MESG

MESTRADO EM ENGENHARIA DE SERVIÇOS E GESTÃO

Application of Lean methodologies in Information Security processes improvement

Francisco Ribeiro Pereira da Silva

Master Thesis

Supervisor at FEUP: Prof. António Carvalho Brito

Supervisor at Strongstep: Duarte Gomes

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

2021-06-18

Abstract

Information Security is a subject that has been gaining a lot of attention lately. Hackers' methods for breaking into systems are getting more sophisticated day by day, while organisations' dependence on information and information technology keeps growing. The processes which allow companies to improve their Information Security performance is now heavily related to their organisational success, since Information Security incidents may affect their businesses in all levels. While companies' requirements for Information Security keep growing, the market for Information Security consultancy services is also suffering heavy changes. Being filled with SMBs that strive to keep up with the changes, the circumstances of this market present a serious challenge to these SMBs. Since their customers' requirements on Information Security consultancy services are becoming more demanding, these organisations will have to present serious time, cost and efficiency gains, so that their services can meet both their customers' expectations and the requirements of the market.

To understand how SMB's address services of this nature, the analysis of several publications was combined with practical field work together with an organisation that operates in this market. The goal was to understand all the stages that both organisations go through when such services are provided, as to figure out where these type of consultancy services can be improved so that both the service provider and the organisation who seeks to improve their Information Security can benefit from the relationship.

As a result, four approaches were developed. In first place, an approach to guide organisations on applying the principle of standardised work to service processes. Next, a PDCA-based approach to handle customer feedback, aiming at generic process improvement. Third, a methodology to tackle non-value-added activities in knowledge-based processes. Lastly, an approach to optimise consultation service process documentation.

These approaches are based upon principles of lean thinking and some of its methodologies. Their purpose is to lead small and medium enterprises that provide consultancy services related to Information Security to be more efficient, so that their customers can have more robust Information Security systems, thus ready to meet market and business requirements quicker and more accurately.

Acknowledgments

Throughout this semester, many people have had an immense importance in the development of this project.

Firstly, I would like to thank my family for the constant support and dedication to my studies and to providing me all necessary conditions to successfully accomplish this goal of mine.

Second, I would like to thank Strongstep for having welcomed me in their family. The wonderful environment of this organisation made my journey much smoother and much more exciting than I expected.

In third place, I would like to thank my supervisor at Strongstep, Duarte, for getting involved and being so dedicated to my project. I could not have asked for a better person to fill your role in this journey.

Lastly, I would like to thank my supervisor at FEUP, professor António, for simultaneously giving me a comfortable level of autonomy and guidance. You gave me space to work by myself, which is something I value a lot, while still being present and providing me your feedback as often as needed.

Table of Contents

List of Figures

List of abbreviations

1. IS – Information Security
2. SMB – Small and Medium-sized Business
3. IMS – Information Management Systems
4. ISMS – Information Security Management Systems
5. DSR – Design Science Research
6. ISA – Information Security Awareness
7. PM – Project Management

1 Introduction

Information is one of the most important intangible assets of any organisation. We live in a world that keeps getting more and more digital day by day, meaning that more and more information is kept on everyone's hands, either in their personal or professional environments. Nowadays, digitalising business partitions may be seen both as a *must* and as a trend. Markets demand companies to be more efficient, whereas companies look forward to digitalising services and processes to be at the vanguard of efficiency and innovation. However, both information and people may be just as vulnerable in the digital reality as they are in the physical world (or even more).

In the digital world, information is exposed to two main dangers (mirrored from the real world): people, and people. In the first case, people are a risk to their own security (and their company's security, from a business point of view) as their lack of awareness, lack of ability or simple carelessness threatens the integrity of any information they may handle. In the latter, people who make money out of exploiting security breaches or are simply malicious enough to do so may shred a corporation's business by acquiring and illegally sharing its information.

Two conclusions can be drawn from the previous paragraph: companies face information security (IS) challenges related to their employees' jobs and behaviour, but also related to their cybersecurity development. This means that to sustain a business in an ever-growing digital reality, companies must prioritize their Information Security strategies and treat information security as a core aspect of whatever business they may be into.

1.1 Project context and motivation

Information security overview

In 1998, Von Solms stated that the aim of information security is to ensure business continuity, using incident prevention and impact mitigation to minimize business damage caused by these incidents. Additionally, the author recognises that as time goes by, there is an increased tendency for IS threats to become more complex, more universal, and to surge in different forms. To Whitman and Mattord (2009), Information security can be defined as "the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information" (Whitman and Mattord, 2009).

Nowadays, the information security process goes beyond the traditional technical dimension. Following Van Niekerk and Von Solms' words (2013), this happened due to the rapid increase in the use of computers and networks (Von Solms, Van Niekerk, 2013) which seems to continue growing at a faster pace day by day. Quoting the beforementioned authors, the complexity in handling Information Security roots to the fact that "the process of information security may require the use of certain products but is not something that can be bought off the shelf." (Von Solms, Van Niekerk, 2013)

ISO 27001: Standardising Information Security Management

With the ever-growing importance of technology not only in corporations but in society, the need for proper information security measures, guidelines and management systems has been reinforced.

