated further to understand if it should be taken into account when deciding whether one should keep duck-taping a software solution or should a wipe off and rewriting project be considered.

Cyber security

Modern governments are becoming increasingly dependent on IT systems since automating processes with digital tools is one of the few ways of providing services to the citizens in an efficient way. But using more and more IT solutions to provide services also increases the risks related to using cyber tools and these need to be kept in mind in order to keep the trust towards digital services.

The world is changing rapidly, new emerging technologies also impact cyber security, introducing new vulnerabilities. Lewis (2002) has named the situation where there are new vulnerabilities related to digital dependency of critical services the *electronic Achilles' heel*, suggesting that adopting new technologies and not being able to think through all possible new weaknesses is a reality that we need to acknowledge and constantly deal with.

Based on State Information System Authority 2015 report (State Information System Authority, 2015), the number of registered cyber security incidence are increasing year by year. The director general of Estonian State Information Authority emphasises that we also have to keep in mind that in our region, we have many politically motivated cyber-attacks (Peterkop, 2015). Making it even more important to make sure our critical it systems are well protected.

Figure 2. Number of cybersecurity incidents registered by the Estonian State Information Systems Authority

The risk factors that need to be taken into account in the cyber room today are completely different of those we had to consider 20, or even 10 years ago (Linden, 2007). The technologies have changed (Anon., 2014; Tsang & Smith 2008), new methods of cyber-attacks have emerged, today huge technical capacities are available at rather low cost, the web is full of tutorials teaching how to attack different IT systems and due to that, people with limited technical skills can cause lot of trouble (Bednarz, 2004). Also, conducting a cyberattack is in many cases much cheaper than attack in a physical world (Lewis, 2002).

One of the examples is that in 1990 the networks of U.S. Department of Defence were penetrated. The initial suspicion was that the attacks were organized by potential opponents at the time (Iraq, China). They were also suspecting that these attacks were acts of war. In reality, they were organised by two high school students in California, who were basically recreational hackers that just did it to fight off boredom (Lewis, 2002).

At the same time, teams of high-skilled hackers are employed by terrorists and criminal organizations, to break important information systems (Tsang and Smith, 2008). Also cyber-attacks that are very likely state-sponsored are becoming a reality. Often attacks in cyber world are part of a hybrid war[8] scenarios. Examples here are the attacks against U.S. military computer networks during operations in Kosovo (Lewis, 2002) or the attacks against Estonia in 2007 and Georgia in 2008 (Beidleman, 2009).

[8] Hybrid war - a type of warfare that involves conventional, unconventional, regular, irregular, and information and cyber warfare (Van Puyvelde, n.d.).

Another way to use cyber world for malicious causes is virtual espionage. In a situation where majority of data is available in electronic format, this poses an additional risk that the victim most probably is not even aware of. In that case it is not the perpetrators interest to cause direct damage by listening in, but rather to collect information he can use against the victim when the time is right (Lewis, 2002).

This has created a situation where the expectations towards information system resilience have radically changed. Cyber threat of today is completely different from what we had to consider 10 or more years ago. Today cyberspace has become one additional setting for war on par with land, sea, air, and space (Beidleman, 2009). The National Strategy to Secure Cyberspace, put together by Department of Homeland Security of United States of America states that "Cyberspace is our nervous system – the control system of our country" (Department of Homeland Security, 2003). To emphasize the importance of cybersecurity – the strategy paper states that because of the fact that cyber-attacks can potentially cause serious damage to national security of the country, these attempts must be treated as an act of war.

In many cases it is almost impossible or extremely expensive to increase the resilience of outdated systems (e.g. the support of basic platform disappears etc.). For example Tsang and Smith (2008) state that many serial-based SCADA[9] systems that are still in operation today were designed decades ago with the focus on availability and personnel safety not IT system security, and are thus now vulnerable to malicious attacks like sniffing and tampering. Years ago this was not a problem because SCADA systems were often operated in dedicated, proprietary networks, but these systems are more and more opened up to internet protocols to exchange data with central information systems that help to make fast business decisions (Lewis, 2002).

One of the examples is the legislative changes in EU energy market. All EU member states had to adopt new regulations to ensure open market and fair competition in energy production and sales (Elering, 2012). Estonia has also adopted that regulation and it has caused a situation where many new business requirements need to be met. The energy price is recalculated almost in real-time and energy production management has to be organised in a very different way to be in sync with the demand for energy and the pricing situation. This in turn has led to a need to get operative feedback from energy production systems – systems that were not created taking these new requirements into account. Systems that in some cases are outdated and need to be kept offline to minimize the risks.

[9] SCADA – Supervisory Control and Data Acquisition systems are real-time process control systems that monitor and control local or geographically remote devices (Tsang and Smith, 2008).

To conclude – there are many aspects of cyber security that need to be taken into account when deciding whether to continue operating an old information system or it is reasonable to initiate rewrite projects. Thus, cybersecurity risks were included as one of the aspect to investigate further during current research project.

3. Related models and concepts

Because of limited previous scientific studies with the focus on issues related to legacy software in governments, to open the topic, the researcher also looked into other related factors and models that need to be kept in mind when dealing with government IT systems. These models and factors were chosen based on the pre-study conducted under the research project. Explaining these aspects help to better understand the general framework that surrounds the IT systems. Since no IT system is an end in itself, understanding the dynamics surrounding it help to better understand the issues related to IT systems turning into legacy. Keeping this principle in mind, the author found it relevant to add explanations about those other aspects and models in addition to the literature review.

Following models and aspects emerged during the pre-study phase (overview of the pre-study process is provided in the next chapter): the **lifecycle management of IT hardware and standard software** as a relevant examples to learn from; **the nature of innovation process** and its connection to legacy; the **impact of emerging technologies**; **changes in the ecosystem**; and the changes brought along with the **concept of open source**.

Lifecycle management of IT hardware

Lifecycle management of IT hardware is relevant to the current study topic for many reasons. On one hand it can be taken as an example of lifecycle management process. On the other hand, the changes in the hardware are also one of the key enablers for software innovation. At the same time they can also be the main influencers that force the software to be rewritten. E.g. when a server with certain attributes is no longer produced and the outdated software will not run on newer versions, then there is no other way but to rewrite at least part of the software to upgrade to more modern hardware.

Looking at hardware as an enabler for software innovation – new devices with enhanced functionalities open new opportunities for creating more advanced software solutions. E.g. new iPhones (since iPhone 6) have built-in fingerprint scanners that application creators can use to create secure authentication modules. Similarly cell phones sold today have much more advanced built-in cameras that can be used for face recognition or even eye retina scanning. These new functional features open up new opportunities for creating much more advanced remote persons' identification procedures and thus enable to create higher levels of trust between the user and the service provider, opening doors for higher security demanding e-services for wide range of users.

The topic of the impact of emerging technologies is covered in more details in one of the following chapter.

At the same time, new functional features of devices also influence customer expectations towards software. E.g. it is becoming increasingly common that people are accessing web solutions with devices that have very different resolutions and increasingly smart phones are used for browsing (Bosomworth, 2015). So it is expected that web solutions use responsive design and thus the web page automatically adapts to the resolution of the specific device that is used. The study (Bosomworth, 2015, Perez, 2014) also shows that users prefer to access content (e.g. social media like Facebook or LinkedIn) that they use often via apps more than web browser, which is another user behaviour pattern that the online content providers need to keep in mind.

So coming to the topic of devices lifecycle management we find that in case of IT hardware, be it the laptops, desktop machines, smart gadgets, servers, or other electronic devices, they become legacy quite fast. The world changes so rapidly, new technologies emerge and latest issued devices have more and more features that make life easier (Pogue, 2013). A good example is the coming of touchscreen in the late 2000s (Erickson, 2012). Just few years later, almost everybody has a smart phone and other touchscreen enabled devices like tablets and laptops in addition. It is considered unreasonable to use a mobile phone with buttons.

Average lifespan of a laptop used in daily work is 2-3 years, so majority of modern organisations tend to exchange these devices in at least every 3 years. It is not expected it to be a good working device for a longer period. Other hardware devices also tend to have a reasonable life-expectancies in place (Garretson, 2010):

Device	**Average life cycle**
Cell phones	2 years
Laptop PC	3 years
Desktop PC	4 years
Server	5 years
Networking gear	5 years
Monitor	8 years

Table 1. Reasonable life-expectancy of IT hardware (Garretson, 2010).

In Estonian government, Centre of Registers and Information Systems is responsible for conducting central procurements of IT devices for the government. The procurements are planned keeping in mind that the reasonable lifespan for laptop is 3 years and for PC its 4 years (Sihvart, 2015).

There are many factors that influence the decision making process when it comes to replacing devices. Manufacturers add new functionalities and features incrementally to keep the customers hungry, also, when it comes to devices that are in personal use, there is an important psychological effect. People tend to like having innovative devices and gadgets (Pogue, 2013) and as long as they are available with reasonable prices, there is a constant drive to upgrade to a better version. A study done by Recon Analytics (Entner, 2011) showed that Americans change their mobile phones on average in every 21 months. At the same time it is common knowledge that the quality of electronic devices provided by an organisation to its employees is considered to be part of the motivation package and not making sure that the tools are up to date will reflect on the attractiveness of the employer. But it is not only a reputation issue – outdated devices can cause lower productivity, downtime, and elevated levels of user misery and thus can influence the general productivity of the employees that in turn also will have a financial effect in bottom line of a company (Garretson, 2010).

So, to conclude, it can be stated that the **rapid changing of IT hardware is a daily reality that forces the software creators to be constantly ready to adopt the new technological innovation and adapt to changes in the user expectations and behaviours**. Keeping these factors in mind, the **lifecycle management of IT hardware can also be taken on board as one of the examples** in putting together similar approach for government software lifecycle management rules, because just as with hardware, **similar drivers are influencing the need to change the software**. E.g. even though it is possible to add storage power to the existing old desktop computer or connect a better web camera with an USB cable to it, it is not done. Instead the devices are changed in every 2-3 years because there are many other benefits that can be harvested by using new, better equipped device, instead of constantly "duck-taping" the old one.

Lifecycle management of standard software

Another relevant example to look into is the lifecycle management of standard software products. Even though one might argue that the big corporations are just greedy organisations who stop supporting the older versions of products just to earn more money by selling customers newer versions, there is much more evidence to support the argument that it is not quite so.

Looking at the lifecycle of standard software products, we discover that often the products lose the official support in around 10 years' time and by the time they lose the support, there are newer versions of those software's already out that have much better functionalities available for the end-users. E.g. Microsoft (hereinafter: MS) recently announced stopping the official support for Windows XP (an operating system that was 12 years old at the time). The reasoning by MS was

that the operation system is too old (has become legacy) and thus, is not in adequate sync with new technological realities – memory and storage are cheaper, processing speeds are faster, and displays have higher-quality (even touch screens). So it was just unreasonable to continue to add incremental changes to the system that was created when **the technological realities were very different from where we are today**. This is one of the reasons why Microsoft's standard support time for products is around 10 years (Keizer, 2012, Microsoft, 2014a), for operating systems the period is often even shorter (Microsoft, 2014b).

There are many other similar examples when it comes to standard software. For example the database software by Oracle typically does not have longer standard support period than 3-6 years and extended support typically ends 5-8 years after the release of a product version (Oracle, n.d.).

Release	**GA date**	**Premier Support ends (years after release)**	**Extended Support ends (years after release)**
8.1.7	Sep 2000	Dec 2004 (4y)	Dec 2006 (6y)
9.2	Jul 2002	Jul 2007 (5y)	Jul 2010 (8y)
10.1	Jan 2004	Jan 2009 (5y)	Jan 2012 (8y)
10.2	Jul 2005	Jul 2010 (5y)	Jul 2013 (8y)
11.1	Aug 2007	Aug 2012 (5y)	Aug 2015 (5y)
11.2	Sep 2009	Jan 2015 (6y)	Dec 2020 (5y)
Enterprise edition 12.1	Jun 2013	Jul 2018 (5y)	Jul 2021 (8y)
Standard Edition (SE) 12.1	Jun 2013	Aug 2016 (3y)	Not Available
Standard Edition One (SE1) 12.1	Jun 2013	Aug 2016 (3y)	Not Available
Standard Edition 2 (SE2) 12.1	Sep 2015	Jul 2018 (3y)	Jul 2021 (6y)

Table 2. Support periods of Oracle database software.

With government software we see a different picture compared to hardware or standard software lifecycle management. Based on the authors' experience as a Estonian government IT policy maker, and having had discussions with other countries government CIO's and policy makers, the author has discovered that many of them are facing difficult decisions about what is the way forward for government IT systems? How long should they keep the systems up and running by using "duct tape" (making small adjustments just to keep the old system alive) or when is the time to wipe the old system off and start again from scratch? What should they take into account when making the decision of fixing vs rewriting etc. So looking into existing models of lifecycle management of IT hardware and standard software as examples and investigating the reasoning

behind rewrite decisions provides many lessons that can be incorporated into the NoLP for governments.

Legacy as an innovation blocker

In order to keep up with time, organisations need to constantly review and update their core business processes. Typically digitalisation of processes starts from trying to automate the core processes. After the main business processes have been digitised, the focus shifts to other, less relevant business processes. Often, when there is no external reason to revisit the core processes, there is a threat, that the optimisation of main functions will lag behind. Rewriting these core systems helps to draw focus back to the main processes and pushes organisation to redesign and innovate again. In contrast, letting core IT systems turn into legacy, will fossilize the main processes of the organisation.

Another important influencer for holding on to the outdated systems is the legacy of the mind-set. Meaning that people who are used to the "as is" processes, might have difficulties to start from *tabula rasa* again and find ways to make processes more efficient. Thus, it is not only the legacy of the old system holding innovation back, but it is also strongly connected to the train of thought that "this is how it has always been therefore it's the best way to continue". In the worst case scenario, when rewrite projects are conducted, the business processes tend to be just like they were in the previous version and not because there was no room for innovation, but because of the mind-set legacy of the team responsible for redesigning processes. Adding new team members to the process redesign team helps to solve that issue.

The world around us is constantly changing and the ability to adapt and even predict these changes is crucial. Christensen (1997) introduces a term *innovator dilemma*, suggesting that in case companies do business based on their current needs and are not pursuing the adoption of new technologies and ways to improve their business to meet the future needs of the customers, they fail to be successful in the future and thus, lose their business advantages. He argues that *disruptive innovation* is needed, and one should not drop innovative ideas just because the customers cannot use those innovative product yet. So in order to be successful in the future, one cannot set a target to keep the status quo, because it actually has built-in tendency to start declining in quality. To be successful, one should every now and then critically review the business model and ask themselves the question – "is the world going to change in the future and how can I be the first adopter of that innovation?" (Christensen, 1997).

Estonia has been considered to be one of the leading e-governments in the world by many international e-government ratings.

- United Nation E-government survey 2014 rated Estonia on 15th place among 193 studied countries (United Nations, 2014);
- IAC International e-Government ranking Survey conducted by Waseda University rated Estonia on 8th place among 63 countries (Waseda University, 2015);
- Among EU countries, Estonia hold a second place in the Digital Public Services ranking. The ranking states that Estonia has been at the forefront of online public services and Estonia remains the leader in the availability of pre-filled online forms (European Commission, 2015a).

Being a successful e-government has become a part of our country's' identity. The e-government story is being used to promote Estonia as an innovative country with smart and open-minded people and to open doors in order to promote cross border economic relations for other sectors. We have not created the e-government solutions to gain more popularity as a country. We did it because of necessity to automate and be able to serve our citizens and companies. The positive attention has been a very good side-effect. Today we cannot forget that keeping the e-government story alive has become important from country's reputation perspective. We need to keep the image of an innovator and come up with new ideas to impress others if we want to continue using these stories in the international arena, be it e-residency, click-free tax-declarations, bring your own device e-cabinet solutions, digital court systems etc. These stories only work for our favour if we ourselves have really benefited from implementing these ideas and we are able to prove it. But to be able to constantly innovate, we have to actively deal with legacy as it gives us the opportunity to start from tabula rasa again and again.

Innovation is an incremental process by nature – meaning that you can improve processes only to certain amount at a time. Getting rid of legacy forces to rethink processes and enables to take next steps towards more efficiency. So one can argue that the more often you wipe off systems and rebuild, the faster you are able to innovate. Thus, having important government IT systems in place that are 20 or 30 years old is not reflecting innovation in government, but rather it is a symptom of processes not being thoroughly redesigned for a long time.

Impact of emerging technologies

As already showcased in the hardware lifecycle chapter, the technology evolves rapidly. Many widespread technologies of today did not exist 10 years ago. For example first touchscreen cell

phone was introduced in 2004, but it gained a significant market share in 2007 (Anon., 2015). Laptops with touchscreens are becoming more and more popular. Cloud based infrastructure has changed the infrastructure market, and voice recognition and language syntax analysis technologies have just recently reached the maturity levels that enable them to be used in mainstream software. Be it controlling your cell phone over voice, inserting search keywords to google search, or something much more complex. For example Skype recently launched their online translation tool that enables people to have a live conversation in different languages so that the skype environment provides simultaneous translation (Skype, 2015). It makes one wonder, that could it be that simultaneous translation service conducted by people is a dying trade in the near future because computers will take over?

IT systems that were created 10 or more years ago were not developed keeping in mind the benefits that came along with these disruptive technologies. E.g. Estonian hospital information systems were developed almost ten years ago (Arengufond, n.d.). And even though Estonian hospitals IT systems are considered to be one of the best and our hospitals have adapted eHealth solutions the most among Europe countries (European Commission, 2012), we know that wiping them off and rebuilding would make it possible to take advantage of new technological realities. For example touch screens would make inserting the data much more efficient. Also voice recognition technologies can be used to make the job of medical personnel much more fluent. Imagine a family doctor performing an infants' health check and inserting data to the system using his/ her voice – saying commands like "insert, baby weight, 4 kilos and 200 grams", instead of going back and forth between the health check table and desk with the computer.

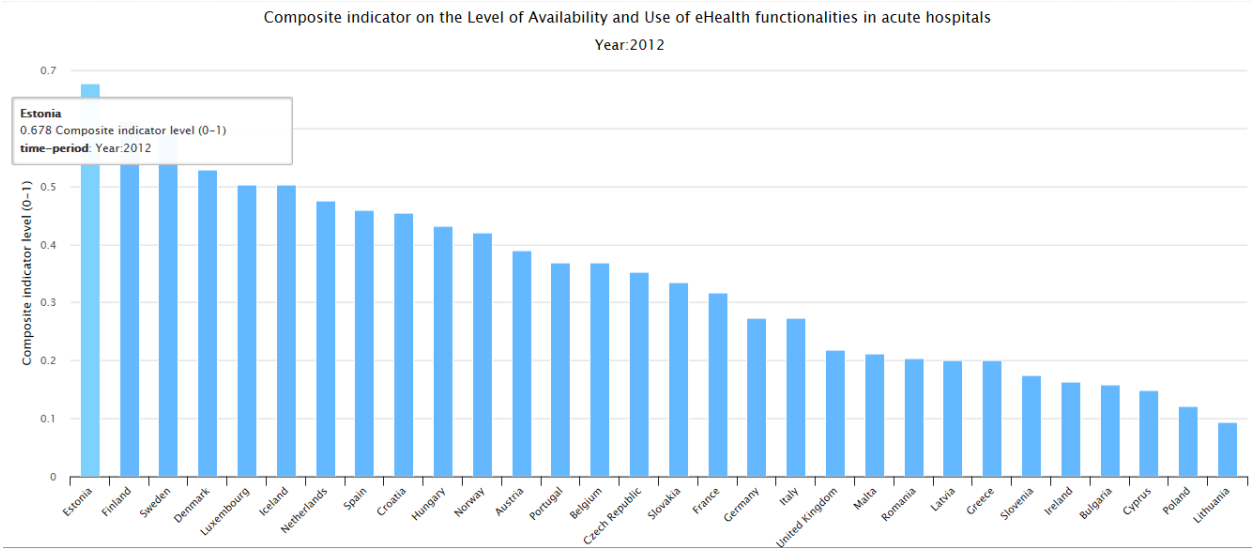

Figure 3. Usage of eHealth in hospitals of European countries (European Commission, 2012).

Today storage is cheaper than ever before. Connectivity is better and internet availability and speed are not even comparable to a situation just 5 years ago. This creates new realities for system development. Using video as an evidence in police traffic control was unthinkable 10 years ago because of the high cost of storage. Now the situation is totally different. So if we would recreate the IT systems used in police cars, we could harvest the benefit of technological developments and start using video as evidence – making it possible to process violations of traffic regulations much faster and efficient. Imagine video camera being used to record the violation situation and get agreement from a traffic violator, instead of protocolling everything on paper. If there is no dispute, traffic ticket can be issued and paid within 5-10 minutes on the spot, instead of spending 20-30 minutes on writing the description of the situation in the paper forms as it is still done today. The impact of such a change is enormous. With the current situation, one police unit is capable of processing at least 2-3 times less violators than it would be able to process if they would have IT solutions in place that would be in sync with the technological realities of today. This in turn would have a huge impact on the traffic safety.