In the case of information and information systems protection, international standards such as ISO 27001 have surged. Georg Disterer (2013) states that these standards "provide control objectives, specific controls, requirements and guidelines, with which the company can achieve adequate information security" (Georg Disterer, 2013). By doing so, this international standard enables a company to present itself as having been certified against the standard, meaning that external entities can perceive information security in the said organisation as being managed and applied according to a standard which is globally recognized (Georg Disterer, 2013). By being ISO 27001 certified, "a company verifies the fulfilment of well-known and accepted security standards and thus promotes customers' trust" (Georg Disterer, 2013).

Lean thinking overview

Dating back to the 90's when Womack, Jones, and Roos published a book entitled *The Machine That Changed the World: The Story of Lean Production*, the concept of lean thinking was first explored (Poppendieck, 2011). Based on a manufacturing environment story on how Henry Ford standardised car components and production, the book shows how a more rudimentary version of what we now call lean allowed Ford to "have low skilled workers and specialized machines (…) make cheap cars for the masses" (Poppendieck, 2011) by combining three major indirect labour components: production planning, engineering, and management (Poppendieck, 2011).

Poppendieck (2011) states that "lean principles have proven not only to be universal, but to be universally successful at improving results" (Poppendieck, 2011). Regardless of being recognised as a concept or set of methodologies that may not suit every organisation or every type of use case, it is quite common nowadays to hear people talk on how lean thinking is revolutionising their workplace and business environment.

Additionally to being universally recognised as a solid and revolutionary approach, it is also quite evident that lean is seen by many as a trend. This may be interpreted as being good since lean's benefits can be considerable when properly applied in a reality where it fits (or which adapted to it). On the other hand, the *trendy* side of lean may lead many enterprises which do not suit the concept or in which the lean transition is led by people who do not properly understand and apply it to see lean as a "one size fits all" problem solving concept.

Project framing

According to IDG's (International Data Group, Inc.) 2016 *Data & Analytics Survey*, the average SMB (Small and Medium-sized Businesses) manages 47.81 TB of data (IDG, 2016). If we consider that most SMB's have a small number of workers who are individually responsible for a portion of this information, we can conclude that these individuals use, handle, and manage large amounts of files and data. Therefore, two main factors must be highlighted.

In first place, information is vulnerable to the workers' level of awareness regarding Information Security. Some people do not understand the value of information assets, while others simply do not care enough to consider the risks involved. Second, the way a company's processes are handled may or may not reflect its concerns regarding Information Security and, in case it does, the scope of its concerns may not be broad enough. Both these aspects boost the importance of having a well thought and developed IS strategy to minimize the amount of IS breaches and their impact in the organisation's success. This is especially relevant in the

reality of SMBs' as their dimension as a company often leads them to ignoring aspects which do not seem to be directly related to the growth of the business.

Lean thinking and its related methodologies have been widely studied and applied to diverse types of businesses, being currently seen as one of the "ways to go" to improve SMBs' value proposition delivery and process performance. In 2007, Hicks highlighted "the relative lack of overall principles or frameworks for improving information management per se and the overall information management infrastructure including people, practices, processes, systems and the information itself" (Hicks, 2007). Following the author's words, the lack of principles to support the development of Information Management Systems (IMS) reinforces the value of further lean approaches to the subject (Hicks, 2007).

Understanding how lean thinking and its concepts can be tailored to the scope of IS, improving existing processes and guiding the development of new ones will be the one of the exploration areas in the present work.

1.2 Problem description

The hereby developed study was conducted together with a software engineering consultancy company, which is described further in this report. Using this organisation's corporate environment, the study started by analysing the internal process the company follows when providing ISO 27001 consultancy services to their clients. This analysis was conducted with the purpose of identifying pain points, gaps, and general improvement opportunities, following the activities and methodology further described. Having these identified, the goal of the study was to address the opportunities with a lean thinking mindset, which could allow improvements to be drawn using lean related concepts and/or methodologies.

Taking this into account, a set of research questions was developed, to limit the scope of the project and drive its development.

1.3 Research questions

Considering what was previously stated regarding this project, a set of research questions was defined to guide the development of the study. For each research question, a brief overview on how each question was planned to be answered is also presented.

The research questions were structured as following:

1. How are Information Security consultancy processes currently handled in SMBs?
2. How can lean thinking and its related concepts and methodologies help SMBs improve their Information Security consultancy processes?

As for the first research question, the topic is explored under two distinct perspectives. In first place, the literature review analyses the current state of art of Information Security and other related and relevant topics. Following this theoretical approach, the question is then addressed in a more practical way, using the organisation with whom the project was developed as a single case study. Here, the reality of this SMB serves as a practical example of how Information Security processes are handled in these companies.

Next, the second question is addressed through an extensive combination of theoretical study and practical collection of feedback and process analysis. Using the literature review as

theoretical foundation, the practical analysis of current process state and the identification of improvement opportunities, this question was set to be answered through studying the beforementioned organisation's corporate environment and implementing the developed improvement proposals.

1.4 Report outline

Starting by the introduction, context for this project is given. Here, the main topics related to the subject are slightly introduced as to motivate the purpose of this study. Additionally, the problem that originated this project is briefly introduced, wrapping up with an introduction to its development and the research questions to be answered by the end of this thesis.

Next, the state of the art of the subject and its related topics is presented in the form of an extensive literature review. Beginning by exploring the current knowledge base on Information Security as main topic, the literature review then progresses by analysing related subjects such as Information Security Awareness, Lean Management, and Information Security standards compliance. This analysis aims at presenting the reader the most relevant insights that could be found in the currently available literature regarding the major topics that cross barriers with the scope of the project.