Of course implementing these kind of new ideas need changing regulations as well, but in most cases that would not be an obstacle. Similar changes have been done to digitise Estonian court systems and use digital court case files as legally binding ones, making it possible to share latest and updated version of court cases with multiple parties at the same time. Whereas in case of paper-based court files lot of copying and manual work was involved. Court assistants needed to be present when representatives of parties needed to work with the main case files, copying was expensive etc. Going digital enables to use the same files in various court levels as well. These changes have made it possible to speed up court proceedings and lower the administration costs of courts as well as parties involved, because of less manual work and reduction of using paper[10].

The impact of emerging technologies needs to be taken into account when deciding, what is the way forward with one or the other IT system. It should not be just a matter of what kind of changes should be done to the processes because of legislative changes, but also what the new technologies enable to do differently and how could these benefits be harvested in making government services better and more efficient.

[10] Information about the impact of digital court files is available to the Author through the Estonian government ICT investment management process.

Changes in the digital ecosystem

The benefits of emerging technologies are often evident and hard to dismiss, whereas many changes that have happened in the digital ecosystem can be rather latent and need efforts to figure out what has changed and how those changes could be exploited to create better services or should be considered as new risks or requirements that need to be fulfilled. For instance, one of the opportunities to benefit from might be reusing data that is gathered somewhere else and thus reducing needed input from the citizens to provide government services. A good example here is the employees registry implemented by Estonian Tax and Customs Board in 2015. The solution was designed in a way that automated the information flow to other government authorities. So every time a new employee is hired and registered in the employee register, the information is also automatically pushed to other relevant authorities (e.g. social insurance fund etc.). Similarly, if the birth of a child is registered in a hospital IT system and that system has interface to population registry, the personal code to that child can be issued automatically. That was not possible before the digitization of hospitals.

More and more information is available in digital format. The amount of open data and sharing data over secure information exchange layer X-Road has been increasing in time (Information System Authority, 2013).

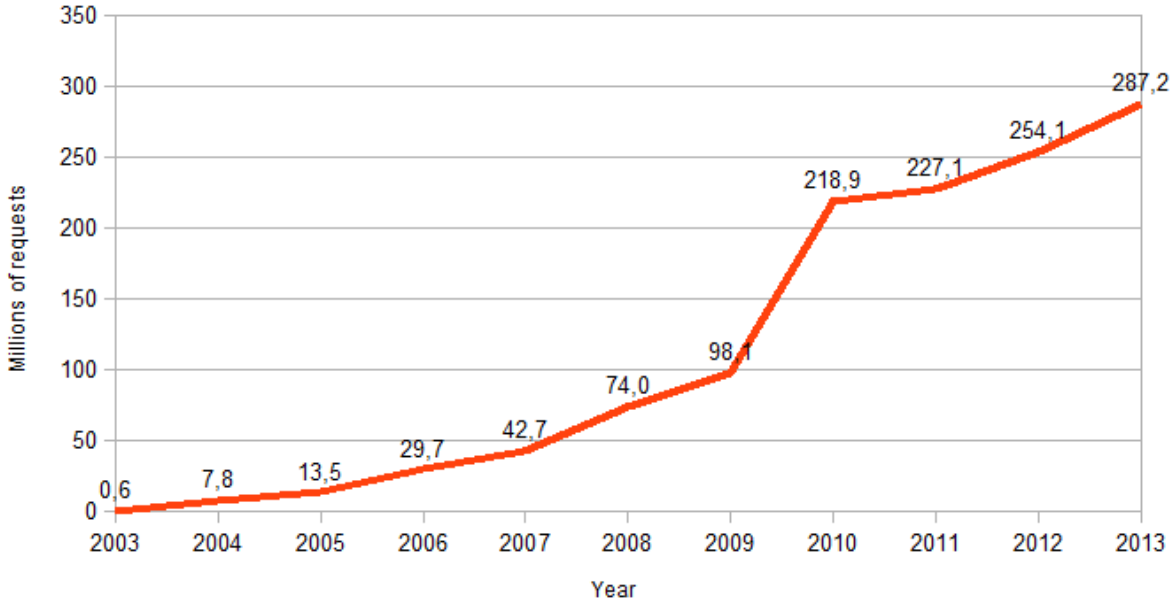

Figure 4. Yearly number of X-Road queries.

Smart reuse of data enables to create less burdensome services. For example road administration changed the logic of applying for the drivers licence. Instead of making people take new

photographs in the automated photo booths in the road administration offices, before filing the drivers' license application, they started reusing digital photographs stored by the Police and Customs Board. Pictures that were collected for issuing identity documents. Reusing the photos existing in another authorities' database enabled to take one time-consuming step out of the process for the end user. At the same time it also helped to reduce the costs of the road administration – there is no need to have many expensive photo booths in the offices or separate photo database in the road administration.

The reuse should not stop there. The road administration has created well working e-services to apply for car licenses, but there are many similar other processes. Take the process for applying for license to steer a ship. A process that is governed by another authority in government. Estonian waterways authority is running an outdated system for issuing ship steering licenses, but instead of building a new system, they are considering moving their service to the road administration platform, because the functional requirements are very similar. This option was not on the table 10 years ago when the first system was created.

Combining different datasets makes it possible to ask successively less data from the customers or citizens and provide services that require less interaction from the end users, making it possible to move towards fully automated, seamless services. Technologically we are already able to make tax declarations fully automatic, so that in more than 90% of cases no interaction is needed from the citizen and all of the calculations are done correctly using automated data flows. The traffic load on different roads could easily be monitored using depersonalized data from telecom companies, instead of measuring the number of cars with old-fashioned rubber bands as it is still done today (Tiru, 2015).

There could also be changes happening in the ecosystem that might bring along new risks or new requirements that have to be complied to. For example it has to be considered that technological capabilities are constantly developing, the calculation powers of computers are constantly growing. Thus, many security measures that have worked for years, might not work anymore in the future. A good example here is the development of cryptography algorithms. Today, cryptographic measures based on SHA-1 signatures are still widely used. But thanks to the cloud computing services, accruing enough computing power to solve complex calculation tasks (e.g. cracking SHA-1 based cryptography) is becoming cheaper every year. Today Microsoft, Google and Mozilla have all announced that their browsers will stop supporting SHA-1 based certificates by 2017. They also recommend that SHA-1 based certificates should not be issued after 2015 (Stevens, et al., 2015).

New requirements can also be related to the fact that bigger amounts of information need to be processed. E.g. in the energy sector one of the recent developments has been the adoption of smart meters that can be read from the distance. So now, instead of having information about every separate location of energy consumption once a month, this data can be read almost in real time and used for smarter decisions in energy production, price offerings to the customers etc. It was impossible to adapt all of the old IT systems to such an increase in the amount of data to be processed (Roos, 2015).

So again, the processes should be regularly reviewed keeping in mind the changes that will happen or have already happened in the surrounding environment.

Impact of Open Source

Open source software is becoming more popular, replacing proprietary solutions and enabling to get rid of high licence fees. A good example here is the Android mobile platform that has become the most popular operating system worldwide. Gartner study shows that Android operating system runs in 82% of all the mobile phones sold globally (Gartner, 2015a).

Operating system	2Q 2015 Units	2Q 2015 Market Share (%)
Android	271 010 000	82,2
iOS	48 086 000	14,6
Windows	8 198 000	2,5
BlackBerry	1 153 000	0,3
Others	1 229 000	0,4

Table 3. Worldwide smartphone sales to end users by operating system in Q2 2015 (Gartner, 2015a)

There are few factors that have made this triumph possible, the most important one has been the openness to enable many different manufacturers to work out products using the operating system – Samsung, HTC and Sony just to name a few. This has resulted in a diversity of different products to choose from – and thus responding to a wider range of customers' expectations regarding functionality and acceptable price points (Triggs, 2013). Triggs (2013) also claims that the competition created by openness has enhanced the innovation – every manufacturer is trying to create products that go above and beyond the basic Android experience. E.g. Samsung has invested a lot to provide enhanced software functionalities for exercise tracking, multitasking, additional camera settings, whilst HTC has invested heavily into sound systems etc. So having an open platform has brought along diversity of products and innovation is not only on the shoulders of one company.

Thanks to the openness of Android platform, its' popularity has increased significantly over the years as seen in the following table (Gartner, 2015b):

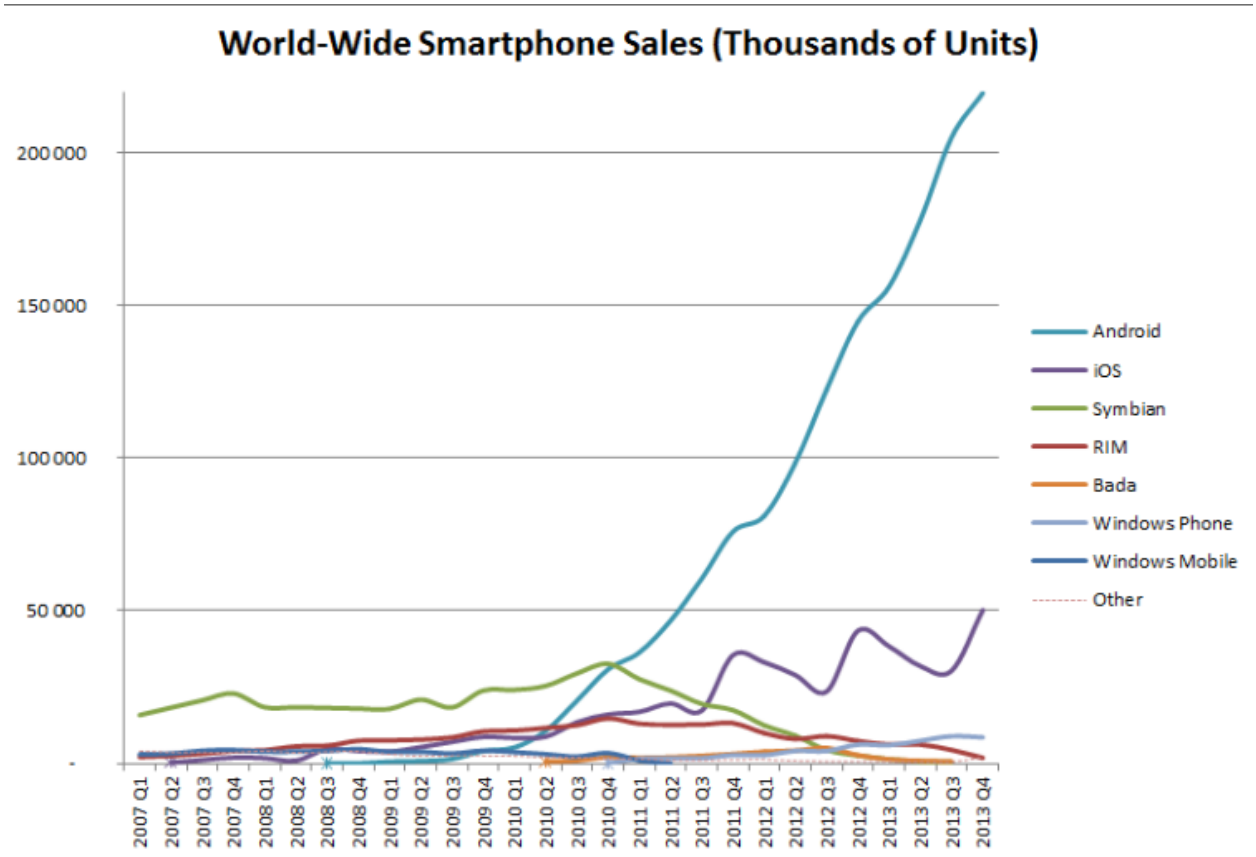

Figure 5. The popularity trends of mobile operating systems over time

The trend of open source is slowly emerging to the public sector in Estonia. Estonian ID-card software was published in GitHub environment in 2014 (Certification centre, 2014). The recommendations put together by public-private joint working group also recommend using open source licence models for procuring software for government and Ministry of Economic Affairs and Communications recommends using these guidelines when procuring software for government (Ministry of Economic Affairs and Communications, 2015).

Using open source models enables to share software bought by one authority to be used for others as well. One good example here is the alfresco based document management system initially developed for Ministry of Interior and Ministry of Justice. Now it is also used for many local governments and also talking to the IT manager of Ministry of Economic Affairs and Communications, he admits that when he will initiate the project to change the outdated GoPro based document management system, he will most probably plan to migrate to the Alfresco based open source solution (Kaiklem, 2015). The main reasons are that it is well working for others, there are no licence fees and the development cost for the platform are shared.

The movement of open source has also brought along many other solutions that are replacing the previous, traditionally license fee based software.

4. Research methods

The topic of IT legacy is difficult to study. It is virtually impossible to use comparative research methods since there are no custom IT systems that are very similar and can be divided into many subgroups that would then be processed differently, so that the impact of those differences could later be measured. There are also many influencers that are difficult to control, and have a considerable impact on IT systems – e.g. different team members, differences in technologies etc. Important factor related to IT legacy is also the time that needs to pass in order to investigate changes. All of these factors make comparative study methods very difficult to use to study IT legacy. Also, as pointed out in the literature review, there are not too many previous studies with the focus on the legacy build-up problem in the public sector. Thus, to investigate the topic, the author found that the best way forward is to conduct a study that is based on expert opinions. In order to get high quality results, the researcher found it important that the experts involved had a high average experience in the ICT field. The results are described in more detail under the "Sample overview" sub-chapter.

Because of lack of extensive previous studies with a similar focus, a **qualitative pre-study** was conducted. The goal of the pre-study was to clarify the issues related to IT legacy, to gather input to draw up a **questionnaire for quantitative study** and also to enrich the quantitative information gathered with the questionnaires with real life examples.

Pre-study interviews with experts

As a pre-study semi-focused interviews with Estonian and foreign experts were conducted. Experts were from business and technical side, who have had experiences with IT legacy, as well as ICT policy makers responsible for IT management in the government. Interviews were conducted with more than 20 experts (see appendix 1 for list of experts).

During the introduction of the study topic, the researcher set the focus, explaining that the goal of the study is to find out whether there is a need for policy guidelines for government and that during the interview the focus should be on important core IT systems that are mission critical for the functioning of the organisation.

During the interviews the goal was to determine following aspects:

- how do experts define IT legacy and what are the main symptoms of it;

- do the experts see the build-up of IT legacy as a problem (for their organisation, for government);
- what is the reasonable lifespan of critical IT systems;
- do they have policy guidelines in place in their organisation to avoid the legacy build-up or are they aware of good guidelines that could be implemented for that purpose;
- what is the size of government IT budget (in case of foreign experts);
- what is the proportion of maintenance costs;
- what have been the lessons learned when dealing with IT legacy;
- have software rewrite projects mostly paid off taking into account the overall costs related to the business processes;
- is there a need for No Legacy Policy for government in their opinion;
- how would a rule that all important IT systems have to be rewritten in at least every 13 years impact their organisations' IT budget etc.

The main goal of the interviews was to clarify the issues regarding IT legacy as an input to compile the questionnaires for the quantitative study, but also to gather ideas about the content and implementation mechanisms of the No Legacy Policy for governments.

Quantitative study questionnaires for experts

The goal of the quantitative study phase was to get a deeper, numbers based understanding of legacy related problems and to clarify which problems are most prevailing or critical.

The quantitative study included two questionnaires. The main instrument for the quantitative study was a questionnaire to gather input from Estonian experts. But as Estonian e-government is still rather young, we might have limited experience with IT systems lifecycle management. Estonia has been building e-government solutions since regaining the independence in 1991, thus now having slightly over 20 years of experience and the build-up of IT legacy is a rather new problem for Estonian government. But based on interviews done during the pre-study with foreign experts it has become evident that in Estonia, government solutions are created somewhat differently than in other countries, using more tailor made software, instead of standard products, and making due with smaller budgets than other countries with successful e-government solutions. E.g. the government IT budget of Finland (including personnel, maintenance and development costs) is 1.6 billion euros (Karjalainen, 2015), IT budget of Singapore is around 2 billion Singapore dollars

(Poh, 2015), and the IT budget of the UK is around 20 billion pounds (Maxwell, 2013), whereas Estonian government IT budget is around 50 million euros.

Thus, another questionnaire to involve foreign experts with longer and more extensive experience with government IT solutions, was compiled.

Overview of questionnaires

Questionnaire for Estonian experts included 5 questions about the respondents' background and 15 substantive questions about the issues related to IT legacy.

Questionnaire for foreign countries experts included all the same questions as the previously mentioned Estonian questionnaire, but also incorporated 6 additional questions to gather background data about each specific country – e.g. name of the country, organisation that the respondent works for and his role there, but also question about the size of the government IT budget and the proportion of the maintenance cost compared to investments into new developments.

Questionnaires included many open-ended questions to get additional qualitative data that is used as relevant background information in planning the next implementation steps for Estonian NoLP principles. Thus, not all of the open ended questions are analysed in the framework of current theses.

See detailed overview of the questionnaires as appendix 2, questionnaire for Estonian experts as appendix 3 and questionnaire for foreign experts as appendix 4.

Questionnaire for Estonian experts was distributed to Estonian government IT managers' network (about 50+ members), posted on researchers Facebook page, and sent to personal contact network of IT architects, analyst, project managers and technological evangelists with extensive experience in dealing with software, including experience with IT legacy.

Questionnaire for foreign experts was distributed to EU government CIOs, OECD e-leaders[11], and ICA[12] networks. The link to the study was also published during many different presentations of international conferences by the researcher and by Estonian government CIO Taavi Kotka.

[11] OECD e-leaders network information is available at: http://www.oecd.org/governance/eleaders/
[12] ICA – International Council for IT in Government Administrations. Non-profit organisation with the goal of informal exchange of ideas, knowledge and experiences on management and the use of Information and Communications Technologies (ICT) in central government administration.

Document analysis

All materials that were referenced in the theses are included in the list of bibliography. Materials used include previously conducted scientific study reports and articles, studies conducted by Estonian State Information System Authority, relevant publications in different IT, tech and management web publications like Computerworld, IEEE, Gartner, Forbes, the Guardian, Microsoft etc., publications from different international bodies like OECD, EU etc., also legacy related materials gathered from experts that were interviewed or who filled in the questionnaire.

Participatory action research

The concept of NoLP was initiated by Estonian government CIO Taavi Kotka. Seeing the problems that were risen in the Estonian government ICT investment management processes, it became evident that there is a need for guidelines that public sector could use to sustainably avoid the build-up of legacy systems. The initial concept was that there should not be any important IT systems that are older than 13 years.

The author of the thesis started investigating the issue of government IT legacy in 2013 when starting to work as a head of state information systems department in the Estonian Ministry of Economic Affairs and Communications. The main focus areas of the department are ICT policy making and coordination of ICT investment management for Estonian government. The department is responsible for coordinating the ICT investment evaluation board. Every year, over 350 different investment requests are reviewed by the evaluation board, including investment needs that are related to replacing out-dated IT systems. The NoLP initial idea was introduced to the public sector in the end of 2013 and since then many steps have been taken to push government organisations to plan and initiate rewrite projects of outdated IT systems. For instance, a business case based approach has been made mandatory to get the investments to initiate projects, forcing organisations to review and recalculate their process related costs when planning IT projects. These steps have provided the author with additional knowledge about the struggles that the government faces fighting the legacy problem. Thus, this knowledge is also partly reflected in this study.

5. Results of research

In this chapter, the main results of the quantitative study are introduced. In every subchapter, the results are coupled with a short analysis of the study results. More complete analysis is presented in the following Discussion chapter.

The objective of this study is to find answers to two main questions (MQ): **how to find out which IT systems are becoming outdated in the right time** and **how to sustainably ensure that the public sector is IT legacy free?** In order to answer these questions, the study includes additionally 7 sub-questions (SQ).

The first sub-chapter gives an overview of the sample of the quantitative study, since the high level of experience of the experts involved is relevant from the study's credibility point of view.

The following three sub-chapters offer answers to the first main question of the study about how to understand in the right time, when an IT system is becoming outdated.

The second sub-chapter focuses on the questions related to **what are the main problems why IT systems need to be re-written**. To answer that question, the questionnaire included a question about what are the main problems related to legacy that emerge most often.

The third sub-chapter focuses on what are usually the **key criteria to consider a rewrite projects**. In order to find an answer, experts were asked about what are the legacy related problems that have the most critical impact in real life.

In the fourth sub-chapter there is an analysis on **whether rewrites of IT systems should sometimes be undertaken even if there are no typical legacy symptoms showing yet**.

The rest of the sub-chapters focus on the second main question about **how to get rid of legacy in the public sector**.

The fifth sub-chapter aims to answer the question of **is there a need for NoLP** in the public sector to avoid the build-up of IT legacy.

Sixth sub-chapter helps to clarify, that in case such guidelines are needed then **how NoLP should be implemented**.