Following the literature review, the characterisation of the problem which originated this study is explored. At first, a brief introduction on the company which proposed the project is provided. Then, the proposal is more deeply explored, including some characteristics of the proposal itself, improvement opportunities which have been identified within the scope of the project, and an exploration stage which explains how these improvement opportunities have been identified, evaluated, and assessed. Going into further detail on how the project has been approached and the problems assessed, the work methodology regarding this thesis is presented. A brief introduction on existing methodologies is followed by an exploration of the methodology used for the purpose of this work, finishing up with a few practical concerns regarding the methodology itself.

In fifth place, more concrete study results are presented. Here, proposed solutions for the identified improvement opportunities and issues are addressed, connecting the research questions to the study findings which allow these questions to be answered. For each of the initially identified improvement opportunities, a lean-based approach was developed to help the case study company properly assess these issues. The proposed methodologies were developed having in mind the corporate environment of the case study organisation, but have been developed, explored and presented in such way that they may prove to be useful for similar organisations. Since all the developed methodologies are based upon lean thinking and its related tools, they are highly flexible and have a broad enough scope so that they can be used both theoretically and practically by other interested parties.

Finally, project conclusions are presented, including an assessment of the writer's expectations for future research in this field of study, followed by references to all used articles, journals, websites, tools, books (among others) and annexes regarding additional relevant information.

2 Literature Review

2.1 Information Security

According to Ashenden (2008), information security is increasingly focusing on protecting all sorts of information across organisations (Ashenden, 2008). In the author's words, it "aims to deliver real business benefits now by both protecting and yet facilitating the controlled sharing of information and managing the associated risks across a changing threat environment." (Ashenden, 2008).

Based on their publication, Von Solms and Van Niekerk (2013) highlight the fact that information security should start off by being perceived as a process, instead of a technology or product (Von Solms, Van Niekerk, 2013). The same authors connect the expansion of information security beyond the technical dimension with the growing increase in the use of networks and computers (Von Solms, Van Niekerk, 2013). While ensuring the existence of proper Information Security Management Systems (ISMS), certain products may be used for their establishment and maintenance; however, there is not a "one size fits all" solution for information security in corporations (Von Solms, Van Niekerk, 2013).

Solms and Niekerk (2013) also generalised that security regards protecting assets from threats which aim at exploring certain vulnerabilities of the said assets (Von Solms and Van Niekerk, 2013). Following Von Solms' developments on his three-wave information security development model (Von Solms, 2006), the author later recognised that a fourth wave should fit in the scope of an IS definition. This resulted in his four-wave information security development model to include not only the previously studied technical, management and institutional waves (Von Solms, 2006) but also the information security governance wave (Von Solms, 2006).

Whitman and Mattord (2009) associated information security with "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman, Mattord, 2009). While recognising that information security does not have a proper "one sentence" definition, Zafar and Clark (2009) affirm that its nature can be seen as "technical, behavioural, managerial, philosophical, and/or organizational" (Zafar and Clark, 2009). Regardless of presenting several contributes to broadly define information security components, Zafar and Clark (2009) highlight that information security research is not following network environment growth at a fast enough pace, identifying the lack of scientific contributions in the field of study (Zafar and Clark, 2009). Ashenden (2008) also mentions that a lack of information security knowledge base is often realised, while business environments keep changing and getting more digital at an increasingly fast rate, together with the demand for connectivity and technology flexibility (Ashenden, 2008).

In 2004, Cavusoglu *et. al* conducted a study which intended to evaluate how a firm's market value would be affected by making public that a certain security breach had taken place (Cavusoglu et al., 2004). As a result of the study, it was concluded that in average, the involved firms suffered a 2.1 percent loss in market value within the two days which followed the announcement (Cavusoglu et al., 2004). Simultaneously, the authors recognize a relationship between security breach disclosure and security developers market value,

suggesting that regarding information security breaches, one company's loss may represent another's gain (Cavusoglu et al., 2004). Further developments on the economic impact of information security and its development can be found in Anderson (2001) and Baker et al. (2011).

A 2011 data breach report explored several components of security breaches by analysing hundreds of data compromise occurrences. Regarding their origin, the study presents that 92% of the breaches were originated by external agents (+22% than in the previous year's report), while only 17% of all breaches involved corporation insiders (Baker et al., 2011). When it comes to the root of these incidents, growth tendency was identified in breaches which involved hacking (50%) and incorporated malware (49%), among others (Baker et al., 2011). Bridging to the human aspects in information security, the same report highlighted that not only 83% of the victims in the studied incidents were targets of opportunity, but also that 92% of the attacks were not of difficult nature (Baker et al., 2011). Motivating the purpose of the hereby developed project, it is also stated that 97% of the analysed security breaches could easily be avoided without any relevant complexity or financial cost (Baker et al., 2011), which strengthens the importance of information security systems and awareness in any modern corporation.

2.2 Behavioural Information Security and Information Security Awareness

In 2003, Mitnick and Simon wrote that "the human factor is truly security's weakest link" (Mitnick, Simon, 2003). Security is said to be an illusion with consequences that are of increased relevance when one aspect of human nature comes into play: ignorance (Mitnick, Simon, 2003). Following Ashenden's (2008) line of thought, the growing tendency for more flat organisational environments is turning risk and trust-based decision making to a personal level, meaning that every individual in an organisation could potentially represent a considerable threat to its data security (Ashenden, 2008).