Seventh sub-chapter includes analysis on **what kind of aspect NoLP should cover**, and the last sub-chapter clarifies **what kind of effect 13-year compulsory rewriting rule of mission critical IT systems would have on IT budgets** in the public sector.

Sample overview

To get an overview of the IT legacy related issues, the goal was to gather input from experts that have a wide experience in dealing with IT systems. It was important to involve experts with technical background as well as experts who are responsible for the business processes that rely on IT systems. So the questionnaire was distributed to contacts that had at least 5+ years of experience in dealing with IT systems as software architects, analysts, project managers, cyber security experts, user experience experts, project managers, IT managers, business process owners etc.

The questionnaires were filled by 72 Estonian experts, who on average had 13+ years of experience in dealing with IT systems and 23 foreign experts from 19 different countries, who on average had over 23+ years of experience in dealing with IT systems.

It was also important to have both public and private sector experiences involved since public sector software is often created in close cooperation with private sector vendors.

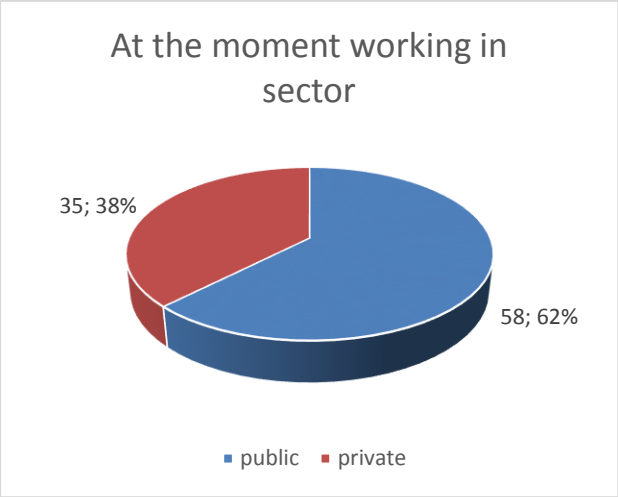

Figure 6. The frequency distribution of which sector experts' are currently working for

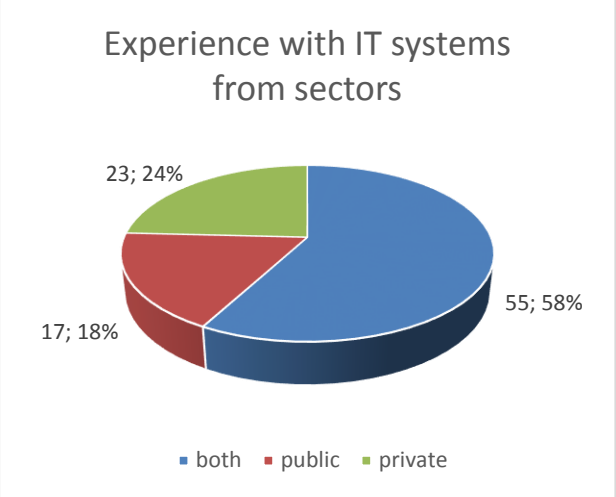

Figure 7. The frequency distribution of experts' experience in sectors

62% of respondents are currently working in the public and 38% in the private sector. 58% of experts had IT related experience from both sectors, 24% of respondents had only worked with IT systems in private and 18% only in the public sector.

The general statistics about the experts allow to claim that experts involved in the study had extensive experience in the field.

SQ1.1. What are the main reasons why IT systems should be rewritten?

The main target of the survey was to clarify, whether there is a need for No Legacy Policy – a set of guidelines that help get rid of systems that are turning into legacy at the right time. In order to achieve that goal, there is a need to clarify what are the main reasons why rewrites should be considered, instead of endlessly continuing to fix legacy system. Thus, the first question in the questionnaire focused on investigating what are the most frequent legacy related problems.

Legacy related problems that emerge most often

To clarify which IT legacy related problems are emerging most often, experts had to rate 10 predefined legacy related problems giving estimate on how often they have encountered these problems during their practical experience in dealing with IT systems. Five-point-scale was used ("(1) never" to "(5) very often/ always").

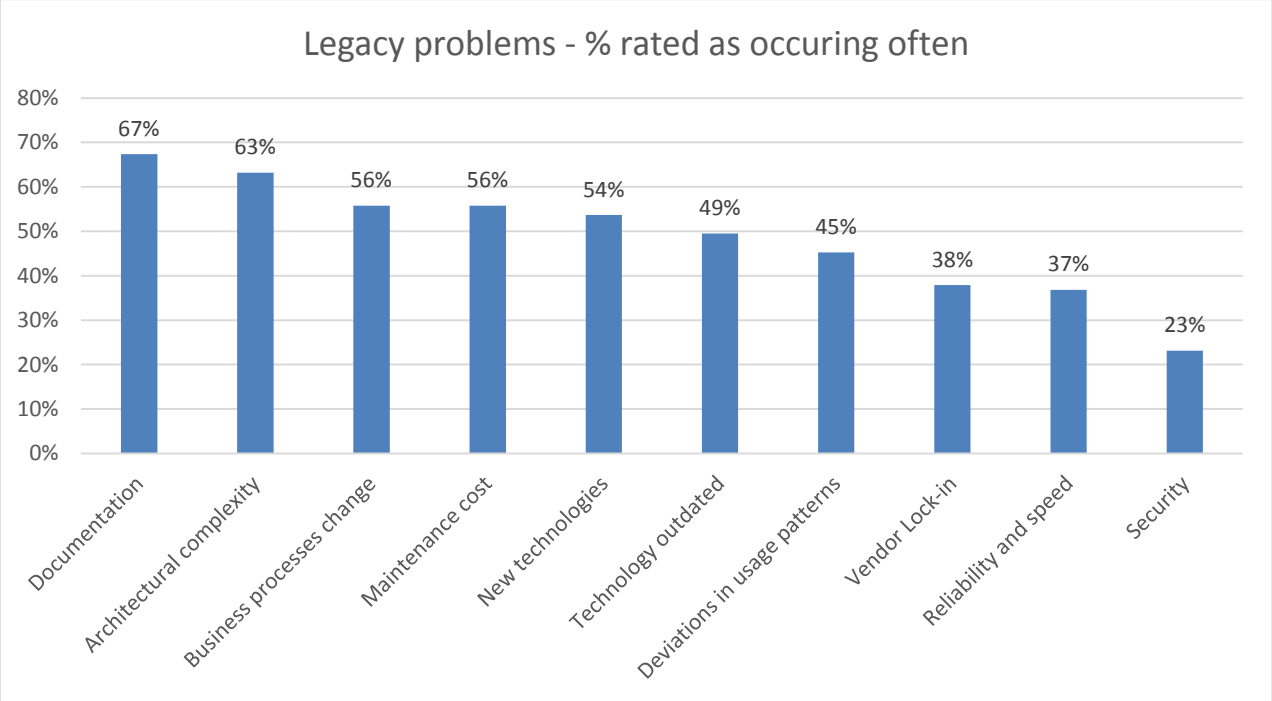

Figure 8. Legacy related problems that were rated as occuring "rather often" or "very often / always"

The symptoms that were rated as manifesting most often (rated with (4) "rather often" or (5) "very often/ always") were **missing appropriate documentation** about the system (76% experts rated is as emerging often; rated with 4 or 5), **architectural complexity** (63%), **need to change business processes**, but legacy impedes (56%), increased **administration and maintenance costs** (56%),

and inability to take advantage of **new emerging technologies**, that would make it possible to make processes more efficient (54%).

These results imply that the systems tend to become hard to understand over the years. The knowledge about the system fades as time passes and team members change. The interviews and open-ended responses added additional explanations to these dynamics, pointing out that the amount of documentation about large information systems is huge, so without exact knowledge about what is written where, it is hard to orient in the pile of all the documents even if it has been kept up to date. New members of the team have hard time finding the right documents and even if they do, then in case of systems that are couple of years old (or older), they often discover differences between the documents and the source code. So the code becomes the main source for information for the new team members, and documentation will not be updated in most cases the code is changed. That in turn becomes a reason why the documentation starts to get more and more out of sync with the system.

At one point there is no one who has a comprehensive overview of the system and its business logic. In case changes need to be implemented, there is a need to understand the as-is situation, but as software creation is a creative process, where different architects and programmers tend to have their own personal styles, the next person might not find it easy to understand what has been done before him. So many hacks are created over the years, and soon there is a situation where no one really understands the solution and thus, system's architecture is seen as too complex and hard to understand. It becomes difficult to do the needed changes because of not being able to predict the side effects that come along with each modification. So experts claimed that often the system will be labelled as legacy or hard to understand just because the new members of the team do not know why certain decisions were made about the architecture or the business logic before "their time" and figure that it would be easier to create a new software then it would be to change the existing one. This hypothesis is supported by the fact that 49% of experts rated the symptom "the IT-Platform has become technically outdated and it is causing problems" as revealing "rather often" or "very often/ always" and 37% of experts rated symptom "the reliability and responding speed of the system no longer meet user expectations" as revealing "rather often" or "very often/ always".

Thus, it can be concluded that the problems related to understanding the logic and architecture of the system and needing to change the business processes and to take advantage of emerging technologies are more relevant problems related to legacy, than the fact that the technology itself will become outdated.

On the lowest end scored the system security problems which were rated with “rather often” or “very often/ always” by 23% of experts, implying that either security problems don’t usually emerge or that they are latent by nature. The latter claim is strongly supported by the previous IT security studies as well as interviews with cyber security experts during the pre-study. The experts claim that the security wholes often tend to be found when something bad already happens, and in some cases they stay hidden even long after there has already been a security breach. E.g. when the perpetrator uses the security flaw to snoop around and steel information or wait for a better time when to reveal the vulnerability.

SQ 1.2. What are the key criteria and risks to be considered when planning a re-write project?

To investigate what are the key criteria to consider a rewrite project, it is important to understand what kind of legacy problems are considered most critical in terms of impact.

So in next question experts had to sort 10 predefined legacy problems based on their criticality in descending order starting with the symptoms that have the most critical impact based on their practical experience.

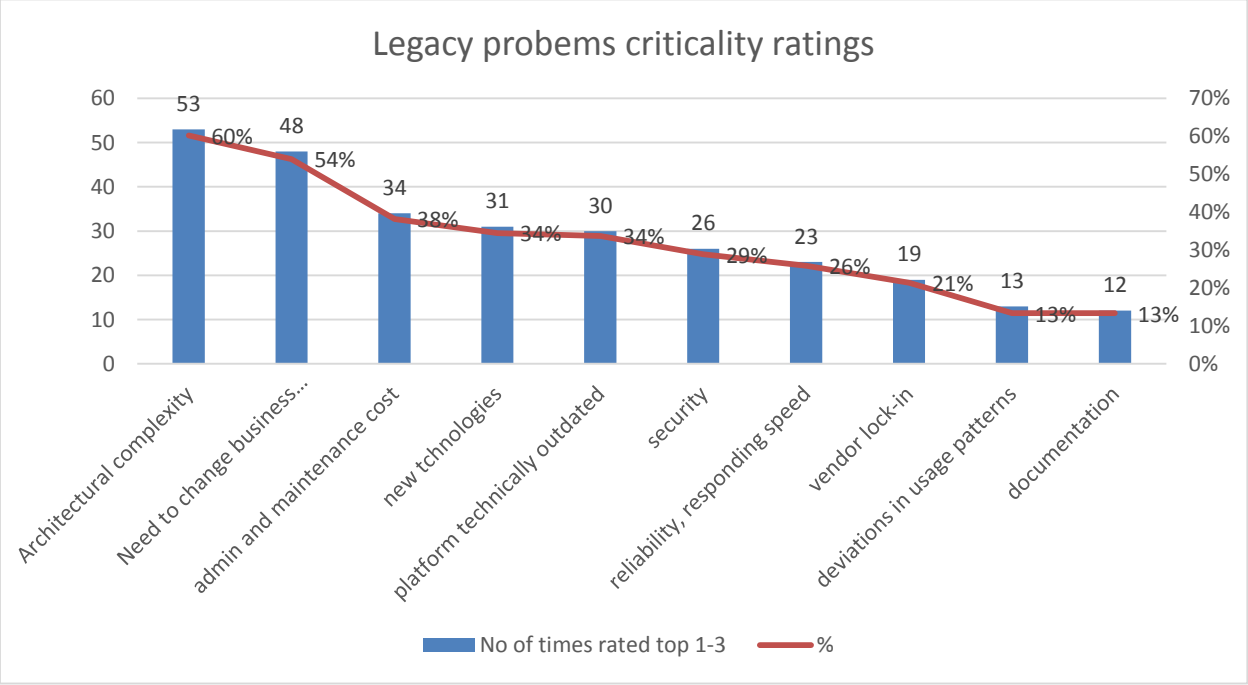

Figure 9. Legacy related problems criticality ratings – how many times each symptom was rated among top-3 most critical problems.

Architectural complexity was rated as most critical issue that is related to IT legacy (60% of respondents rated it as top 1 to top 3 most critical problems), followed by need to **change the business process** (54% rated as top 1-3), increase of **administration and maintenance costs**

(38% rated as top 1-3). Approximately one third of respondents found that the problem of not being able to take advantage of **new emerging technologies** because of legacy and platform being **technologically outdated** were critical problems (34% rated both top 1-3 most critical problems).

Problems with **security** (29%), **reliability and responding speed** of the system (26%), **vendor lock-in** (21%), **deviations in usage patterns** (13%) and lacking appropriate **documentation** about the system (13%) were rated as most critical problems (top 1-3) by less than one third of the respondents.

So the problem of not having appropriate documentation is not a critical problem in itself, and even though it emerges often, it does not have a critical impact on its own.

These responses illustrate again that the systems' architecture gets complex over time, making it hard to understand it and at the same time there is a constant need to change processes, but over time legacy starts to impede these changes. Without further investigation it is difficult to understand the main causes of the architectural complexity problem. Is it more related to the fact that systems objectively get too complex – too many layers of changes are implemented over the years, too many additional modules are developed etc., or is the perception of complexity strongly related to the fact that the team members change and thus no one really understand the system anymore and that is why the architecture is perceived as being too complicated. There is one additional factor that may influence the situation. It is the fact that there is a huge lack of IT personnel on the market. That lack of IT professionals has been a problem for Estonian market for many years and the studies prognosticate that it will be a problem for many years to come (Praxis, 2013). Same goes for EU market where the need is to get additional 825 000 specialist by year 2020 (European Commission, 2015b). Experts with experience in software companies know well that it is a common practice that the best architects are usually involved in the creation of software, and since there is a constant lack of knowledgeable resources, they tend to be faded out of the teams once systems go from active development to maintenance phase. Leaving less capable team members there to do the smaller changes to the system. So one can argue that since the IT systems tend to fall in to the hands of less capable team members once they go live, the quality and simplicity of the architecture may start declining from that point on. These different hypotheses about the architectural complexity problems should be studied further in future research projects.

The answers to the legacy problems criticality question also confirm that the maintenance costs grow in time making it harder to innovate and this was also strongly supported by experts interviewed during the pre-study phase. This resonates well with the previous studies introduced in the literature review chapters. It is also relevant to note that the advantages that come along with

emerging technologies rate higher than the symptoms that are related to technology becoming obsolete (e.g. problems with reliability and responding speed or deviations in usage patterns). So based on these results, one can argue that the **reasons to rewrite systems are much strongly found in the needs to change the business processes and take advantage from new emerging technologies, then they are to be found in the fact that the technology itself will become so outdated** and the system so frustrating for users that it needs to be replaced. These results raise a question that could this be one of the reasons why often getting rid of IT systems at the right time (before they become 20 or 30 years old) does not happen organically? Meaning that there is still a stereotype like opinion that system has become legacy when the technology has become obsolete, even though from the business process perspective the old system might not be in adequate sync with the actual needs. So it can also be concluded that **in order to not miss the right time, systems compliance with expected business processes and potential benefits from emerging technologies has to be regularly re-evaluated**.

SQ 1.3. In which cases should rewrites be considered even if there are no symptoms of outdated technologies present?

Typically people associate symptoms like systems' responding speed getting too slow, solution becoming technologically outdated or software not being visually attractive (modern looking) as indicator that show when IT systems are turning into legacy. But as seen in the previous questions analysis, these may not be the first symptoms to keep an eye on to figure out whether the system is turning into legacy or not. IT system might be responding just fine, have platform support from the vendor etc., but still be turning into legacy because of having too much built-in complexity that has been added over the years and thus impeding innovation of business processes. Complex architecture and lack of appropriate documentation make it difficult to do changes in the system and thus increase the administration and maintenance costs over time because it just takes a lot of time to understand the existing system and analysing possible side-effects of each planned change. All of the problems that were rated as most critical, are typically not visible to the end users making it difficult to realise that the system is already turning into legacy.

In addition, about one third of experts pointed out during the interviews, that one of the criteria that should be considered when estimating the expected lifespan of IT systems is the issue of losing support for the platform. This is mostly the case with solutions based on standard platforms, but it also happens with custom software. The most important negative effects is that the producer of the platform will stop providing updates for the solution, including security updates, and that will in time create a big risk factor for the whole solution. The experts interviewed suggested that the

systems vendor support should be another aspect that need regular re-evaluation. In case there is a threat that the system will lose the vendor support in upcoming 2-3 years then starting to migrate off the platform should be planned.

Interviewed cyber security experts gave example of software solutions that are connected with mission critical production lines of critical service providers (e.g. energy production, water purification, etc.). In some cases there is a specific standard software solutions in use that is strongly tied with the production line. The production lines sometimes have life expectancy of over 20 years (even 30 to 40 years), but the SCADA[13] software that is used to control those production lines ages much faster because it is not updated as regularly as needed by the producer of the production line and control system. And in many cases there are no alternative software that could be used to replace the existing one that has become legacy. So in time, the owner of the process will end up with a control system software that has to run 10 or more years on an outdated operation system (e.g. Microsoft XP) that has no support from vendor anymore and thus there are very limited ways to avoid security breaches because of the fact that the manufacturer of the operation system has stopped supporting it. Based on security experts' opinions, the only way to protect these systems is to defend the perimeter – isolating the system from all external networks. At the same time the business process owners have higher expectancies of having more live' data available to make more rapid business decisions – e.g. to efficiently run energy market, there is a need to get live' data from the production lines about the production volumes. That in turn entails pressure to connect networks to move data between different physical locations. If this is not done under the watchful eyes of cyber security experts, it might lead to a situation where the networks are connected in a way that makes it easy to jump from one system to another, ending up in production line control systems that are running on outdated software and hardware and are thus very vulnerable for cyberattacks. Similar risks are also pointed out by report compiled based on penetration testing exercises of Estonian critical service providers (Vaks, 2014).

The IT manager of Ministry of Economic Affairs and Communications brought out an example that he would like to migrate of from GoPro based document management system and move towards open source alfresco bases system to get rid of licence fees, and minimise development costs by sharing them with other authorities who are already using the alfresco based solution (Kaiklem, 2015).

[13] SCADA - Supervisory Control and Data Acquisition systems are real-time process control systems that monitor and control local or geographically remote devices (Tsang and Smith, 2008).

More than half of the experts' interviewed also emphasised factors like changes in the user expectations (e.g. responsiveness of the application, using touch screens etc.), new emerging technological realities that could be harvested etc.

So to conclude – there are many problems that are related to using outdated technologies and also many opportunities that can be latent to the everyday users but still need to be considered when evaluating the timeliness of IT systems. These include need to change the processes, potential security risks related to using outdated platforms, increase of maintenance costs or high license fees, new technologies, changes of the users expectations etc. In order to notice these aspects and benefit from those, again, regular re-evaluation has to take place.

SQ 2.1. Is there a need for No Legacy Policy guidelines in the public sector to avoid the build-up of IT legacy?

Is there a need for No Legacy Policy in the public sector

The experts were asked for their opinion about the question – is there a need for No Legacy Policy for governments.

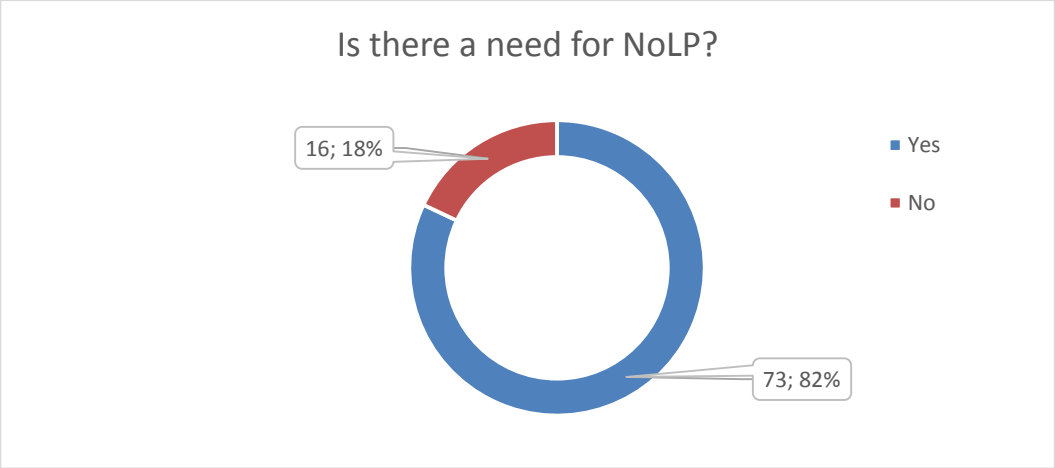

Figure 10. Experts' opinion on whether there is a need for No Legacy Policy.

82% of experts said "yes" to the question "is there a need for a No Legacy Policy guidelines in the public sector?", and 18% thought that such a policy is not needed. 37% of experts who found that NoLP is not needed, argued that it would be too difficult to find such a set of rules that would make it easy to make the decisions about the wipe-off. They though that these rules would be too abstract and hard to measure and decisions should be depending on the specific systems. Similarly 37% of those experts stated that these decisions should mostly be based on the needs to change the business processes and emphasised that processes need to be thoroughly analysed to find enough financial reasoning to do the investment to rewrite the system. 13% of experts found that if a

system is working fine it should not be changed or that some IT systems work just fine for longer than 13 years. Also, 13% of experts stated that NoLP will bring along too high costs and the public sector will just use the rules to demand for budgets for rewriting systems.

During the expert interviews around 90% of the experts stated that NoLP guidelines are needed.

Existing guidelines for fighting against legacy

In order to take advantages from already existing guidelines that different organisations have implemented to get rid of legacy, the experts were asked whether they already have such guidelines in place and what do these guidelines cover.

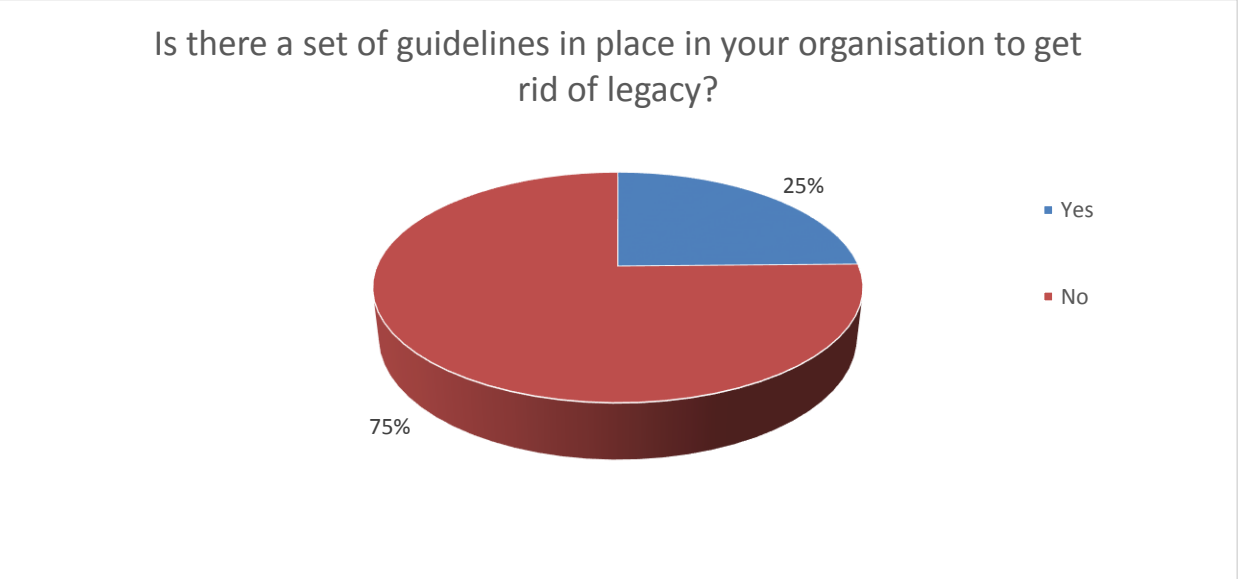

Figure 11. Are there NoLP guidelines in use in the organisations where the experts work at.

75% of respondents admitted of not having such guidelines in their organisation, whereas 25% said that they have them.

Responses about what do these guidelines include were very different – 23% of those who said they have such guidelines in place, explained that it is covered by either some general architectural guidelines document or general principles they apply in software management, e.g. standard software is always upgraded to the latest versions or implementing SOA principles. 18% of them said that it is covered by non-functional requirements document. Two to three respondents also mentioned at least one of the following instruments: having owners of systems in place who are responsible for making sure that systems are kept up to date, implementing portfolio management process, applying common sense, regularly re-evaluating the timeliness of the systems or applying business case based approach – calculating whether it is more reasonable to continue with the existing system or it is more reasonable to replace it with a new one. Typically experts mentioned

having only one of those measures in place. Follow-up questions were sent to all of the respondents who mentioned having these guidelines in use to find out whether they have these guidelines in written format and could they share them to be used as best practices in current research. Only 2 documents were shared with the researcher. Rest of the respondents said that they do not have anything written down. The documents that the researcher received were one non-functional requirements document and one software development guideline document. Both of them had very limited and indirect connection with getting rid of legacy at the right time. The non-functional requirements document is an important document when it comes to procuring software so that it will be built keeping best practices in mind and thus prolonging the potential lifetime of the software, but it usually has little to do with making sure that the software is kept up to date in the long run and is replaced at the right time.

So based on these results, it can be concluded that there were no comprehensive best practices in use that could be taken over to create NoLP for Estonian government. So even tough over 80% of the experts admit that such a set of guidelines is needed, no one of them has implemented comprehensive rules to make sure that the mission critical software solutions are kept up to date.

SQ 2.2. In case such guidelines are needed, how should they be implemented?

There are two relevant aspects that the author of the study finds relevant in terms of how to move forward with No Legacy Policy implementation. First of all, we should learn from the experience of other successful e-governments and consider the fact that their experience shows that fighting against legacy does not happen organically. Based on their experience one can conclude that having no plan to fight off legacy is the way towards a situation where there are many systems that are beyond reasonable lifetime. Secondly, the fact that even tough experts admit that rules need to be in place to fight against legacy, they don't implement them on their own in their organisation. Thus it is clear that central rules need to be in place and to make sure that governmental IT systems are kept up to date, those rules should be implemented on mandatory basis.

SQ 2.3. What kind of IT management aspects should the No Legacy Policy guidelines include?

Some of the aspects about what the NoLP should cover were revealed in the answers to questions covered in previous sub-chapters, but there were several additional questions in the questionnaire to clarify the content of the set of guidelines the policy should include.

One of the key questions was what is the **reasonable lifetime** of an important IT system is. To learn from the existing obstacles that need to be overcome, there was also a question about **what**

impedes getting rid of legacy at the right time, and to learn from what has worked as arguments based on practical experiences, the experts were also asked about **what have been the main reasons why rewrite projects have been initiated**. Experts were also asked about what have been the **lessons learned** while dealing with the legacy solutions.

Maximum reasonable lifespan of critical IT systems

Discussion with IT policy makers of other countries have proven that without clear No Legacy Policy, governments end up with IT systems that are older than 20 years. All representatives of other countries have admitted that they are struggling with legacy systems.

So one of the first steps to clarify where the line should be drawn is to find out how old is too old? Of course there is no ultimate truth as majority of experts also claimed during the interviews in the pre-study phase, but 90% of them still admitted that there is a reasonable "last line" somewhere. So the goal was to find out what is the reasonable lifespan of critical systems based on experts' practical experience and common sense.

In Estonia's case the ICT policy makers have set a goal, that there should not be any important IT systems in use that are older than 13 years. The logic behind that idea is that the reasonable timeframe to use a software is around 10 years. That is the latest time when rewrite projects should be planned and initiated and taking into account that it takes about 3 years to plan, procure and implement a large rewrite project, it makes the lifetime of the system around 13 years. This idea was so far based on a gut feeling of couple of experienced experts. So the aim for the researcher was to clarify, what a wider range of experts think is the reasonable life expectancy of important IT systems.

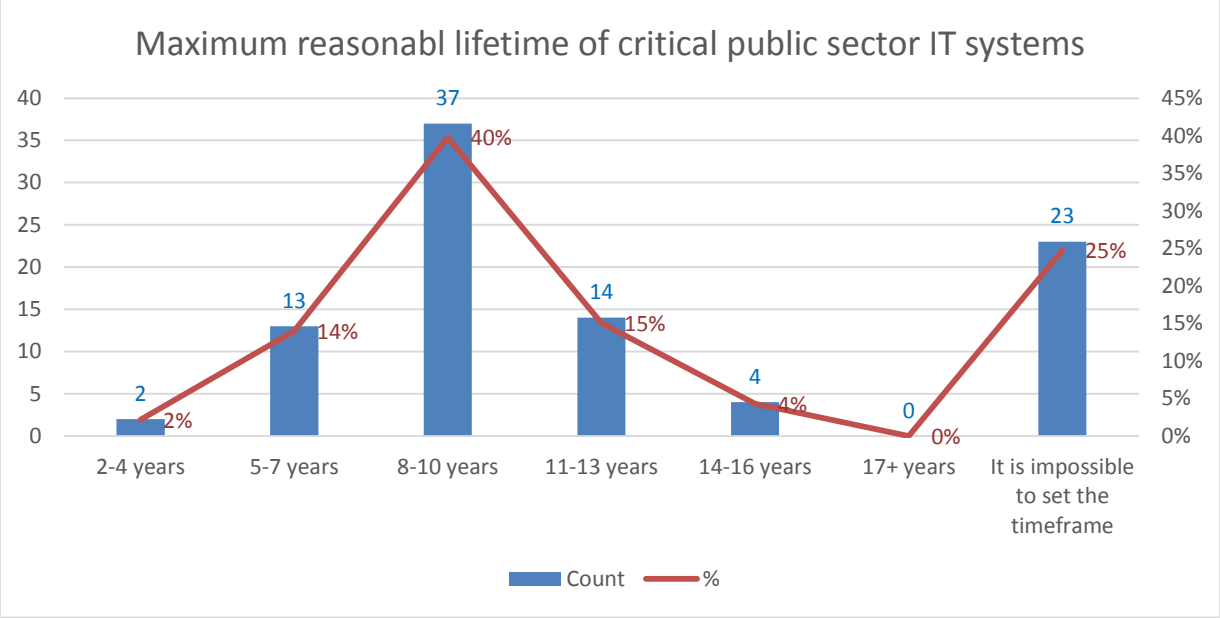

Figure 12. Maximum reasonable lifetime of critical public sector IT systems based on experts' opinions (count and percentage).

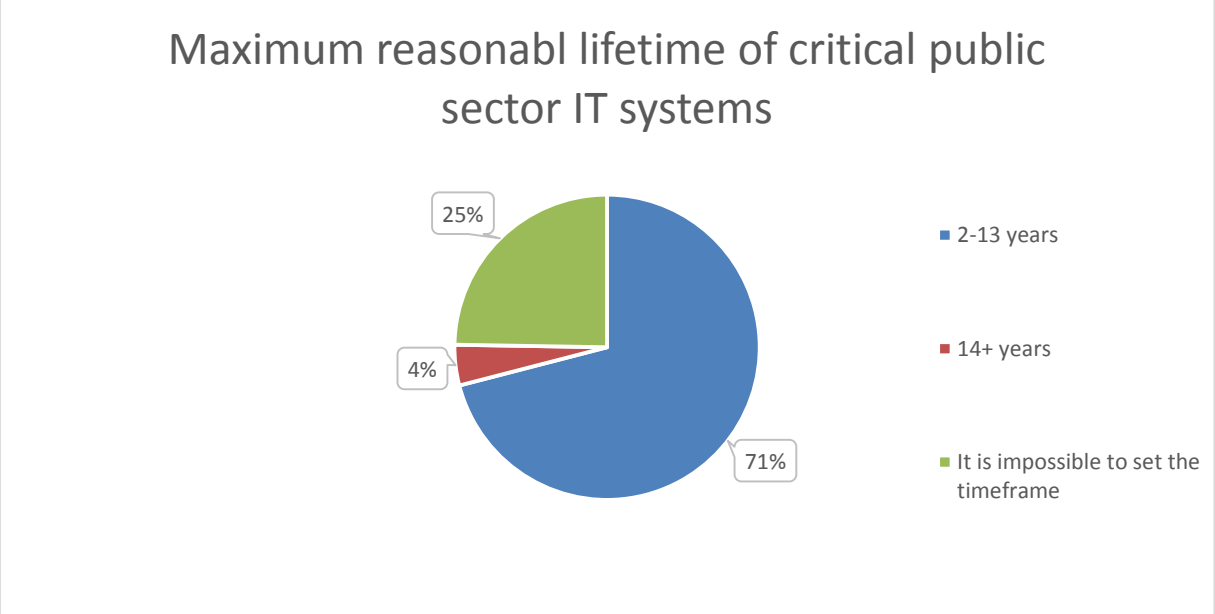

Figure 13. Maximum reasonable lifetime of critical public sector IT systems pie chart.

Majority of respondents (71%) stated that reasonable lifetime of critical public sector IT systems is up to 13 years. Most popular response was that IT systems reasonable lifespan is somewhere between 8-10 years (40%). 4% of respondents thought that reasonable age is between 14-16 years and 25% of respondents found that is impossible to set such a timeframe. During the pre-study only 10% of the experts found it impossible to set such timeframe.

These results confirm that the idea to implement NoLP with the principle that critical IT systems should not be older than 13 years, is well justified based on practical experience of experts in the

field. It can even be claimed that the Estonian 13-year plan is conservative, considering the opinions of experts.

What impedes from getting rid of legacy in the right time

Experts were asked to assess predefined problems on how often they have encountered these in their practical experience as obstacles that impede getting rid of legacy at the right time. 5-point scale was used (1-never; 5-very often/ always).

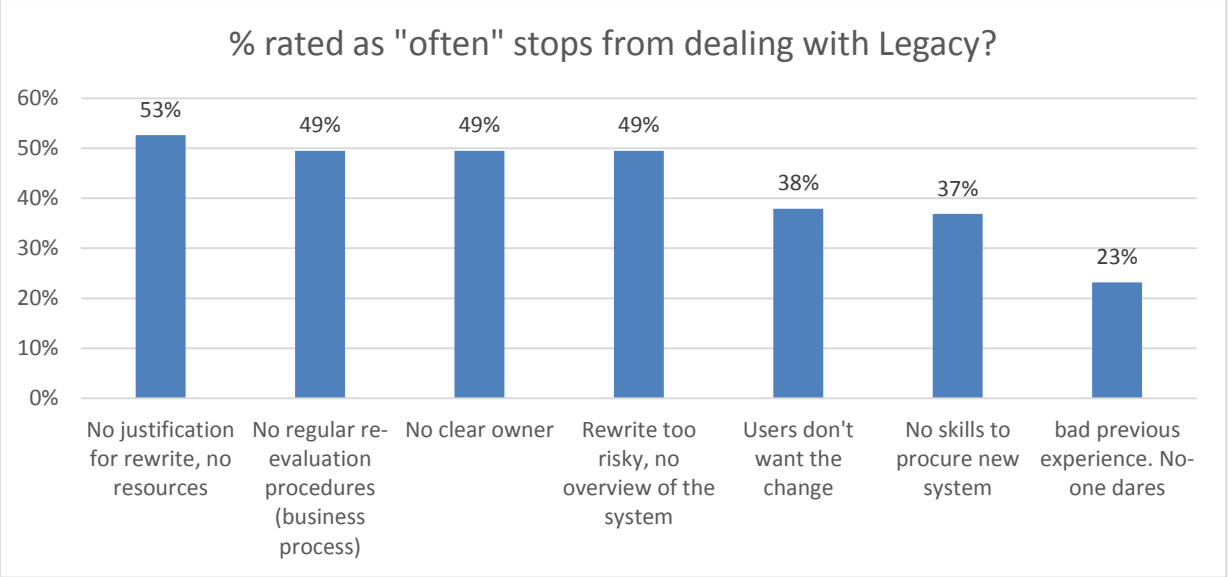

Figure 14. The main obstacles that impede dealing with legacy on time.

The biggest obstacle to get rid of legacy, based on experts' opinion, was not being able to **justify the need to replace the system to the management**, and thus not having the **financial resources** available at the right time. 53% of respondents rated that problem as emerging often (rated with "4-rather often" or "5-very often/ always"). This was followed by problems of **not having regular re-evaluation processes in place** to find out whether the systems are still in sync with changes business needs, **not having clear owners** for every systems, so it is nobodies clear responsibility to conduct the re-evaluation process of the system, and the problem of considering the **rewrite project too risky** because there is a lack of knowledge about the system and related business processes. All these 3 problems were rated as emerging often by half of the experts (49% rated them as being an obstacle often).

These results give good input to what the NoLP should include in order to make sure that IT systems would be monitored more closely to realise once systems are turning into legacy. As the most important obstacle is the inability to justify the rewrite project to the managements and get the funding to move forward with the rewrite project, it makes it evident that business-case based approach has to be inevitable part of NoLP. To convince managers about the necessity of a rewrite

project, the business case calculations about what are the costs with continuing with the as-is situation and what would be the result of the change (to-be), need to be revealed. The financial aspects are covered in more details in a latter chapters.

Main reasons to initiate a rewrite project

Experts were asked to respond in free-form to the question of "based on your practical experience – what have been the 3 main arguments to rewrite a system?"

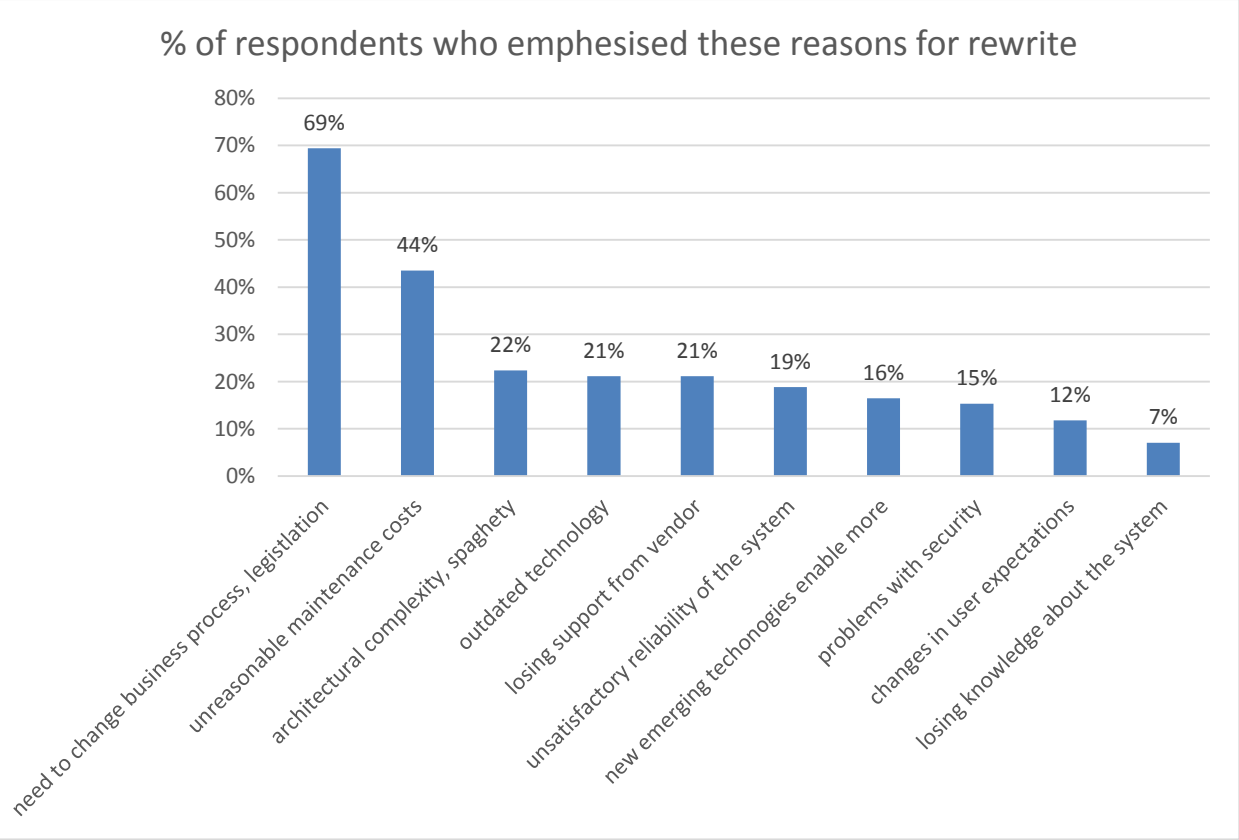

Figure 15. The main reasons for initiating a rewrite project.

Based on experts' opinions, the main reason to initiate the rewrite project is the need to change business process (e.g. comply with new regulations) that is not possible to achieve by modifying old IT systems and thus, new system is needed. 69% of experts who responded to this question, found this to be among top 3 most frequent triggers for rewrite projects. This was followed by wish to get rid of unreasonable maintenance costs (44%), architectural complexity (22%), technology becoming outdated (21%), and losing support from vendors or not having interested partners on the market (21%).