According to Crossler et al. (2013), information security research is progressing throughout the years. However, the authors state that the focus of information security research has been on the technical dimension rather than the human dimension (Crossler et al., 2013). Additionally, it is highlighted that the human user within a corporation is the main weakness of information security assets and vulnerability in their protection (Crossler et al., 2013). This opens doors for an emerging study field named Behavioural InfoSec, which deals with challenges such as "separating insider deviant behavior from insider misbehavior, approaches to understanding hackers, improving information security compliance, cross-cultural Behavioral InfoSec research, and data collection and measurement issues in Behavioral InfoSec research." (Crossler et al., 2013). Regarding the Behavioral InfoSec study field, the author states that albeit an increasing number of studies are being published, a lot is still yet to be discovered (Crossler et. al, 2013).

In 2011, Baker et al. recognised that there is a huge variety of ways in which an organisation insider can cause or contribute to information security incidents (Baker et al., 2011). Plus, a three-rank classification for insider behaviour is applied: there are people who act deliberately with malice, people who act inappropriately with no malicious intentions, and those who act unintentionally and non-maliciously (Baker et al., 2011). In this same study, it was concluded that only 1% of the analysed insider security breaches where unintentional (without malice),

6% were due to inappropriate behaviour (with no malicious intentions) and 93% resulted from deliberate (and maliciously driven) action (Baker et. al, 2011).

A 2017 study on *Individual differences and Information Security Awareness* defined information security awareness as "individuals' knowledge of what policies and procedures they should follow, their understanding of why they should adhere to them (their attitude) and what they actually do (their behaviour)" (McCormac et al., 2017). As stated by the authors, a method named Human Aspects of Information Security Questionnaire (HAIS-Q) can be used to measure such awareness (McCormac et al., 2017). This questionnaire details seven focus areas which are said to be crucial for information security: "internet use, email use, social media use, password management, incident reporting, information handling and mobile computing" (McCormac et al., 2017). Additionally, it is said that during the 2014/15 financial year, a 38% increase in reported security incidents was measured (McCormac et al., 2017). Contradicting what was hereby previously stated regarding the origin of these incidents, McCormac et al. (2017) affirm that security incidents originated externally were by then outnumbered by internal security breach occurrences (McCormac et al., 2017).

Information security awareness (ISA) aims at evaluating the "extent to which an employee understands the importance and implications of InfoSec policies, rules and guide- lines, and the extent to which they behave in accordance with these policies, rules and guidelines" (Kruger and Kearney, 2006; McCormac et al., 2017). Findings indicate that 34% of security incidents happen because of current employees' behaviour (Pricewaterhouse Coopers, 2015; McCormac et al., 2017). McCormac et al. (2017) presented a global overview of these conclusions, stating that there is a direct relationship between an employee's information security policy and procedure knowledge and their behaviour towards these (McCormac et al., 2017).

Studies were developed around a model named *The Big Five personality model* (Shropshire, Warkentin, Johnston and Schmidt, 2006). This model approaches five different aspects of human nature: neuroticism, extraversion, openness, agreeableness, and conscientiousness (Costa & McCrae, 1992; John & Srivastava, 1999; McCormac et al., 2017). Research based on models such as the beforementioned one suggest that less workplace incidents are associated with people who are more conscientiousness and agreeable (Cellar et al., 2001; McCormac et al., 2017). Additionally, other authors state that personality variability (Heinstrom, 2003; Stankov, Boyle and Cattell, 1995; McCormac et al., 2017), demographic variability (Pattinson et al. 2015; McCormac et al., 2017) and risk-taking propensity (McCormac et al., 2017) are some of the human aspects that most heavily impact information security awareness.

According to Ashenden (2008), information security management is a human challenge (Ashenden, 2008). This happens since organisations when dealing with an individual are forced to deal with two identities at a time: the personal and social identity which they as humans possess, and the identity they are attributed by their role (Ashenden, 2008). As time goes by, information security and its associated management systems depend less on the traditional process and technical dimensions and more on people (Ashenden, 2008). The author attributes part of the fault of human-based security issues to information security managers, as she argues that they "not often engage with end users to try and understand how they perceive Information Security. Instead, they rely on how they think end users see Information Security" (Ashenden, 2008).

2.3 ISO 27001 and Information Security standards compliance

Following the growth in the popularity and relevance of information technology, an increasing need for information security control systems can be verified (Disterer, 2013). As defined by ISO (2013), "ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization" (ISO, 2013). In Disterer's (2013) words, these standards provide "control objectives, specific controls, requirements and guidelines, with which the company can achieve adequate information security" (Disterer, 2013). Additionally, the author states that by doing so, the standard allows companies to document their information security as being developed, applied, and managed according to a standard which is globally recognised (Disterer, 2013). According to Ashenden (2008), this standard is frequently implemented in business environments to ensure that information security issues and vulnerabilities are handled in an auditable, repeatable, and consistent way (Ashenden, 2008).

Boehmer (2016) stated that the ISO 27001 certification picks up the information security processes which are of critical nature and ensures that they are handled in an unordinary way by going through an ISO 27001 based rigorous risk analysis (Boehmer, 2016). This will allow a company to promote their customers' trust by exhibiting the certification under these internationally accepted security standards (Disterer, 2013). Ashenden (2008) concluded that the beforementioned factors and the certification itself would offer "confidence to internal and external stakeholders that security is being effectively addressed" (Ashenden, 2008). According to Disterer (2013) and ISO (2009), the ISO 27 K family of standards is decomposed as following (Figure 1):

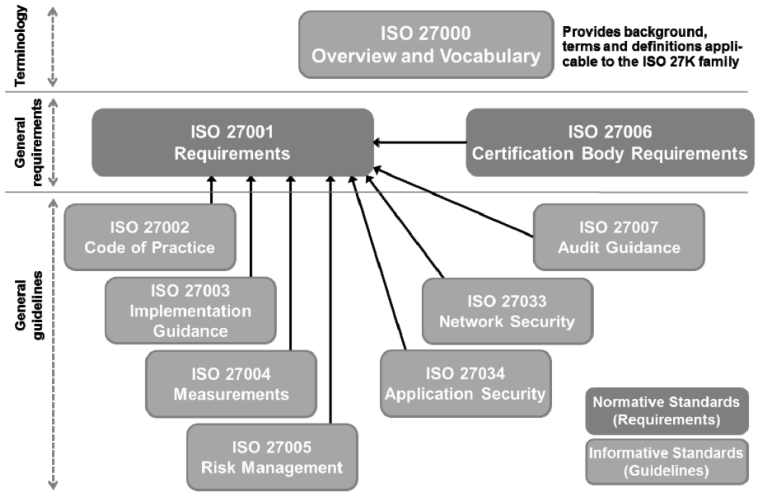

Figure 1 - Interrelations within the ISO 27 K family of standards. From Disterer (2013) based on ISO (2009).

2.4 Lean thinking

In 1990, a book named *The Machine That Changed the World: The Story of Lean Production* was published (Womack et al., 1990). Here, the authors first explored lean thinking as a management philosophy (Hicks, 2007). The book aimed at deconstructing and analysing the Toyota Production System (TPS), based on the Japanese car manufacturers' work practices and philosophy (Hicks, 2007). Later in 1996, Womack and Jones defined lean under five different lean principles (Womack and Jones, 1996):

1. Specify value – Value definition begins from the end customer.
2. Identify value streams – Which steps are necessary to get the final product on the customer's hands?
3. Flow – Value creating steps should flow.
4. Pull – Production should be pulled from customers' demand.
5. Pursue perfection – Reducing waste (time, cost, space, etc.) is a never-ending process.

Hicks (2007) identified the main techniques which are used to ensure a proper organisational lean transformation (Hicks, 2007): Kaizen (Imai, 1986), SMED (Shingo, 1985), Six Sigma (Pyzdek, 2003), value stream mapping (Hines & Rich, 1997) and the five 'S's (Warwood & Knowles, 2004). However, Hicks (2007) highlighted that whereas many lean techniques and methodologies have surged and even become mainstream, "it is the fundamental understanding of waste that is critical to successful lean transformation." (Hicks, 2007).

The lean philosophy heavily relies on identifying waste and developing methods to eliminate this waste (Hicks, 2007). Based on a former Toyota executive, Womack and Jones (1996) adapted seven types of waste which they claimed that can be found in every process (Womack and Jones, 1996; Ohno, 1988):

1. Transportation – unnecessary movement of parts which are work in progress (WIP).
2. Inventory – products waiting to be used or processed.
3. Motion – unnecessary steps taken by employees
4. Waiting – inactivity of products/processes due to upstream delays
5. Over-Processing – additional operations which are necessary due to other wastes
6. Over-Production – producing/processing products when the end customer or the upstream activities do not require these
7. Defects – production which does not meet defined standards

Lean thinking is increasingly being applied to all sorts of processes and organisational environments, allowing companies to identify improvement gaps and implement these improvements (Hicks, 2007). To sum this up, Hicks (2007) stated that "it is arguable that the principles of lean thinking and in particular the removal of waste and pursuit of perfection can be applied to any system where product flows to meet the demand of the customer, user or consumer" (Hicks, 2007).

2.5 Lean in Information Management

In 2007, Hicks deeply explored how lean can be framed and adapted to the reality of information security management. In this publication, he stated that "information management can be considered to involve adding value to information by virtue of how it is organised, visualised and represented; and enabling information (value) to flow to the end-user (customer) through the processes of exchange, sharing and collaboration" (Hicks, 2007). Further ahead, the author states that even though lean has the potential to enhance and improve information management systems, the lack in understanding how the concepts of waste and value fit the reality of information management is often a barrier to its proper application (Hicks, 2007). From a different point of view, Poppendieck (2011) has explored how lean thinking can be adapted and applied under the context of software development.

Within the context of information management, Hicks (2007) identified and characterised four different causes of waste (Hicks, 2007):

1. Information that cannot flow because it has not been generated, a process is broken, or a critical process is unavailable (Hicks, 2007).

2. Information is unable to flow because it cannot be identified, and flow activated or shared processes are incompatible (Hicks, 2007).

3. Excessive information is generated and maintained or excessive information flows, and therefore, the most appropriate and accurate information cannot be easily identified (Hicks, 2007).

4. Inaccurate information flows resulting in inappropriate downstream activities, corrective action or verification (Hicks, 2007).

Applying lean to information management, value is defined as the result of the critical activities which are performed under the scope of information and information systems (Hicks, 2007). Value streams are said to be dictated by the flow of processes and work activities which result in information being presented to its consumer, therefore highlighting the need for proper integration and automation of processes. (Hicks, 2007). The principle of flow in information management seeks to ensure that "information flows efficiently and that the most valuable (appropriate, accurate and up-to-date) information flow" (Hicks, 2007); to make this happen, the author says it is mandatory that information is available as soon as it surges, regardless of the source (Hicks, 2007).