Lessons learned with legacy

Experts were asked to reflect on what have been the main lessons learned in dealing with legacy and what they would do differently in the future. The main target of that question was to get input about what kind of principles the NoLP should include.

Over 40% of experts emphasised that in case rewrite project are undertaken, **processes need to be thoroughly analysed and redesigned** if needed. They explained that in majority of cases with IT systems becoming obsolete, the processes are also outdated and there are many ways of making them more efficient. Around 20% of experts emphasised that one should **avoid building big and monolete systems, instead simple architecture should be preferred and SOA principles** should be implied. About 15% of respondents found it important to just **make the decision** to rewrite when the system has turned into legacy and not wait too long, since it will be much harder and more expensive to change later. Similarly 15% of experts emphasised the need to **take clear responsibility** during the rewrite project (have process owners in place who are able to make important decisions etc.) and also to **avoid excessive complexity** while rewriting a system. They commented that a **business case based** approach helps to maintain common sense and not automate functions where there is no real need to do it. Additionally following lessons learned were brought out by experts: importance of **close cooperation between IT and business process owners** (8% of experts found it important), using **agile development methods** (7%), making sure that the system has **proper documentation** (7%). Other aspects were mentioned more rarely and are thus left out from this analysis.

SQ 2.4. What kind of effect the No Legacy Policy might have on IT budgets of public sector organisations?

One of the main concerns of implementing a rule that there should not be any important IT systems in use that are older than 13 years is the cost of that rule. Thus, experts were asked to give opinions on what kind of impact such a rule would have on IT budgets. Also, since IT can be used to optimise and automate processes, the experts also shared their opinion about whether the rewrites pay off by helping to reduce other process related costs and thus justifying the cost of a rewrite project.

Do rewrite projects mostly pay off

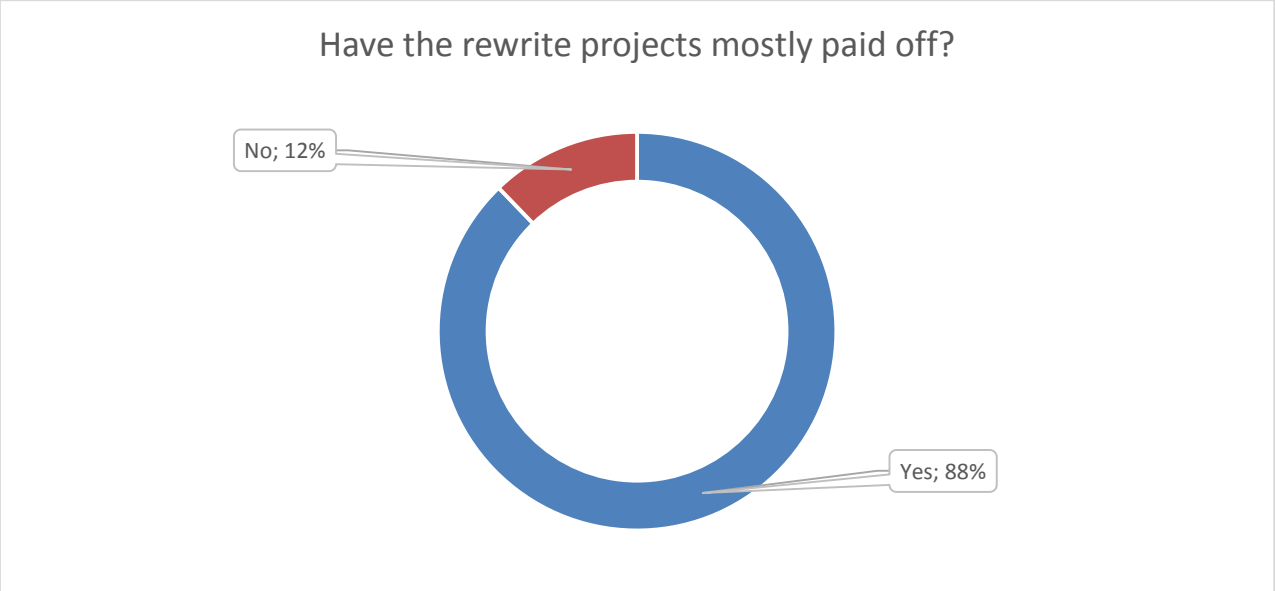

Figure 16. Have the rewrite projects mostly paid off based on experts' opinions.

88% of experts stated that in their opinion, rewrite project mostly do pay off. 12% stated that rewrites don't mostly pay off.

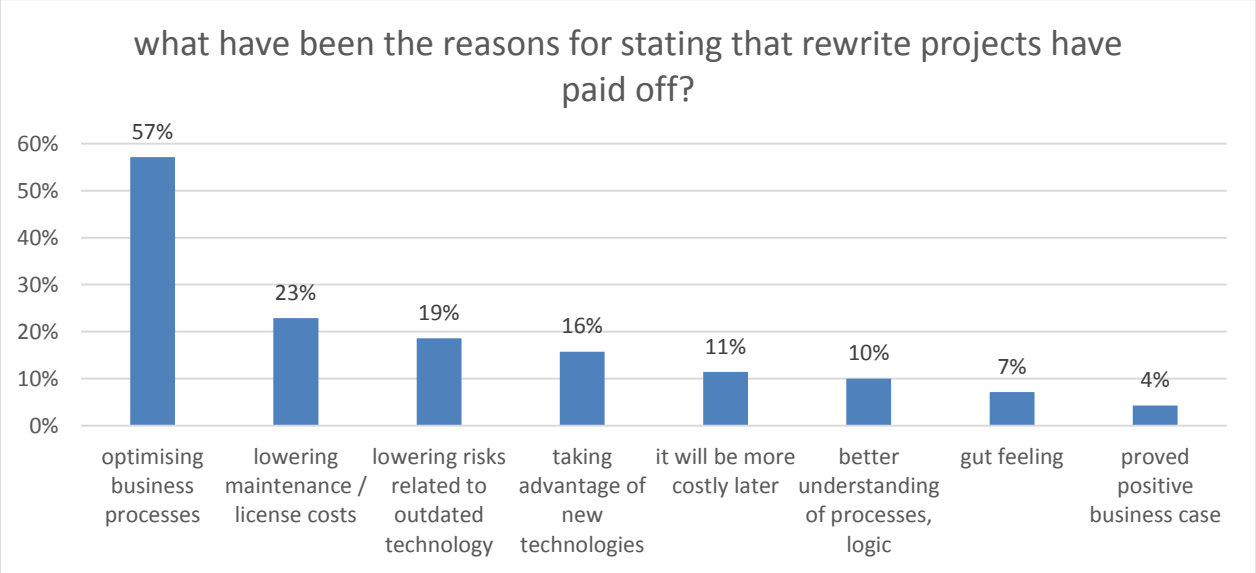

Figure 17. Have the rewrite projects mostly paid off based on experts' opinions (bar chart of percentages).

Respondents were able to add free-form explanation to their opinion. Experts who believed that rewrite projects mostly pay off mostly explained that the biggest benefits come from **optimising business processes** to justify the cost of the rewrite (57% of experts mentioned that as the main benefit). 23% of experts who agreed that rewrites pay off, said that it is due to being able to **lower the maintenance or license costs** of outdated IT system. These reasons were followed by **lowering the risks** related to using outdated platforms (19%), taking advantage of new

technologies (16%). 11% of experts said that the rewrite is inevitable eventually anyway and it was better to do it once the system was turning into legacy, because the **longer you wait the more painful it gets**. 10% mentioned that rewrite project has given a chance to get an understanding of business processes again.

NoLPs' impact on IT budgets

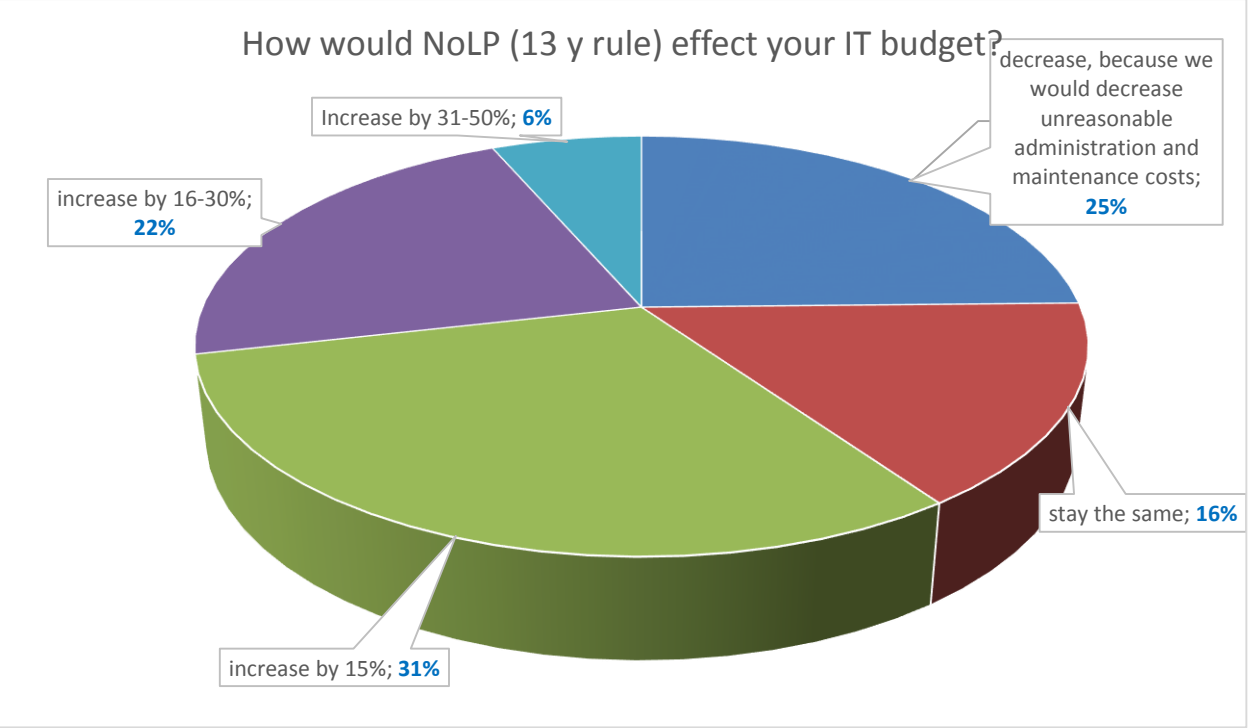

Figure 18. The impact of rewriting all important IT systems in every 13 years to IT budgets (whole sample).

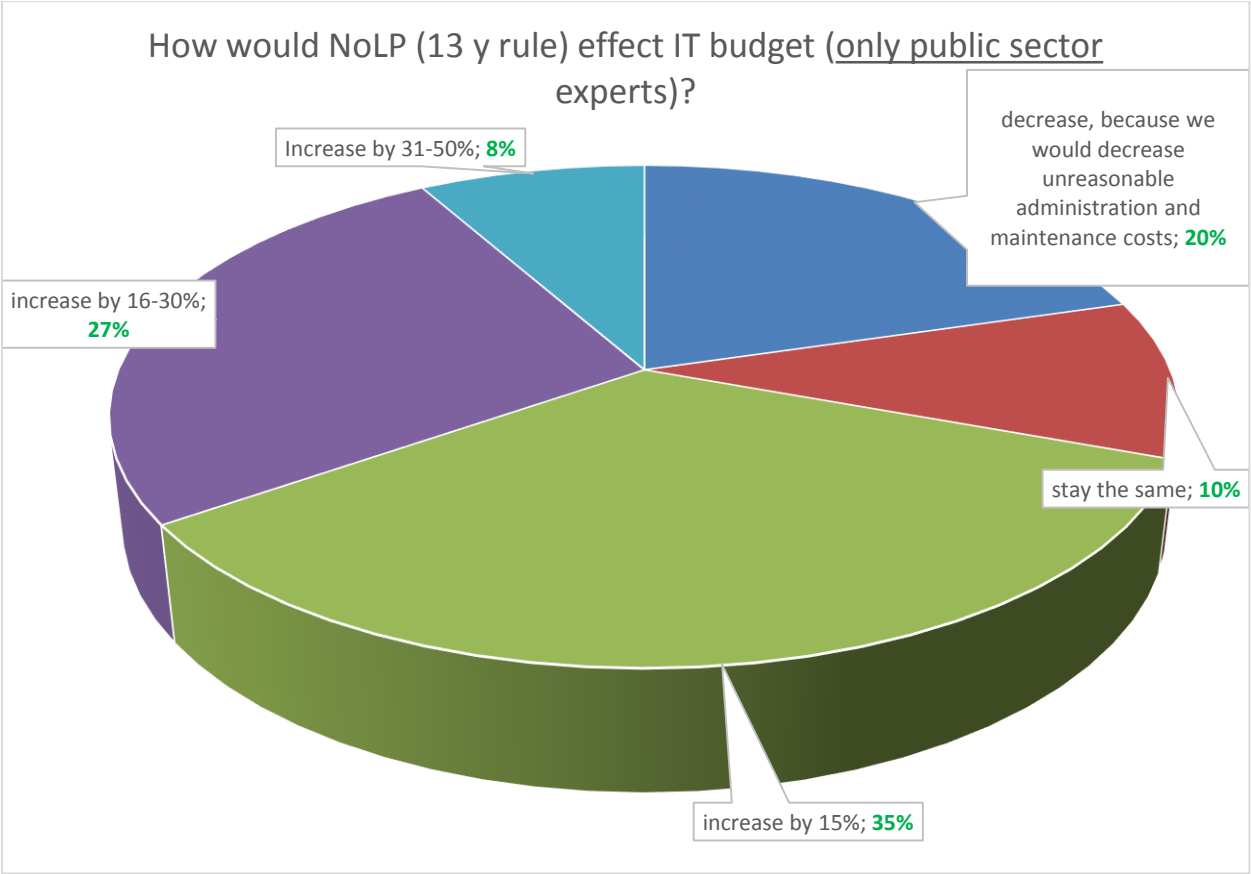

Figure 19. The impact of rewriting all important IT systems in every 13 years to IT budgets (public sector subsample).

72% of all experts stated that in case there was a rule that important IT systems should not be older than 13 years, the **IT budgets would either decrease** (25%), **stay the same** (16%) or **increase up to 15%** (31%). 22% of experts thought that the IT **budgets would increase 16-30%** and 6% found that IT budgets would **increase 31-50%**.

Because the goal is to work out NoLP for Estonian public sector, the researcher found it important to examine the answer to this question among the public sector subsample. 65% of public sector stated that the IT budget would **either decrease** (20%), **stay the same** (10%) or **increase up to 15%** (35%). 27% of respondents found that IT budget would **increase 16-30%**, and 8% of public sector experts thought that the IT **budget would increase 31-50%.**

6. Discussion

The results of this study support the idea that there is a need for clear guidelines that would help governments to sustainably eliminate IT legacy. The experience of other countries also shows that this policy should be **mandatory**, since even though experts are aware of the problems related to legacy build-up, it has not organically lead into a situation of having clear rules in place to fight against legacy in governments.

The study proves that there are many different aspects to be considered while tackling the IT legacy issue. There is no one specific trigger to be carefully monitored, but the whole dynamics needs to be **re-evaluated regularly**. Strong and clear **disciplines** are needed to sustainably fight against the build-up of IT legacy.

In order for these evaluations to happen, **certain prerequisites need to be in place**.

In the following chapter, the author of the study elaborates what could be the mechanisms to systematically deal with IT legacy to make sure that outdated systems are rewritten at the right time and, thus, the build-up of legacy systems could be avoided.

Recommendation about how should No Legacy Policy be implemented

As this study focuses only on mission critical IT systems, processes for solely such systems will be described. Similar rules and processes could be applied also to other IT systems. However, in case these rules are applied to systems with lower criticality ratings, the dates of reviews and rewrites may differ due to lower risks and dependencies.

Prerequisites

One of the key prerequisites of the recommended model is the requirement to have an **information systems portfolio –** a catalogue that contains information about all IT systems an organisation uses**.** The responsibility for IT systems portfolio management should be assigned to IT department as this unit generally has the best overview of all the IT systems used in an organisation.

The following information **has to be stored about all the IT systems**:

- Criticality of the IT system (is it a mission critical system or not);
- Owner of the system (owner of the business processes; in case there are many owners of processes, a main owner has to be agreed);
- Go Live year (year when the system went to production);

- Estimated rewrite project initiation year (as a default: 10 years after Go Live; re-evaluated regularly but cannot be longer than 10 years after Go Live year since it takes about 3 years to plan and implement a rewrite project);
- Current administration costs of the IT system (overview of yearly costs since the system went live, maintenance and investment costs differentiated);
- Cost prediction of the IT system (today + 5-10 years cost estimations about maintenance and investment costs; investment costs also include estimated re-write cost);
- Date of the last re-evaluation;
- Date of next planned re-evaluation (as a default: last re-evaluation date + 1 year in case of mission critical IT systems).

#	IT system	Criticality (high = mission critical)	Owner	Next review date	Go Live	Rewrite year	Costs	2010	2011	2012	2013	2014	2015	2016	2017
1	System A	high	John Doe	aug.16	2007	2017	Mainten.	170 000	150 000	165 000	168 000	172 000	175 000	180 000	180 000
							Investm.		20 000		37 000		15 000		500 000
2	System B	high	Jane Doe	apr.16	2008	2018	Mainten.	16 000	16 500	18 000	17 000	18 200	25 000	27 000	27 000
							Investm.	38 000		25 500			27 000		
3	System C	avarage	John Doe	Jul.17	2014	2024	Mainten.					12000	47 200	48 000	52 800
							Investm.			472 000	84 960	42480		35 000	
4	System D	high	Jill Banks		2006	2016	Mainten.	103 000	120 000	89 000	135 000	128 000	189 000	190 000	209 000
							Investm.			250 000	78 000			650 000	400 000
5	System E	low	Kate Boss	May.17	2010	2020	Mainten.	5600	37 000	20 000	22 900	25 190	25 670	26 000	26 000
							Investm.	50000		16 700	10 500		67 000		20 000
							Total maint.	294 600	323 500	292 000	342 900	355 390	461 870	471 000	494 800
							Total Invest.	88 000	20 000	764 200	210 460	42 480	109 000	685 000	920 000
							Total cost	382 600	343 500	1 056 200	553 360	397 870	570 870	1 156 000	1 414 800

Figure 20. Example of IT systems catalogue table.

IT department is **obliged to make sure that all mission critical IT systems are re-evaluated at least once a year**. Taking into account the fact that governmental budgeting is done once a year, the author suggests that the re-evaluation of all the critical systems should take place **2-3 months before the budgeting for the next year**, since in case major changes need to be planned, it takes at least couple of months to clarify the costs of these changes.

Finally, the business **process owners have to be willing and able to critically analyse and redesign business processes**. It is important to keep in mind the threat of mind-set legacy. Thus, it is strongly recommended, that additional pair of eyes should be involved in these processes.

Process overview

Following figure describes the annual process that should be implemented to review all the mission critical IT systems that the organisation has.