Lastly, two of the most important lean principles can be applied to information management in a very similar way as they have traditionally been applied to manufacturing industries. Regarding the *pull* principle, it is said that end-user demand for information and functionality should be the main drivers of development (Hicks, 2007). Next, the continuous improvement logic is applied through "regular reviews of the information management system, all associated infrastructure and processes" (Hicks, 2007).

Although not every traditional lean concept or principle may be applied or easily identifiable within the context of information management, it is argued that the major principles which guide lean as a philosophy may serve well to support information management systems development and maintenance (Hicks, 2007).

3 Case study analysis

In this chapter, details regarding the single case study that was conducted during this project are presented. First, some information about the company which this work was developed with is given, followed by a brief description of the scope of the case study. Then, the problem under analysis is characterised and the improvement opportunities which were identified together with the company are listed. This chapter wraps up with an "Exploration" section, where details are given regarding how the problem has been assessed and how the improvement opportunities were set to be approached.

3.1 Company details and context

Strongstep is a software engineering focused company that aims at improving their customers' development performance in terms of software quality. In larger scale, Strongstep works to be a global reference in the software quality industry through years of experience and its team's competences and dedication.

The company's main activity regards improving software development projects and processes through implementing practices and policies that address not only projects from a technical point of view, but also people. The goal of these projects can range from simply helping the client organisation become more efficient, achieve higher productivity, and deliver higher quality products/services, to preparing these organisations for obtaining international certification such as ISO 27001.

Being ISO 27001 one of the most important standards for Strongstep's service offering, the process of preparing client organisations to be certified against the ISO 27001 standard will be explored in this thesis, as this standard supports the main globally recognised information security management certification.

3.2 Case study scope

The problem to be explored is fundamentally associated with the ISO 27001 standard and certification process. Since the ISO 27001 is a majorly recognised standard for information security in organisations, its content is heavily related to the purpose of this study, thus serving as pillar for the presented developments.

Considering what was defined by both the university and the company, the problem is set upon Strongstep's internal process which the company follows when providing ISO 27001 consultancy services. Even though smaller and incremental objectives will later be described, this thesis focuses on two main objectives to be accomplished throughout the beforementioned study process. First, the internal ISO 27001 consultancy service process is set to be analysed, both in terms of how it is defined and handled, with a critical mindset which will connect lean thinking-based concepts with the identified gaps, allowing for practical improvements to be defined and applied to the process. Then, this study should lead to a significant contribute to the existing literature by presenting study findings and generalising this work's methods into theoretical guidelines on how to address and improve information security processes through a lean mindset and its related tools and concepts.

From the company's standpoint, the main interest and objective of this work is to update and improve their ISO 27001 consultancy service process, allowing it to perform better both time, effort, and costs wise through incorporating lean thinking and its related tools as a pillar for enhanced process effectiveness and efficiency.

3.3 Problem characterisation

The identified problem is set upon improving the organisation's ISO 27001 consultancy service process. Regardless of being well documented, the organisation has recognised that this process does not perform optimally, and that there is a significant gap between what this process is and what it could be. Additionally, the existing process documentation is said to be presented in an old fashioned-looking template and lacking a critical review (which had been conducted for the last time several years earlier), as well as to be inconsistent with the process documentation that is available on the internal project management platform.

As of the beginning of this project, the company's ISO 27001 consultancy process was divided into 3 major stages, each of them including a set of activities or tasks to be performed. Within each activity, the documentation goes into further detail on several aspects of the process. First, the responsible for each activity is identified. Then, a list of inputs which precede the activity are listed. Following the inputs, the activity is described, addressing which tasks should be completed, which meetings should be scheduled, which requests should be made, among other aspects. Lastly, the outputs which result from the inputs being processed throughout the activity are presented. These are documented as following:

- Activity number + Activity name
- Responsible
- Inputs
- Actions to be performed
- Outputs

Taking these aspects into account, a first analysis of how the process is documented and handled allowed a few pain points and opportunity gaps to be identified. The goal of this analysis is to set a basis of improvement opportunities to later be addressed through a lean thinking approach. The following major improvement opportunities were initially identified:

- There were considerable discrepancies between the ISO 27001 process documentation and the ISO 27001 process lifecycle within the company's internal project management platform; The process stages were not documented accordingly, and the language used to describe activities was different on each of the sources.
- The process documentation was said not to be representative of how the consultancy services were provided anymore; it lacked a critical review that would identify and update these aspects of the process. It was said to include stages which were not applicable or were unnecessary, while more relevant stages were not well documented enough.
- Part of Strongstep's ISO 27001 consultancy service offer is based upon providing clients training sessions, which generally take the form of conventional workshops. Regardless, these workshops were prepared and conducted using the ISO 27001 structure, which may not be optimal as certain subjects may need to be introduced

sooner in the process, while some may require more effort and time than others. Therefore, an improvement opportunity was identified regarding both the order and the content of the beforementioned workshops.

- The templates which the company uses to get their clients to fulfil certain requirements of the ISO 27001 standard received frequent feedback, indicating that these were too extensive and repetitive, thus too complex to be filled by relatively unexperienced individuals (regarding knowledge of the norm).