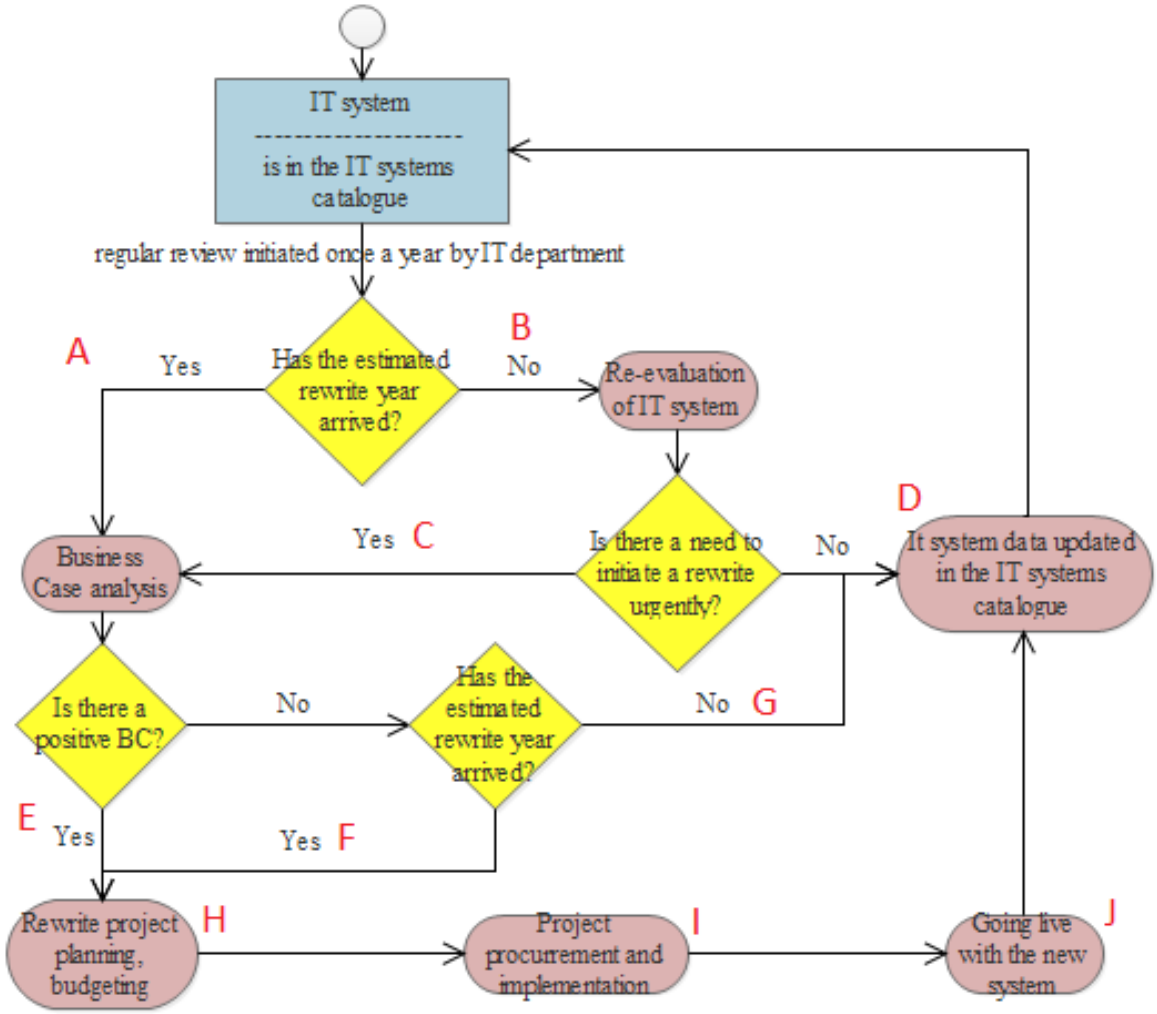

Figure 21. Process overview of annual review of critical IT systems.

Explanation of the process

- Each mission critical IT system is reviewed at least once a year, once the "next re-evaluation date" arrives.
- In case the system has reached the "estimated re-write initiation year", it moves to **business case analysis** phase (see A in Figure 21).
- In case the system has not yet reached the "estimated re-writing initiation year", it moves to full **re-evaluation process** (the process is described in more details in the following sub-chapter) (see B in Figure 21).

Re-evaluation process

- Detailed re-evaluation is done to find out are there enough reasons to initiate a rewrite project right away.
- In case urgent rewrite is needed, the process continues with the **business case analysis** phase (See C in Figure 21).
- In case there is no need to initiate a rewrite project right away, the process continues with **updating the IT systems' information in the IT systems catalogue** (see D in Figure 21). Among other things, the "estimated rewrite project initiation year", "prognosis for the costs for next years" and "date of next planned re-evaluation" have to be analysed and updated.

Business case analysis

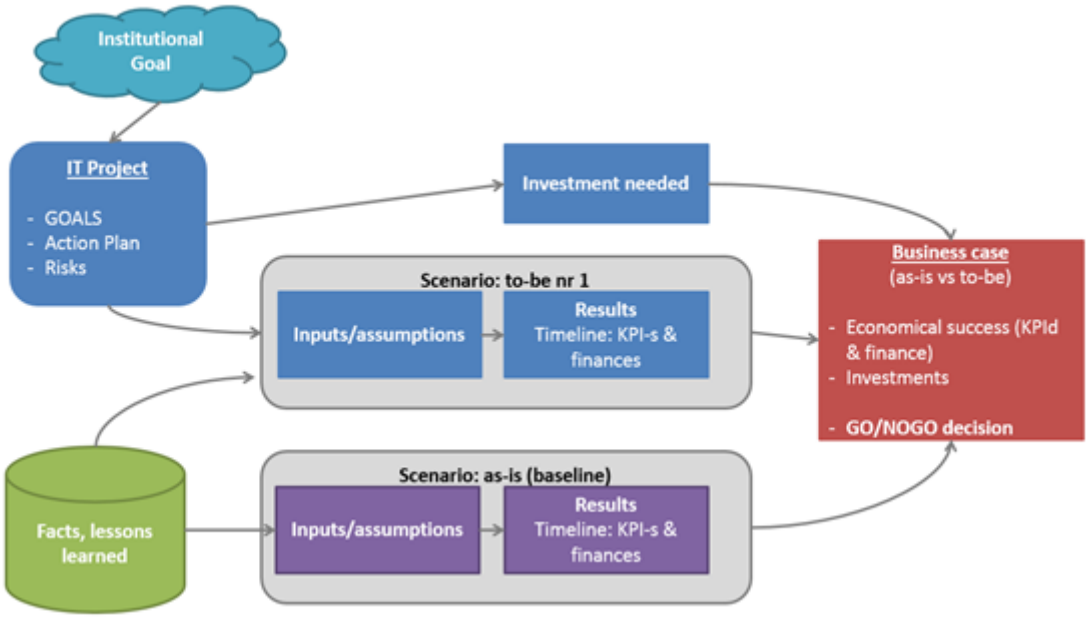

Figure 22. Description of business case analysis (author of the picture: Urmo Pärg).

- During business case analysis process, the as-is and to-be processes are analysed and process related costs calculated for both scenarios (including all major costs like IT, personnel, transportation, storage, postage etc. the costs calculations should include the costs of all related parties including public sector authorities, businesses, citizens).
- In case **there is a positive business case** for rewrite project, the process continues with initiating more detailed **rewrite project planning** (see E in Figure 21).

- In case the business case in negative, but the "estimated rewrite project initiation year" has been reached, the process also continues with more detailed **rewrite project planning** (see F in Figure 21).
- In case the business case is negative, but the "estimated rewrite project initiation year" has not been reached, the process continues with **updating the IT systems' information in the IT systems catalogue** (see G in Figure 21).

Rewrite project planning and implementation phases

- During the rewrite project planning concrete steps forward will be planned including budgeting, project implementation timeline (initial project plan is compiled) etc. (see H in Figure 21).
- After planning, project implementation is initiated. During this phase, procurement is conducted and project is undertaken to implement new version of the system (see I in Figure 21).
- Once system is developed (all requirements for go live are fulfilled), the new IT system moves into production (see J in Figure 21).
- Once IT system has moved to production phase, the system is registered in the IT systems catalogue and the old system is removed from the catalogue (see D in Figure 21). In case there will still be certain functions running in the old version and thus it is not possible to switch the system off, then the IT department and system owner have to agree a clear plan for shutting the old system down. This plan has to include steps that have to be taken to close the system down with clear responsibilities and deadline.

Re-evaluation process

Due to the fact that the reasoning for rewrites usually comes from the need to change the processes to an extent that the outdated system does not enable, the re-evaluation process should be led by IT system owners not IT department.

During the re-evaluation process following (but not limited to) aspects need to be reviewed:

- Is the system still **in sync with the business process needs**? If not, is it possible to implement the new requirements in the existing system with reasonable efforts?

- Does the system have a **vendor support** today and for the next three years on reasonable terms (cost, competence levels, and readiness to provide services)?
- Is the system still **in sync with technical realities** of today? Following sub-questions should be reviewed:
- Is the infrastructure is still up to date?
- Is the technical platform still up to date?
- Is the system in compliance with user expectations?
- Have there been **changes in the ecosystem** that would enable to optimise processes so that it will help to significantly reduce the process related costs to public sector, businesses or citizens or are there new emerging risks or requirements that have to be complied to? E.g.:
    - *reusing data that has become available to reduce need for interaction or manual work;*
    - *have some of the previously existing technological capabilities now more reasonably prices, and thus implementing them now could have positive business case (e.g. storage, cloud services pricing etc.);*
    - *are there new risks or requirements that are impossible to manage in the existing IT system.*
- Are there open source or better priced new platforms available today that would help to significantly lower the operational costs (get rid of license fees etc.)?
- Are there **new emerging technologies** that are mature enough for implementation and could help to significantly reduce the process related costs to public sector, businesses or citizens? (E.g. maturity of voice control technologies, using new gadgets etc.)?
- Are the **maintenance costs** of the system unreasonably high and would rewrite of the system help to significantly reduce those costs?
- Are there increased **cyber security risks** that have high probability and high impact when realising, thus should a rewrite project be undertaken because of the cyber risks?

Budget management

During the study, many problems with budgeting were revealed and overall it can be concluded that on average there is a low maturity in IT budget planning in the Estonian public sector. Thus

the author finds it relevant to also describe what kind of budgeting mechanisms should be implemented.

System owners should be able to **separate maintenance costs from innovation costs** since the increase of maintenance costs proportion is one of the symptoms of systems turning into legacy. This might not be a trigger in its self, rather than an issue to discuss while re-evaluating the systems timeliness. E.g. in case the maintenance costs have been 70-90% of the overall costs of the system for many years, there is a threat that people (owners, vendors) are losing the competence about the system. Thus, the IT department and business process owners should discuss whether this is a result of actual reality (there are no needs for process changes) or is it a symptom of system becoming legacy. IT department and system owner should have a mutual understanding about the main causes of high maintenance cost proportions. They should agree on whether there are no major changes done (and thus innovation cost proportion is low) because there are no needs for changes or are they not done because they are avoided since the systems has turned into a spaghetti that no one understands any more.

Regarding investment planning – **business case based approach** is crucial since one of the main problems that stops from dealing with legacy at the moment is the inability to justify the investment needs to managers. At the same time, the investment management practice in Estonia clearly shows that in many cases the investment will pay off if the processes are redesigned during the rewrite project. So even though all the rewrite projects will not always pay off when looking at them separately, the study supports the idea that **on average, the rewrites do pay off taking into account the overall process related costs**.

It has also become clear that additional **budgeting rules are needed**. For example, the **replacement costs of mission critical systems should be planned well ahead**, similarly to the replacement costs of other important infrastructure, be it the real estate, roads etc. In case an IT system helps to **reduce other process related costs, part of those savings should be permanently redirected into IT system maintenance and later replacement costs**. So the maturity of IT management has to go hand-in-hand with the maturity of IT budget planning. At the moment these agreements are rarely done in advance of IT system development, often leading to a situation where there is not even maintenance costs planned for the systems after the development, not to mention the replacement costs of the system. It is critical to brake this cycle of budget planning in order to be successful in implementing the No Legacy Policy.

7. Conclusions

This study focused on the legacy build-up problem in the public sector. The experience of ICT investment management process in Estonian government has shown that more systematic approach in investment planning is needed in order to be able to sustainably avoid the build-up of legacy. Also the experience of other countries who have been successful in implementing e-government solutions, shows that getting rid of legacy systems does not happen organically.

Governments all over the world are becoming increasingly dependent on IT solutions, moving more and more towards automated processes and enabling citizens and businesses to self-serve themselves. At the same time threats in the cyber world are increasing and the build-up of outdated systems raises the proportion of maintenance costs, leaving less money to be invested into innovation. These problems need to be tackled to ensure cyber security, continuity and sustainability of IT systems in the public sector.

Currently there are no policy guidelines that support a sustainable investment planning process of critical IT systems and help to deal with the problem of outdated IT solutions.

Thus, the goal of this masters' thesis was to find out it there a need for more concrete guidelines that help to solve the legacy build-up problem for governments. The study aimed to find answers to two main questions: **how to find out which IT systems are becoming outdated in the right time** and **how to sustainably ensure that the public sector is IT legacy free?** In order to answer them, these main questions were broken into 7 sub-questions.

The study was conducted in two stages. During the pre-study phase over 20 Estonian and foreign experts were interviewed to clarify issues related to legacy. As a next step, quantitative study was conducted. 95 experts from Estonia and 19 foreign countries completed the questionnaire based on their practical experience in dealing with legacy. In addition, a document analysis was done to study previously existing materials relevant to the research topic.

The pre-study revealed many aspects to be considered when deciding whether an IT system has turned into legacy or not. For example, there are many enablers that create additional value if used well to enhance the government services, lower the costs or help to meet changed customer expectations. Just to name a few – emerging technologies, benefits of open source, wide availability of data for reuse, or other changes in the ecosystem that could improve public governance by digital means. Also, the idea of legacy as an innovation blocker was explained as a

relevant concept. Innovation is an incremental process – one can only innovate to certain extent at a time. Getting rid of legacy enables to redesign and optimise processes again and again. Therefore, the more often systems are wiped off, the faster one can innovate the processes.

The lifecycle management of IT hardware and standard software were introduced as relevant examples to learn from.

The results show that the main reasons hindering dealing with legacy include inability to justify the investment need to management (53% rated as revealing often), not having regular re-evaluation procedures in place (49%), lack of clear agreement on the ownership of systems (49%) or rewrite projects are considered too risky (49%).

Rewrites of IT systems are usually initiated, when there is a need to change processes to an extent that cannot be done in the outdated solution (69%). The second most important reason for the re-write is related to increased maintenance costs of the outdated system (44%).

88% of the experts' claim that rewrite projects mostly pay off taking into account the overall process related costs. 57% of them claim that the main benefit comes from optimizing the business processes, 23% state that it helps to lower maintenance costs, 19% state that rewrites help to lower risks related to using outdated technologies. 16% of the experts say that rewrites help to harness the benefits of emerging technologies.

Regarding NoLP impact on budgets 72% of experts were of opinion that IT budgets would either decrease, stay the same, or increase by 15%. 22% of the experts thought that implementing NoLP would increase IT budget by 16-30% and 6% of respondents thought that the budget would increase 31-50%.

The results of the study confirm that there is a need for No Legacy Policy in the public sector (82% of the experts stated that it is needed) and that the implementation of such policy should be centrally coordinated, as it does not happen organically. The study also shows that a number of criteria need to be considered to decide whether an IT solution is still up to date or a rewrite project should be initiated. Many strict rules and procedures have to be implemented in order to keep governments legacy-free. It is also evident that the maturity of ICT budget management is crucial in eliminating legacy in the public sector. None of the experts involved in the study knew or had implemented a good, comprehensive model that helps to deal with the legacy issue and sustainably avoid the build-up of legacy. 25% of experts claimed having such guidelines in place, but further questioning revealed that these did not provide a complete solution. 71% of the experts agreed that reasonable lifetime of mission critical IT systems is 2-13 years, supporting the initial idea proposed

by Estonian government CIO Taavi Kotka, which stated that governments should not have any important IT systems in use that are over 13 years old.

Summary of main conclusions and policy recommendations

The 5th chapter introduces one possible model about how No Legacy Policy could be implemented. The chapter covers aspects relevant for the implementation of the NoLP, such as main prerequisites of NoLP, process overview, and recommendations for improving IT budget management and planning.

The main contribution of this thesis can be summarized in the form of the following policy recommendations:

- Governments have to implement No Legacy Policy as a mandatory rule since ensuring that governments are sustainably IT legacy free. This does not happen organically.
- Having a comprehensive overview of existing IT systems in a form of a catalogue (including information about each systems criticality, 'go to live' date, costs to date, estimated costs in the future, and clear owners), is a key pre-requisite of implementing the NoLP.
- Yearly re-evaluations of all the critical IT systems must take place.
- Both technical and business requirements have to be re-evaluated on a yearly basis to ensure timely realization that an information system is turning into legacy.
- Business case based approach is needed to make sure that cost-optimised solutions are being created.
- In case a system does not meet the business needs anymore and redesigning processes or adapting new technologies would make it financially reasonable to rewrite a system, the rewrite project should be planned and implemented.
- In case a system has turned 10 years old, rewrite project should be planned and initiated to make sure that the old system is replaced at latest when its 13 years old.
- Higher maturity of ICT budgeting is needed in the public sector to implement NoLP. Savings from process related costs have to be partially redirected into maintenance and replacement costs of the IT system. Replacement costs of IT systems need to be planned well ahead similarly to other infrastructure replacement costs.

Suggestions for follow-up studies

There are many aspects that need to be studied further. For instance, the effect of the NoLP on IT budgets should be calculated based on highly IT dependent government organisations. This analysis should not only focus on IT budget analysis, but also explore the impact on other business process related costs (e.g. personnel, postage, office, workstation etc.).

Another aspect needing further in-depth analysis is the issue of architectural complexity that emerges when IT systems age. A thorough analysis is needed to understand, what could be done in order to prolong the period where the system is still understandable for the process owners as well as the developers who have to do the changes in the system.

It is important that the cybersecurity aspects of legacy systems should also be studied further because of their tendency to be latent by nature. In order to find out what is the actual status of outdated IT systems, penetration testing should be done. In case such testing is conducted with many systems in different age ranges, it would give a clearer understanding of what is the age range where the risks get too high to be managed successfully.

Working out suitable funding mechanisms is a crucial part of NoLP implementation. For example, rules for redirecting process cost savings partially into IT systems' maintenance and system replacement costs could be part of that funding model. The replacement cost planning is needed to maintain the cycle of rewrites in at least every 10-13 years etc. Concrete models need to be developed and agreed to support the implementation of NoLP.

Bibliography

1. Anon., 2015. *Interview about legacy related problems with an expert who has extensive previous experience managing IT systems in the private sector.* (Personal communication in the semi-focused interview format during the pre-study phase of current theses research, spring 2015).

2. Anon., 2014. Federal IT budgets not enough to combat cyber threats. Merlin. [Online] 31 March.

   Available at: http://www.merlin-intl.com/federal-it-budgets-not-enough-to-combat-cyber-threats/

   [Accessed 30 November 2014].

3. Anon., 2010. Story of Shapes and Sizes: Mobile phone evolution. *GSMArena.* [Online]

   Available at: http://www.gsmarena.com/mobile_phone_evolution-review-493.php

   [Accessed 20 October 2015]

4. Arengufond, n.d. An overview of the smart specialization situation in the world and in Estonia. #3 Health Technologies. [Online]

   Available at: http://ns.arengufond.ee/en

   [Accessed 01 December 2015]

5. Bednarz, A., 2004. Profiling Cybercriminals: A promising but immature science. [Online]

   Available at: http://www.networkworld.com/article/2327820/lan-wan/profiling-cybercriminals--a-promising-but-immature-science.html

   [Accessed 31 October 2015]

6. Beidleman, S. W., 2009. *Defining and Deterring Cyber War*. Masters. Carlisle Barracks, PA: U.S. Army War College.

7. Bosomworth, D., 2015. *Statistics on mobile usage and adoption to inform your mobile marketing strategy.* [Online]

   Available at: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

   [Accessed 26 October 2015]

8. Buchmann, I., Frischbier, S. & Pütz, D., 2011. *Towards an Estimation Model for Software*

Maintenance Costs. Oldenburg, Germany. March 2011. IEEE: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5741327

9. Certification centre, 2014. Alates oktoobrist 2014 on ID-tarkvara arendus üle viidud GitHub keskkonda, mis on leitav https://github.com/open-eid

   Available at: http://www.id.ee/index.php?id=37014

   [Accessed 12 November 2015]

10. Christensen, C., 1997. *The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail.* 2nd ed. Boston, Massachusetts: Harvard Business Review Press.

11. Department of Homeland Security, 2003. *National Strategy to Secure Cyberspace*. [Online]

    Available at: http://www.dhs.gov/national-strategy-secure-cyberspace

    [Accessed 20 July 2015]

12. Eastwood, A., 1993. Firm fires shots at legacy systems. *Computing Canada* 19 (2), p. 17.

13. Elering, 2012. *Eesti elektrituru täielik avanemine.* [Internet] (Published 2012)

    Available at: http://avatud2013.ee/wp-content/uploads/2012/09/Elektrituru_avanemise_bros%CC%8Cu%CC%88u%CC%88r_est_september2012.pdf

    [Accessed 31 October 2015]

14. Entner, R., 2011. International comparison: the handset replacement cycle. *Recon Analytics.* [Online].

    Available at: http://mobilefuture.org/wp-content/uploads/2013/02/mobile-future.publications.handset-replacement-cycle.pdf

    [Accessed 10 October 2015]

15. Erickson, C., 2012. The touching history of Touchscreen Tech, [Online].

    Available at: http://mashable.com/2012/11/09/touchscreen-history/

    [Accessed 24 October 2015]

16. Erlikh, L., 2000. Leveraging legacy system dollars for E-business. *(IEEE) IT Pro*, May/June 2000, p. 17-23.

17. European Commission, 2015a. Digital Agenda Scoreboard 2015, Estonian country report. [Online]

Available at: https://ec.europa.eu/digital-agenda/en/scoreboard/estonia

[Accessed 12 October 2015]

18. European Commission, 2015b. Grand Coalition for digital jobs. [Online]

Available at: http://ec.europa.eu/digital-agenda/en/digital-jobs-0

[Accessed 10 December 2015]

19. European Commission, 2012. Digital Agenda Scoreboard. Indicators analysing environment. [online]

Available at: http://scoreboardtest.edw.ro/charts/copy2_of_analyse-one-indicator-and-compare-countries#chart={"indicator-group":"EHS","indicator":"h_ehealthAvail_Use","breakdown":"TOTAL","unit-measure":"v_compInd","ref-area":["BE","BG","CZ","DK","DE","EE","IE","EL","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","UK","EU27","HR","IS","NO"]}

[Accessed 12 December 2015]

20. European Union, n.d. The EU in brief [Online]

Available at: http://europa.eu/about-eu/basic-information/about/index_en.htm

[Accessed 01 December 2015]

21. Garretson, C., 2010. Pulling the plug on old hardware: Life-cycle management explained. *Computerworld*, [Online].

Available at: http://www.computerworld.com/article/2517337/computer-hardware/pulling-the-plug-on-old-hardware--life-cycle-management-explained.html

[Accessed 24 October 2015]

22. Gartner, 2015a. *Gartner Says Worldwide Smartphones Sales Recorded Slowest Growth Since 2013.* [Online]

Available at: http://www.gartner.com/newsroom/id/3115517

[Accessed 1 November 2015]

23. Gartner, 2015b. *Gartner Says Smartphone Sales Surpassed One Billion Units in 2014.* [Online]

Available at: http://www.gartner.com/newsroom/id/2996817

[Accessed 15 November 2015]

24. Information System Authority, 2013. *Andmevahetuskiht x-tee.* [Online]

    Available at: https://www.ria.ee/x-tee

    [Accessed 26 October 2015]

25. Information System Authority, 2014. *Study about digital dependency of vital service providers.* (Study report is not publicly available).