As previously explored, the goal of this work is to address these improvement opportunities plus include some others that may surge throughout the project. As often as possible, proposed improvements will be based upon lean thinking and its related methodologies, as to keep the development of this work within its scope. For this thesis to enhance the current knowledge base on the subject, the way these opportunities are addressed will be presented as potential guideline for any reader who may be interested in approaching similar issues from a lean thinking point of view. While the proposed improvements will be based on the case study of ISO 27001 consultancy service process, they can be generalised to any process related to Information Security and, ultimately, to any consultancy service an organisation may provide.

3.4 Exploration

To explore these issues and identify additional improvement opportunities, an exploration phase was conducted. The goal of this phase was not only to verify how the initial issues discussed came close to reality, but also to figure out other improvement opportunities that could be identified after taking a more dynamic approach. For the particular purpose of exploring these improvement opportunities, various actions were undertaken.

In first place, it was needed to understand if the issues the organisation identified in their process documentation translated into improvement opportunities. To achieve so, an extensive reading and analysis of the documentation was performed. This analysis revealed that the initial feedback from the organisation was representative of the documentation's issues: the template in which the process was presented was old fashioned, certain diagrams and activities had mistakes which could compromise the readers' understanding and, most importantly, the documentation did not match the process template available on the organisation's project management platform.

Second, the discrepancy between the documented process and the process that was followed when providing ISO 27001 consultancy services was evaluated. Such analysis was performed by spectating several meetings each involving one out of 3 major client companies. In these meetings, a more practical overview of how the process was handled and applied was possible, through observing and analysing the different activities, workshops and follow-ups which were conducted with these clients. Having done so, it was possible to confirm that the existing documentation was outdated, in the sense that many activities had suffered changes, both regarding their content and the order by which they were performed. The way the organisation provided these consultancy services was a mix between the process they had documented and the process (available to everyone) on their project management platform, but not either of them specifically.

Next, the workshops' content and order were analysed. As before, this could be achieved through several weeks of client meetings observation. In these meetings, it was possible to observe and take notes on how the participants (from the client organisation) would react to

each workshop, which doubts they would have, what would make them feel uncomfortable, what would they have a harder time understanding, and so on. Having observed meetings with 3 different client organisations covering each workshop at least once, it was easily noticeable that certain subjects represented clear pain points for the clients. This happened both in terms of the content being too dense (either because the norm requires so or because no better way of presenting these subjects had yet been developed) and certain subjects being too complex for the client-side participants to understand and translate into properly fulfilling the templates' requirements. Here, a clear improvement opportunity was set upon critically reviewing and analysing the workshops' content and the order by which they were lectured, seeking to develop a new workshop framework which would increase their performance both in terms of increasing effectiveness and reducing amount of "problem solving" meetings needed.

4 Methodology

This chapter aims at presenting the research methodology which has been adopted for the development of this project. In the first section, the different possibilities for research approach are presented, highlighting a few advantages and disadvantages of each. Next, the chosen methodology will be explored in order not only to justify why it is the most appropriate, but also to present how it will be applied throughout the project development.

4.1 Existing approaches

When conducting a research project, there are a few approaches which the researcher can opt from. The two most common and basic approaches to research are the qualitative and quantitative. Maxwell (2008) said that people often overlook the true value of a qualitative approach, "which is in understanding the process by which phenomena take place." (Maxwell, 2008). Quantitative approaches can usually be the most useful when the questions involve justifying or analysing variance, as they include powerful tools to define if a certain outcome is related to a certain variable and to determine how deeply they are connected (Maxwell, 2008). In such case, a qualitative approach would provide valuable insight on justifying how the said situation occurred (Maxwell, 2008). In certain situations, these two methods may be combined, generating an approach which includes aspects from both methodologies.

Besides these traditional methodologies, Design Science Research (DSR) is growing as a research method. According to Gregor and Hevner (2013) in DSR, "the problem definition and research objectives should specify the purpose and scope of the artifact to be developed" (Gregor, Hevner, 2013). Additionally, the authors state that to properly use DSR as a research methodology, the relevance of the research problem to real-world practice must be clearly stated" (Gregor, Hevner, 2013).

4.2 Method used in the project

The scope of this project allows it to be characterised as an improvement-focused study. The project goals were built upon improvement opportunities which were locally identified at Strongstep yet developed in such way that other SMBs operating in similar markets or struggling with similar circumstances can benefit from their exploration. Taking this into account, a qualitative approach has been selected as the major methodological path to be followed in the development of the present work.

For the practical purpose of evaluating the current state of the subject, Strongstep was used for a single case study research. This shall add up to the literature review which incorporates several types of theoretical contributions, allowing a deeper understanding of the study fields involved and their evolution over time. From a practical point of view, the single case study research within the company is conducted with the goal of understanding how the main information security process (ISO 27001 consultancy service) is performing, how up to date its documentation is, how well the collaborators follow the documented process and how may a lean based approach help Strongstep improve the performance of the process. All the before mentioned aspects target the same major aspect: service quality.

To collect information regarding the current state and performance of the ISO 27001 consultancy service process, the major data collection technique used was observation. Observation was performed in two different environments:

- Internally – by observing how the organisation's collaborators prepared client meetings and how they handled the internal process activities which they had to perform;
- Externally – by observing client meetings to understand both how these clients perceive the sessions and how Strongstep collaborators handle them.

Understanding all aspects of the collaborators' work through observation provided the main path for the development of this project. Even though formal interviews did not take place, many interactions through internal meetings caused meeting notes to be a core source of information and feedback for this study. Major inputs were extensively collected during meetings (whenever applicable). This is also relevant when it comes to external meetings (involving Strongstep and its clients), since these are considered to have been one of the main sources for feedback regarding the improvement opportunities. By allowing observation of how Strongstep's ISO 27001 consultancy service process performs next to individuals from client organisations, these meetings provided further theoretical understanding of the process but also practical understanding of its applicability and performance.