26. Information Systems Authority, 2015. *RIA 2015 I poolaasta kokkuvõte (translation: State Information System Authority 2015 first half-year summary report).* (Report is not publicly available).

27. Kaiklem, K., 2015. Discussions about IT Legacy related issues at the Ministry of Economic Affairs and Communications. NoLPs effect on IT budget of the ministry. (Personal communication, several meetings in September 2015)

28. Karjalainen, A.-M., 2015. *Discussions with Finnish government CIO about legacy and state IT budgets.* (Personal communication, 30.04.2015, EU CIOs meeting in Riga).

29. Keizer, G., 2012. Microsoft adds 6 months to Office 2007's support lifespan. *Computerworld.* [Online].

    Available at: http://www.computerworld.com/article/2503103/enterprise-applications/microsoft-adds-6-months-to-office-2007-s-support-lifespan.html

    [Accessed 20 October 2015]

30. Konkel, F., 2012. Legacy systems still power much of government. *FCW*, [internet] 10 December.

    Available at: http://fcw.com/articles/2012/12/10/legacy-systems.aspx

    [Accessed 30 November 2014]

31. Konkel, 2013. COBOL still integral to government systems. *FCW*, [internet] 12 December.

    Available at: http://fcw.com/Articles/2013/12/12/cobol-legacy.aspx

    [Accessed 30 November 2014]

32. Kotka, T., 2014. *Concept of Estonian government cloud and data embassies*. Masters. Tallinn: Tallinn University of Technology.

33. Lewis, J. A., 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* [E-book]. Washington, DC: Centre for Strategic & International Studies.

Available at: http://www.steptoe.com/publications/231a.pdf

[Accessed 29 March 2015]

34. Linden, E. V., ed. 2007. *Focus on Terrorism.* Hauppauge NY: Nova Science Publishers, Inc.

35. Maxwell, L., 2013. *Discussion about government IT management* (Personal communication with Taavi Kotka, 2013).

36. Microsoft, 2014a. Windows XP support has ended. [internet]

Available at: http://windows.microsoft.com/en-us/windows/end-support-help

[Accessed 30 November 2014]

37. Microsoft, 2014b. Windows lifecycle fact sheet. [internet] April.

Available at: http://windows.microsoft.com/en-us/windows/lifecycle

[Accessed 30 November 2014]

38. Ministry of Economic Affairs and Communications, 2015. Tarkvara riigihangete soovituslik tüüpleping. [Online]

Available at: https://www.mkm.ee/et/tegevused-eesmargid/infouhiskond

[Accessed 4 December 2015]

39. Mitchell, R. L., 2006. COBOL: Not Dead Yet. *Computerworld*, [internet] 4 October.

Available at: http://www.computerworld.com/article/2554103/app-development/cobol--not-dead-yet.html.

[Accessed 30 November 2014].

40. Moore, S., 2013. Gartner Survey Shows 75 Percent of Government CIO Budgets Flat or Increasing 2013. *Gartner*, [internet] 12 August.

Available at: http://www.gartner.com/newsroom/id/2572815

[Accessed 30 November 2014].

41. Nordic countries IT policy coordinators. 2015. *EU government CIOs meeting in Riga under the Latvian presidency of EU*. Discussion about IT Legacy related issues, government IT budgets etc. (Personal communication, 5.-6. May 2015).

42. Occleshaw, T. 2015. Discussion about IT Legacy related issues in New Zealand, government IT budget etc. (Personal communication, 24. April 2015, Singapore).

43. OECD, n.d. About OECD. [Online]

Available at: http://www.oecd.org/about/

[Accessed 02 December 2015]

44. Oracle, (n.d.). Oracle Lifetime Support, Coverage for Oracle technology Products. [Internet]

Available at: http://www.oracle.com/us/support/library/lsp-tech-chart-069290.pdf

[Accessed 20 October 2015]

45. Perez, S., 2014. *Majority of Digital Media Consumption Now Takes Place In Mobile Apps.* [Online]

Available at: http://techcrunch.com/2014/08/21/majority-of-digital-media-consumption-now-takes-place-in-mobile-apps/

[Accesses 26 October 2015]

46. Peterkop, T., 2015. Meie regioonile on iseloomulikud poliitiliselt motiveeritud küberrünnakud. [Online]

Available at: https://www.ria.ee/meie-regioonile-on-iseloomulikud-poliitiliselt-motiveeritud-kuberrunnakud/

[Accessed 25 October 2015]

47. Pogue, D., 2013. Should You Upgrade Your Phone Every Year? – Not Anymore. *Scientific America.* [Online].

Available at: http://www.scientificamerican.com/article/should-you-upgrade-your-phone-every-year-not-anymore/

[Accessed 24 October 2015]

48. Poh, J. 2015. Discussion about IT Legacy related issues in Singapore, government IT budget etc. (Personal communication, 20. April 2015, Melbourne).

49. Praxis, 2013. Eesti IKT tööjõu uuring. [Online]

Available at: http://itl.ee/index.php?page=224

[Accessed 10.12.2015]

50. Roos, A. 2015. Discussion about IT Legacy related issues in the energy sector. (Personal communication, 26. March 2015, Tallinn]

51. Seacord, R., Plakosh, D. & Lewis, G., 2003. *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices.* Boston, MA: (SEI Series in

Software Engineering). Addison-Wesley Longman Publishing Co., Inc.

52. Sihvart, M. 2015. Discussion about the sustainability of ICT funding in the government. (Personal communication, 17. November 2015, Tallinn).

53. Skype, 2015. *An article about skype translator.* [Online]

    Available at: http://www.skype.com/en/translator-preview/

    [Accessed 30 October 2015]

54. Stevens, M., Karpman, P., & Peyrin, T., 2015. The SHAppening: freestart collision for SHA-1. [Online]

    Available at: https://sites.google.com/site/itstheshappening/

    [Accessed 12 December 2015]

55. Tiru, M. 2015. Meeting with representatives of Positium – discussion about the opportunities behind using anonymised telecom data for analytics. (Personal communication, 27. November 2015)

56. Triggs, R. 2013. The five reasons why Android is killing Apple. [Online]

    Available at: http://www.androidauthority.com/five-reasons-android-killing-apple-234364/

    [Accessed 01 December 2015]

57. Tsang and Smith, 2008. YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems. In: Jajodia, S., et al. ed., *IFIP 20th World Computer Congress, IFIP SEC'08*, Milano, Italy, 7-10 September 2008.

58. United Nations, 2014. E-government survey 2014, Country report – Estonia. [Internet]

    Available at: http://unpan3.un.org/egovkb/en-us/Data/Country-Information/id/57-Estonia

    [Accessed 24 October 2015]

59. Van Puyvelde, D., n.d. Hybrid war – does it even exist? *NATO Review magazine.* [Online]

    Available at: http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm

    [Accessed 12 December 2015]

60. Vaks, T., State Information System Authority, 2014. *Overview of key findings in vital service providers penetration testing*. Vihula mõis, 28.-29. November 2014. (Unpublished report due to state security reasons).

Seminar agenda available at: http://infoyhiskond.eesti.ee/infouhiskonna-kursused-2014/paevakava

61. Wagner, G. 2015. *Panta Rhei conference in Luxembourg*. Discussion about IT Legacy related issues. (Personal communication, 7. October 2015).

62. Waseda University, 2015. 2015 Waseda – IAC International e-Government Ranking Survey. [Online]

    Available at: http://e-gov.waseda.ac.jp/pdf/2015_Waseda_IAC_E-Government_Press_Release.pdf

    [Accessed 12 October 2015]

Appendices

Appendix 1 – list of experts interviewed as part of qualitative study

No	Role
1	Estonian government architect, State Information System Authority
2	IT manager, Estonian road administration
3	Director General, Estonian road administration
4	IT project manager, Ministry of Social Affaires
5	Director General, Estonian Social Insurance Board
6	Head of Business Technology and IT, Eesti Energia AS
7	Head of IT architecture department, Eesti Energia AS
8	Deputy Director General, Estonian Tax and Customs Board
9	IT architect, Nortal AS
10	Software Development Project Manager, Estonian Unemployment Insurance Fund
11	E-services expert, owner of Ziraff
12	Head of Critical Information Infrastructure Unit, Estonian State Information System Authority
13	Cyber security and ISKE expert, Estonian State Information System Authority
14	IT system analyst and product owner, Avita publishing
15	Head of IT operations department, Eesti Energia AS
16	Head of Information Society Services Development Department, Ministry of Economic Affairs and Communication
17	Deputy chief Executive, New-Zealand government
18	Managing Director, Info-communications Development Authority of Singapore
19	Director-General, Directorate-General for Informatics (DG DIGIT), European Commission
20	System Architect, [private sector company]
21	IT manager, Estonian Ministry of Economic Affairs and Communications
22	Director, Centre of Registers and Information Systems
23	Head of Information Technology and data security unit, Ministry of Justice
24	Estonian government CIO, Ministry of Economic Affairs and Communications

Appendix 2 – overview of the questionnaires

No in Eng. / No in Est.	Question	Comment
Q1 / N/A	Country	
Q2 / Q1	You name	
Q3 / N/A	Your contact details in case of further questions (phone, e-mail, skype)	The goal of the question was to enable follow-ups to respondents. This option was especially important for further details about Q22 / Q16 and Q23 / Q17 – about existing guidelines used by organisations to fight against legacy. Since Estonian questionnaire was distributed personally through existing networks, there was no need to ask contact details again.
Q4 / N/A	Organisation that you work for	
Q4 / Q2	Your role / job title	In case of Estonian experts, the researcher was aware of in which organisations the experts were working.
Q6 / Q3	How many years of experience do you have in dealing with IT systems *(have participated in creating or maintaining IT systems from IT or business side, have participated in IT policy formulation or IT budgeting)*	Question was used to establish the level of expertise of the sample, the goal of the researcher was to include experts who have at least 5+ years of experience with IT systems
Q7 / Q4	Have you dealt with IT systems: *a. Only in private sector* *b. Only in public sector* *c. In both sectors*	The goal of a researcher was to include at least 50% of experts who have experience from both sectors, having thus a better understanding of the legacy issues in the public sector. It was important to include experts from private sector because majority of Estonian government IT systems are procured from the market, thus, the technical expertise is usually not in-house.
Q8 / Q5	At the moment you work in *a. public sector* *b. private sector*	See previous comment. The sector where the respondent works at was relevant to the researcher to be able to do correlation analysis should it be necessary.
Q9 / N/A	What is the approximate size of your government's IT budget in euros (including IT development and maintenance costs)? Explanation: I'm interested to find out estimated size of the budget not exact number. If	Q9, Q10 and Q11 in the English version of the questionnaire were added to get data about the approximate government IT budget sizes (including software development and maintenance) and find out whether there is a correlation between the average age if IT systems and budget sizes and proportions of maintenance cost.

	you don't know it then move on to the next questions.	Researcher recognised that there is a high chance that the respondents don't have detailed data available to give correct answers to Q9, Q10 and Q11. These three question were not added to the questionnaire for Estonian experts because the researcher already knows the answer to these questions.
Q10 / N/A	What is the ratio between maintenance and development costs of ICT (%)? *a. Maintenance cost is up to 30%* *b. Maintenance cost is 31-50%* *c. Maintenance cost is 51-70%* *d. Maintenance cost is over 70%* *e. We have no overview of the maintenance cost*	Question was added to find out whether there are correlations between the average age of government IT systems and estimated maintenance proportion.
Q11 / N/A	What is the lifespan of your important government IT systems? *a. mostly the systems are less than 5 years old* *b. mostly the systems are less than 10 years old* *c. mostly the systems are less than 15 years old* *d. mostly the systems are less than 20 years old* *e. mostly the systems are over 20+ years old* *f. I don't know*	This question was relevant to get comparative data about how severe is the IT legacy build-up in other countries governments who have had a longer experience in building government IT systems.
Q12 / Q6	Based on your experience – what are the main problems when dealing with legacy IT systems? *Please rate how often you have encountered the following problems when dealing with legacy systems.* • *10 predefined sub-choices were rated* • *respondents could also add answers as free text*	Researcher compiled a list of legacy related problems based on the text reviews and expert interviews performed during the pre-study. The goal of the question was to analyse how often these legacy related problems (legacy symptoms) emerge. Respondents were able to add additional answers as a free text to find out whether there are other important legacy symptoms / problems that did not emerge during the pre-study.
Q13 / Q7	Please, sort the following legacy symptoms based on	In addition to clarifying how often certain legacy symptoms reveal, the researcher found it important to

	their criticality in descending order *Explanation: based on your experience, rank the most critical legacy related problem (e.g. problems with system security) first and sort the rest of the symptoms based on their criticality in descending order.* • *10 predefined sub-choices were rated (same choices as in previous Q)*	also clarify, which of them are considered more critical than others by experts.
Q14 / Q8	Based on your practical experience – what have been the main reasons that prevent from actively dealing with legacy? Please rate how often in your opinion are following problems obstacles in actively taking steps to get rid of legacy. • *7 predefined sub-choices were rated* • *respondents could also add answers as free text*	Researcher compiled a list of legacy related problems based on the text reviews and expert interviews performed during the pre-study. The goal of this question was to clarify what stops from getting rid of legacy at the right time? Respondents were able to add additional answers as a free text to find out whether there are other important obstacles that did not emerge during the pre-study.
Q15 / Q9	In your opinion, what are the three most IMPORTANT and, in practice, most frequently occurring problems that impede taking steps to get rid of IT legacy?	The goal of the question was to determine what the experts see as the most common obstacles in fighting against IT legacy.
Q16 / Q10	Based on your practical experience - what have been the 3 main arguments to re-write a system? *Explanation: why the decision to initiate a rewrite project has been usually done?*	The goal of the question was to better understand what are the so called killer-arguments, that actually work as initiators of legacy rewrite projects.
Q17 / Q11	In your opinion – have the rewrite projects mostly paid off? Yes ____ No _____	The goal of the question was to determine whether expert find getting rid of IT legacy as purely actions that create cost or whether they see also an economical benefit in rewriting out-dated systems.
Q18 / Q12	Explain briefly your previous answer.	The goal was to get better understanding of why respondents think that the legacy re-write projects pay off / don't pay off.
Q19 / Q13	What have been the biggest lessons you have learned in dealing with legacy? What	The goal of the question was to find out what other important factors come to play when dealing with IT legacy, to find input about what other issues should be considered when compiling the No Legacy Policy.

	would you do differently next time?	
Q20 / Q14	In your opinion, what is the maximum reasonable lifetime of a critical public sector information system, considering the need to change processes, the speed of technological innovation, changes in cyber security and system resilience expectations etc.? Explanation: pick a lifetime in years when the usage of the system should stop because there is a high probability that the solution has turned into legacy (that means – new version of the system needs to be available already). a) 2-4 years b) 5-7 years c) 8-10 years d) 11-13 years e) 14-16 years f) 17+ years g) It is impossible to set the timeframe	The goal of the question was to determine whether the experts think it is possible to set a certain timeframe as a maximum reasonable lifetime of critical government information systems or not and if yes, then what would that timeframe be?
Q21 / Q15	If necessary, add explanation about your choice in the previous question	Researcher found it necessary to enable respondents to explain the choice they made to better understand the reasoning behind their choice.
Q22 / Q16	Is there a set of guidelines in your organisation, which help to avoid the build-up of IT legacy or to get rid of existing legacy systems? Yes ____ No _____	The goal of the question was to find if any guidelines are already used by organisations to knowingly fight against IT legacy build-up.
Q23 / Q17	In case such guidelines exist, please describe briefly the content and implementation principles of these.	It was important to gather that input for further analysis of what kind of guidelines the No Legacy Policy should include.
Q24 / Q18	In your opinion, is there a need for No Legacy Policy guidelines in the public sector (a set of guidelines that help to prolong the reasonable lifetime of IT systems and to get rid of systems that are turning into legacy at the right time)?	The goal of the question was to understand whether experts with extensive experience in the field find it necessary to have No Legacy Policy in place to fight against the build-up of IT legacy.

	Yes ____ No _____	
Q25 / Q19	In case there was a rule, that important, mission-critical IT systems should be rewritten in every 13 years, would the yearly IT budget of your organisation Explanation: try to estimate the change in IT-budget considering the fact that all changes will not be made at the same time, during the same year. a. stay the same, because you already comply to this rule b. increase by 15% c. increase by 16-30% d. increase by 31-50% e. increase over 50% f. decrease, because we would decrease unreasonable administration and maintenance costs	Based on expert interviews during the pre-study, the concern about the possible high cost of the No Legacy Policy was mentioned very often. So the goal of the question was to clarify how severe is the cost issue and could it potentially be the show-stopper or at least a huge obstacle to overcome when working out the No Legacy Policy?
Q26 / Q20	In your opinion, would implementing the rule that all important information systems should be rewritten in at least every 13 years help to decrease other process-related costs so much that it would justify the cost of IT investment? *Explanation: e.g. would regularly rewriting IT systems help to optimise other process related costs – reduce manual work and save personnel costs or reduce the time spent by a citizen enough to justify the IT investment cost. Please try to take into account the costs of both sides: service provider and service user.*	The goal of that question was to determine wheteh experts agree or disagree with the fact that if all the critical systems are rewritten in 13-year cycles then this would enable to decrease other process related costs to the extent of making the investment pay off. So even if overall IT costs increase, it helps to decrease the overall process related cost enough to justify the IT investment.
Q27 / Q21	In case you know someone else who I should contact to get input for the research or who should fill in this questionnaire, then please provide his / her contact details (name, phone, e-mail, short description of why his / her input would be valuable?).	The goal was to find additional experts who could respond to the questionnaire.

Q28 / Q22	In case you would like me to share the results of my research, please insert your e-mail address here	Researcher wanted to be able to express the gratitude for the input by experts by sharing the study report to them if they find the topic relevant.

Appendix 3 – questionnaire for Estonian experts

Remark: SurveyMonkey environment was used to collect response data.

***

Eksperdi küsimustik

Sissejuhatus

Käesolev küsimustik on osa uurimustööst, mille eesmärk on uurida infosüsteemide vananemisega (legacy'ks muutumisega) seonduvaid probleeme. Antud töö kontekstis pean *legacy* infosüsteemi all silmas infosüsteemi, mis ei vasta enam tegelikele ärivajadustele või on muul põhjusel muutunud organisatsioonis takistuseks ning mille kaasajastamine ei ole mingil põhjusel enam otstarbekas, vaid mõistlik on luua uus lahendus.

Töö eesmärk ongi selgitada, millised probleemid legacy infosüsteemidega kaasnevad ning kas on vajalik töötada välja poliitikasuunised (ing. k.: *No Legacy Policy*), mis aitavad avaliku sektori organisatsioonidel *legacy* tekkimise vastu võidelda ja/ või saada juhiseid ja toetavaid argumente juba tekkinud legacyst vabanemiseks. Uurimuse fookuses on eelkõige **olulised põhiinfosüsteemid**, mis on muutunud organisatsiooni toimimise seisukohast missioonikriitiliseks. Seega küsimustele vastates püüa mõelda oluliste põhiinfosüsteemide kontekstis.

Küsimustiku vahendusel püüan saada ka sisendeid selle kohta, mida need poliitikasuunised sisaldama peaksid.

Juhul, kui tead täiendavaid materjale või raamistikke, mille läbitöötamine on käesoleva uurimustöö teostamisel otstarbekas, siis edasta need aet.rahe@mkm.ee.

Küsimustik sisaldab 20 sisulist küsimust ning selle täitmine võtab aega kuni 20 minutit.

VASTAJA TAUST

Kuupäev: _____

1. **Sinu nimi**: _____
2. **Sinu tänane roll / ametinimetus:** _____
3. **Mitu aastat on Sul kogemus IT süsteemidega (osalenud IT lahenduste loomisel / täiendamisel IT või äri poole spetsialisti või juhina)**: _____
4. **Kas oled IT lahendustega kokku puutunud**
    a. ainult erasektori töötades
    b. ainult avalikus sektoris töötades
    c. töötades mõlemas sektoris

5. **Hetkel töötad**
    a. erasektoris
    b. avalikus sektoris

Küsimused legacy infosüsteemide kohta

Selgitus: Palun anna järgnevatele küsimustele vastus tuginedes enda praktilisele kogemusele legacyks muutunud infosüsteemidega töötamisel.

Kui Sa mõnele küsimusel ei oska hinnangut anda, siis jäta see vahele ning liigu edasi järgmise küsimuse juurde.

6. **Millised on Sinu kogemusele tuginedes peamised probleemid seoses Legacy infosüsteemiga?**

Märgi järgmiste valikute puhul, kui sageli oled legacy'ks muutunud infosüsteemide puhul kirjeldatud probleemiga kokku puutunud

Küsimus	**mitte kunagi**	**harva**	**aeg-ajalt**	**pigem sageli**	**väga sageli / alati**
#1 - Haldus- ja hoolduskulud on aja jooksul muutunud ebaproportsionaalselt suureks					
#2 - ärilised / seadusandlikud muudatused on toonud kaasa vajaduse protsesse muuta sellises ulatuses, et selle realiseerimine vanal platvormil on riskantsem ja kallim, kui uue lahenduse loomine					
#3 – Arhitektuuri keerukuse (seoste rohkus, spageti) tõttu ei ole mõistlik enam süsteemi täiendada, välditakse igasuguseid muudatusi *(täiendustega kaasnevad ennustamatud tagajärjed. Muudatusi välditakse, süsteem muutunud innovatsiooni piduriks)*					
#4 - Tekkis vendor lock-in probleem *(partneril puudus huvi arendamist jätkata või partner pakkus ebakvaliteetset teenust; lock-in võib olla kompetentsi põhine, intellektuaalse omandi põhine vmt.)*					
#5 - Tekkisid **probleemid turvalisusega**, mida ei ole võimalik olemasolevas infosüsteemis lahendada					
#6 - Tehniliselt aegunud platvorm tekitas probleeme *(tehniline lahendus on eksootiline ja puudub piisav pädevate partnerite valik, tehniline platvorm ei võimalda uute tehnoloogiate/ seadmete kasutuselevõttu, kadus tootjapoolne tugi)*					
#7 - **kasutamismustrites on olulisi kõrvalekaldeid**, kasutatakse **"abistavaid" vahendeid** *(kasutatakse hack'e, lisafaile, -tabeleid, protsessid osaliselt süsteemist välja viidud, infot talletatakse valedel väljadel kuna vajalikud väljad puuduvad, vmt)*					
#8 – puudub korrektne dokumentatsioon ja see tekitab lahenduse mõistmisel ja muudatuste mõjude analüüsimisel palju probleeme					
#9 - süsteemi **töökindlus ja töökiirus ei vasta enam kasutajate ootustele**					

(süsteemi töö katkeb sageli, töökiirus takistab oluliselt kasutajate tööd vmt)					
#10 – uued tehnoloogiad võimaldavad soodsamalt ja efektiivsemalt ärilisi vajadusi lahendada kuid nende rakendamiseks tuleb infosüsteem suures osas uuesti luua					
Muu (lisa ise legacyga seotud probleeme, millega oled praktikas kokku puutunud ning täpsusta kui sageli need on esinenud)					

7. **Järjesta alljärgnevad legacy sümptomid kriitilisuse järgi**

Selgitus: esimeseks märgi suurim probleem (näiteks probleemid turvalisusega), mis on praktikas kõige suuremaks legacyst tulenevaks takistuseks ning järjesta ülejäänud kriitilisuse järgi kahanevalt.

Legacy sümptom / probleem	**Märgi prioriteet 1, 2, 3, … (kasuta igat numbrit vaid 1 korra)**
#1 - kõrged **haldus ja hoolduskulud** legacy tõttu	
#2 - vajalik rakendada olulised **muudatused protsessides**, kuid legacy takistab	
#3 – **arhitektuuri keerukus** (**seoste rohkus, spageti)** takistab vajalike muudatuste tegemist	
#4 – **Vendor lock-in** probleem	
#5 – **probleemid turvalisusega**	
#6 – platvorm on **tehniliselt aegunud**	
#7 - **kasutamismustrites on olulisi kõrvalekaldeid, kasutusel „abivahendid“**	
#8 – **puudub korrektne dokumentatsioon**	
#9 – süsteemi **töökindlus ja töökiirus ei vasta ootustele**	
#10 – **uued tehnoloogiad** tagavad ärivajadused soodsamalt ja efektiivsemalt	

8. Mis on Sinu praktilisele kogemusele tuginedes olnud peamised probleemid, mis takistavad legacy'ga aktiivset tegelemist?

Selgitus: märgi järgmiste valikute puhul, kui sageli on üks või teine konkreetne probleem Sinu hinnangul takistuseks legacyst vabanemisel.

Küsimus	**mitte kunagi**	**harva**	**aeg-ajalt**	**pigem sageli**	**väga sageli/ alati**
#1 – Legacyst vabanemise vajadust **ei suudeta juhtkonnale põhjendada**, mistõttu ei leita õigel ajal piisavalt **finantsvahendeid**					
#2 – Ei hinnata piisavalt regulaarselt **infosüsteemi vastavust tegelikele muutunud ärivajadustele**, seetõttu ei märgata õigel ajal süsteemi asendamise vajadust					
#3 – Infosüsteemil **puudub omanik,** infosüsteemi ajakohasuse regulaarne **üle hindamine ei ole otseselt kellegi töö**					
#4 – Uue tarkvara loomist peetakse liiga riskantseks kuna kellelgi ei ole olemasolevast süsteemist ja äriprotsessidest täielikku ülevaadet					
#5 – Organisatsioonis **puudub kogemus/ piisav tehniline kompetents mahuka tarkvara ümber kirjutamise**					

tellimiseks ja seetõttu ei ole kedagi kes projekti algatada suudaks					
#6 – Kasutajad on süsteemiga harjunud (s.h. selle vigadega) ning **ei taha uut** / teistsugust lahendust					
#7 – eelmine / hiljutine infosüsteemi vahetamise kogemus oli nii raske / **valus**, seetõttu keegi ei julge uut vahetust alustada					
Muu (lisa ise praktikas esinenud legacy'st vabanemist takistanud asjaolu):					
Muu:					
Muu:					

9. **Sõnasta enda vaatest kolm OLULISIMAT, praktikas kõige sagedamini esinevat probleemi, mis on takistanud legacyst vabanemist.**

_____

_____

_____

10. **Mis on olnud Sinu praktikas kuni 3 peamist argumenti, miks hakati astuma samme legacy 'st vabanemiseks/ otsustati süsteem ümber kirjutada?**

_____

_____

_____

11. **Kas Sinu hinnangul on legacyst vabanemise projektid enamasti ära tasunud?**

    Jah ____ Ei _____

12. **Põhjenda lühidalt oma eelmist vastust.**

_____

_____

_____

13. **Mis olid suurimad õppetunnid, mida oled legacyga kokku puutudes õppinud? Mida teeksid edaspidi teisiti?**

_____

_____

_____

14. **Mis on Sinu hinnangul avaliku sektori kriitiliste infosüsteemide maksimaalne mõistlik eluiga arvestades äriprotsesside muudatuste vajadusi, tehnoloogia arengut, andmeturvet jm olulisi asjaolusid?**

Selgitus: vali selline ajaraam, mille möödudes hiljemalt tuleks infosüsteemi kasutamine lõpetada kuna suure tõenäosusega on lahendus muutunud legacyks (s.t. enne peab olema uus süsteem väljatöötatud).

a) 2-4 aastat
b) 5-7 aastat
c) 8-10 aastat
d) 11-13 aastat
e) 14-16 aastat
f) 17+ aastat
g) Sellist ajaraami ei ole võimalik paika panna

15. **Vajadusel lisa siia eelmise küsimuse vastuse valiku kohta selgitus:**

_____

_____

_____

16. **Kas Sinu organisatsioonis on kehtestatud suunised, mille eesmärk on vältida Legacy süsteemide tekkimist või vabaneda juba tekkinud legacy süsteemidest?**

Jah ____ Ei ____

17. **Kui Sinu organisatsioonis on legacyst vabanemise suunised rakendatud, siis palun kirjelda lühidalt nende sisu ja rakendamise põhimõtteid.**

_____

_____

_____

18. **Kas sinu hinnangul on avalikus sektoris vaja vaja No Legacy Policy't – juhiste kogumit, mis aitab pikendada infosüsteemide mõistlikku eluiga ja vabaneda vananevast infosüsteemist õigel ajal?**

Jah ____ Ei ____

19. **Juhul, kui kehtiks reegel, et olulisi infosüsteeme peab maksimaalselt 13 aastaste tsüklitena ümber kirjutama, siis kas kõhutunde järgi Sinu organisatsiooni iga-aastane IT eelarve**

Selgitus: püüa kulude hindamisel anda hinnang arvestusega, et legacyst vabanetakse jooksvalt ega tehta kõiki investeeringuid korraga, samal aastal.

a. jääks samaks kuna juba täidame seda reeglit
b. suureneks kuni 15 %
c. suureneks 16-30 %
d. Suureneks 31-50 %
e. Suureneks üle 50%
f. väheneks, kuna vähendame ebamõistlikke IT haldus- ja hoolduskulusid

20. **Kas Sinu hinnangul võimaldaks sellise kohustusliku oluliste infosüsteemide ümber kirjutamise reegli kehtestamine vähendada muid protsessidega seotud kulusid sedavõrd, et see õigustaks tehtavate IT investeeringute kulud?**

Selgitus: kas näiteks regulaarne IT süsteemi uuendamine aitaks vähendada käsitööd sedavõrd, et võimaldab säästa tööjõukuludelt või hoida kokku kodaniku ajakulu sedavõrd, et see kokkuhoid on suurem kui süsteemi arendamise kulu? Arvesta nii teenuse osutaja kui teenuse tarbija poolt tehtavaid kulusid.

_____

_____

_____

Lõpetuseks

Suur aitäh küsimustikule vastamise eest!

21. **Juhul, kui tead veel kedagi, kellega võiksin selle uurimuse raames veel ühendust võtta või kes võiks seda küsimustikku täita, siis palun lisa siia kontaktandmed (nimi, tel, e-mail, lühikirjeldus miks just see isik võiks sisendit anda?)**

_____

_____

_____

_____

22. **Juhul, kui soovid, et jagan Sulle hiljem oma uurimuse tulemusi, sisesta siia oma e-maili aadress:**

_____

Appendix 4 – questionnaire for foreign experts

Remark: SurveyMonkey environment was used to collect response data.

***

No Legacy Policy Study - Questionnaire for experts

Introduction

As Estonian ICT policy makers the department of State Information Systems of Estonian Ministry of Economic Affairs and Communications is conducting a study to find out whether governments need policy guidelines to avoid the build-up of ICT legacy and to get rid of the legacy that already exists at the right time.

In Estonian government we have reached an understanding that the digital dependencies of mission-critical processes are increasing in time and because over the years we have heavily invested into IT to automate processes, more and more legacy is starting to build up.

Build-up of legacy causes many problems and can turn into obstacle in innovating processes and keeping up with the emerging technologies, changes in user expectations and behaviours, bring along an increase of maintenance costs or cause security incidents. This realisation has been the main cause to initiate No Legacy Policy study with the aim to work out policy guidelines for Estonian public sector organisations.

With the current survey, the aims is to investigate what kind of problems other governments face in dealing with IT legacy and learn whether any specific measures have been implemented to fight against the build-up of IT legacy in the public sector or is there a need for guidelines to start taking these steps.

In this work, a ***legacy system*** means an IT system that is not in compliance with the actual business needs any more or has for other reasons turned into an obstacle for the organisation that needs to be wiped off and recreated because continuing to operate it is no longer reasonable.

Study focuses primarily on **important core information systems** that have become mission critical for the functioning of the organisation. Thus, when answering to this questionnaire, try also to think in the context of important / core IT systems.

The survey will also help to clarify what kind of policy guidelines NoLP should include.

In case you are aware of additional materials or frameworks that are related to our research topic, please send the information to aet.rahe@mkm.ee (with subject line: No Legacy Policy).

The questionnaire includes 26 substantive questions and filling it will take 20-25 minutes.

Thank you in advance for sharing your thoughts.

In case you would like to receive information on the results of the study, you can add your e-mail at the end of the study.

Aet Rahe

Head of State Information Systems Department

+372 5567 7997 | Skype: aetrah

www.mkm.ee | Harju 11, Tallinn 15072

Estonian Ministry of Economic Affairs and Communications

Respondents background

Date: _____

1. **Country:** _____
2. **Your Name**: _____
3. **Your contact details in case of further questions (phone, e-mail, skype):**

_____

_____

_____

4. **Organisation that you work for:** _____

_____

5. **Your role / job title:** _____
6. **How many years of experience do you have in dealing with IT systems** (have participated in creating or maintaining IT systems from IT or business side, have participated in IT policy formulation or IT budgeting)

_____

7. **Have you dealt with IT systems:**
   a. Only in private sector
   b. Only in public sector
   c. In both sectors
8. **At the moment you work in**
   a. public sector
   b. private sector

9. **What is the approximate size of your government's IT budget in euros (including IT development and maintenance costs)?**

Explanation: I'm interested to find out estimated size of the budget not exact number. If you don't know it then move on to the next questions.

_____

_____

_____

10. **What is the ratio between maintenance and development costs of ICT (%)?**

    a. Maintenance cost is up to 30%
    b. Maintenance cost is 31-50%
    c. Maintenance cost is 51-70%
    d. Maintenance cost is over 70%
    e. We have no overview of the maintenance cost

11. **What is the lifespan of your important government IT systems?**

    a. mostly the systems are less than 5 years old
    b. mostly the systems are less than 10 years old
    c. mostly the systems are less than 15 years old
    d. mostly the systems are less than 20 years old
    e. mostly the systems are over 20+ years old
    f. I don't know

Questions about legacy IT systems

Explanation: please give answers to the following questions based on your own practical experience.

In case you do not have an answer to some questions, please skip them and move on to next questions.

12. Based on your experience – what are the main problems when dealing with legacy IT systems?

Please rate how often you have encountered the following problems when dealing with legacy systems.

Question	never	rarely	from time-to-time	rather often	very often/ always
#1 – Administration and maintenance costs have become disproportionate over time					
#2 – Changes in business / legislation have entailed a need to **change processes** to such an extent that it is more expensive or risky to carry them out in the old system than to create a new one					
#3 – Architectural complexity (many interconnections, spaghetti) makes it unreasonable to update the old system, and, thus, all changes are avoided *(changes have unpredictable side-effects, avoiding changes turns system into innovation blocker)*					
#4 – A vendor lock-in problem has emerged *(the partner has no interest to continue supporting the system, or provides low quality service; lock-in can be competence or IP based)*					
#5 – Problems with the **security of the system** have emerged that are impossible or unreasonable to solve in the existing solution					
#6 – the **IT-Platform** has become **technically outdated** and it is causing problems *(the technical solution is exotic, there is limited choice of potential partners, platform prevents the uptake of new technologies or devices, loss of vendor support)*					
#7 – there are **significant deviations in usage patterns, many additional "helpful" tools** have been taken into use *(Users use hacks, additional files, -tables; the processes are partly outside the system, information is stored in wrong fields etc.)*					
#8 – **No appropriate documentation** exists about the system, making it difficult to understand the system and analyse the side-effects of changes					
#9 – The **reliability and responding speed** of the system no longer meet user expectations *(frequent interruptions of work, the slowness of the system substantially impedes the work of end-users)*					

#10 – New technologies enable to meet business needs in a more cost-effective and efficient way, but to implement them the old platform needs to be replaced					
Other (add any legacy related problems you have encountered in your practice and specify how frequently it occurred)					
Other:					
Other:					

13. **Please, sort the following legacy symptoms based on their criticality in descending order**

Explanation: based on your experience, rank the most critical legacy related problem (e.g. problems with system security) first and sort the rest of the symptoms based on their criticality in descending order.

Legacy symptom / problem	**Set the priority of the symptom 1, 2, 3, … (use each number only once)**
#1 – **Administration and maintenance costs** have become disproportionate over time	
#2 – Need to **change business processes,** but legacy impedes	
#3 – **Architectural complexity** (many interconnections, spaghetti) makes it unreasonable to update the old system	
#4 **– Vendor lock-in** problem	
#5 – Problems with the **security of the system**	
#6 **– The platform is technically outdated**	
#7 – There are **significant deviations in usage patterns, many additional "helpful" tools** are in use	
#8 – **No appropriate documentation exists**	
#9 – The **reliability and responding speed** of the system no longer meet user expectations	
#10 – **New technologies enable to meet business needs in a more cost effective and efficient way**, but to implement them the old platform needs to be replaced	

14. Based on your practical experience – what have been the main reasons that prevent from actively dealing with legacy?

Please rate how often in your opinion are following problems obstacles in actively taking steps to get rid of legacy.

Question	**never**	**rarely**	**from time-to-time**	**rather often**	**very often/ always**
#1 – No one is able **to justify the need** to replace the system **to the management**, thus there is a lack of **financial resources** available at the right time					
#2 – The system **is not regularly re-evaluated** to find out **whether it is still in**					

sync with changed business needs and thus no one notices the need for a rewrite at the right time					
#3 – Information system has **no clear owner**, so it is **nobody's direct responsibility to regularly re-evaluate the system**					
#4 – Recreating the system is considered too risky because nobody has a clear / comprehensive overview of the current system and business processes					
#5 – The organisation **lacks experience/ technical competence to procure the rewrite of a big information system**, so there is no one who would be able to initiate the process					
#6 – Users are used to the old system (including its mistakes) and they **do not want new** / different solution					
#7 – previous / **recent IT system exchange experience was so difficult** / painful, so **no one dares to take on a new project** to replace old system					
Other (Describe an obstacle that you have encountered in getting rid of legacy?)					
Other:					
Other:					

15. **In your opinion, what are the three most IMPORTANT and, in practice, most frequently occurring problems that impede taking steps to get rid of IT legacy?**

_____

_____

_____

16. **Based on your practical experience - what have been the 3 main arguments to re-write a system?**
Explanation: why the decision to initiate a rewrite project has been usually done?

_____

_____

_____

17. **In your opinion – have the rewrite projects mostly paid off?**
Yes ____ No _____

18. **Explain briefly your previous answer.**

_____

_____

_____

19. **What have been the biggest lessons you have learned in dealing with legacy? What would you do differently next time?**

_____

_____

_____

20. **In your opinion, what is the maximum reasonable lifetime of a critical public sector information system, considering the need to change processes, the speed of technological innovation, changes in cyber security and system resilience expectations etc.?**

Explanation: pick a lifetime in years when the usage of the system should stop because there is a high probability that the solution has turned into legacy (that means – new version of the system needs to be available already).

h) 2-4 years
i) 5-7 years
j) 8-10 years
k) 11-13 years
l) 14-16 years
m) 17+ years
n) It is impossible to set the timeframe

21. **If necessary, add explanation about your choice in the previous question:**

_____

_____

_____

22. **Is there a set of guidelines in your organisation, which help to avoid the build-up of IT legacy or to get rid of existing legacy systems?**

Yes ____ No _____

23. **In case such guidelines exist, please describe briefly the content and implementation principles of these.**

_____

_____

_____

24. **In your opinion, is there a need for No Legacy Policy guidelines in the public sector (a set of guidelines that help to prolong the reasonable lifetime of IT systems and to get rid of systems that are turning into legacy at the right time)?**

    Yes ____ No _____

25. **In case there was a rule, that important, mission-critical IT systems should be rewritten in every 13 years, would the yearly IT budget of your organisation**

Explanation: try to estimate the change in IT-budget considering the fact that all changes will not be made at the same time, during the same year.

g. stay the same, because you already comply to this rule
h. increase by 15%
i. increase by 16-30%
j. increase by 31-50%
k. increase over 50%
l. decrease, because we would decrease unreasonable administration and maintenance costs

26. **In your opinion, would implementing the rule that all important information systems should be rewritten in at least every 13 years help to decrease other process-related costs so much that it would justify the cost of IT investment?**

Explanation: e.g. would regularly rewriting IT systems help to optimise other process related costs – reduce manual work and save personnel costs or reduce the time spent by a citizen enough to justify the IT investment cost. Please try to take into account the costs of both sides: service provider and service user.

_____

_____

_____

Finally

Thank you very much for your contribution!

27. **In case you know someone else who I should contact to get input for the research or who should fill in this questionnaire, then please provide his / her contact details (name, phone, e-mail, short description of why his / her input would be valuable?).**

_____

_____

_____

28. **In case you would like me to share the results of my research, please insert your e-mail address here: _____**