Next, the literature review must also be mentioned as a part of this methodology. Considering the literature review as one of the research methodologies involved, it aims at studying the current state of the art on the subject. Since "Lean application to information security" is a very broad and likely vague subject, literature regarding several of this subject's components was approached. Once the state of the art is discussed and presented, the potential for this project's research contributions is explored both from a theoretical point of view (scientific contribution to literature) and practical point of view (findings development, application, and results within the single case study).

4.3 Ethical concerns

Like most research projects, this project involved obtaining information from people, mostly through observing them perform their day-to-day activities. In this case, it involved collecting data on how people work, how certain aspects of their jobs are organised and performed and how they react when handling certain types of uncomfortable situations. Since most information was collected through observation this may be an issue, since some people may not see the researcher's approach as something that could improve their jobs and perhaps develop them as people, but as an exercise of questioning the *whats*, *hows* and *whys* of their actions. Additionally, part of the success of the project is set upon developing further studies which can not only have a scientific contribute to literature, but also that can be applied in the company they work for. This means that the project includes both understanding and questioning people's jobs, but also ideally changing them for better. Here, subjects as expectations and change management surge as a potential requirement for the success of the practical application of these changes.

The goal of the field work is that individuals perceive the project (and the researcher) as being constructive, inclusive and worth their time, clearly helping them understand that this project is meant to improve their jobs and facilitate their daily working lives. It is important that these individuals realise that the project does not mean that they are acting wrong towards their

jobs, but that the way and standards upon which they act could be improved. The same principle applies to the clients, who have way less to gain from this project. In fact, the potential benefits of this project will most likely not affect them at all, as the developed improvements might only be present in future iterations of the process. Despite the existence of non-disclosure agreements, having the cooperation and the acceptance of the presence of a stranger (the researcher) in client meetings was also one of the initial concerns and challenges.

5 Lean methodologies as a path for process improvement

This chapter presents the study results. Here, the field study over the improvement opportunities identified at the case study company connects with the research regarding lean thinking and its related methodologies. The results are presented in four separate sections, each including a lean-based approach to help the company address each of the improvement opportunities which were identified. Each approach is described both in theoretical terms (as a problem-solving framework) and in specific terms (tackling the specific need of the case study organisation).

The first section presents an approach to service processes based upon the lean concept of standardised work. This section is followed by the second developed approach, which details a framework to address customer feedback using an adapted version of the well-known PDCA cycle. Third, the concept of *knowledge pull* is introduced in the form of guidelines which can be used to improve project planning by eliminating activities which do not add value to the final output. Lastly, the study details a waste reduction approach which was developed having in mind the improvement of one of the case study company's processes.

5.1 Standardised work in service processes

Standardised work is one of the principles of lean manufacturing. It refers to the systematic documentation of work procedures and sequence for each job, including three main elements:

1. Takt time – time required per unit production
2. Work sequence – sequence and method for work performing
3. Standard inventory – minimum inventory necessary for operations

From a service process point of view, it is here defined as a way of establishing and documenting concrete and concise procedures and guidelines which will allow collaborators to know when and how activities should be performed, to ensure process flow and reduce variability. Here, the three elements of standardised work are set as:

1. Activity duration – estimate time effort required for each process activity to be performed; since there is a considerable degree of variability in these processes, activity duration may be defined and updated according to record statistics following regular revisions.
2. Activity process – sequence and method which should be followed for each activity; work documentation should extensively explain how each activity should be conducted and how the expected outputs are set to be achieved
3. Activity requirements – the inputs and requirements necessary for each activity to be properly conducted; these represent everything that will incorporate the process and allow the expected outputs to be achieved.

The main purpose of shaping the concept of standardised work to the reality of service processes is to provide more concrete guidelines on how service companies (namely SMBs) can standardise their activities, reducing variability across different projects and process performance across different individuals. This may be particularly useful in helping consultancy companies (such as Strongstep) properly documenting their processes and

practices, which is traditionally harder to achieve in smaller businesses. Besides that, several other benefits were identified as consequence of service process standardisation:

- Following work standards enhances service quality consistency, since the same set of rules, processes and guidelines is followed by all individuals on all projects;
- The existence of documented work standards facilitates training and onboarding, thus allowing time, effort, and financial savings to be achieved;
- Work standards serve as a baseline to facilitate the performance measurement process, thus feeding improvement opportunities and a continuous improvement culture;
- Increased work efficiency means that individuals are more likely to have the time and chance to be creative and help improve organisations;
- Individuals have an easier time dealing with improper task performance, since they are able to compare the way they handle tasks with the way these should be handled;
- Less "gut feeling" involved in process performance not only decreases variability, as it also decreases the number of risks that the individual, the process, and the organisation are exposed to;

To facilitate the understanding of the proposed approach, a visual model was developed (Figure 2). This model intends to allow the reader to better understand the applicability of standardised work to service processes, and to guide any individual who may be interested in applying such approach in an organisational context. In first place, a structured model for documenting work procedures regarding service process activities is presented. For this model, 5 different aspects are considered as critical: the name of the activity, the inputs which are required for this activity to be conducted, the process which should drive individuals in achieving the expected outputs, the outputs and the estimate time effort required for the activity to be completed.

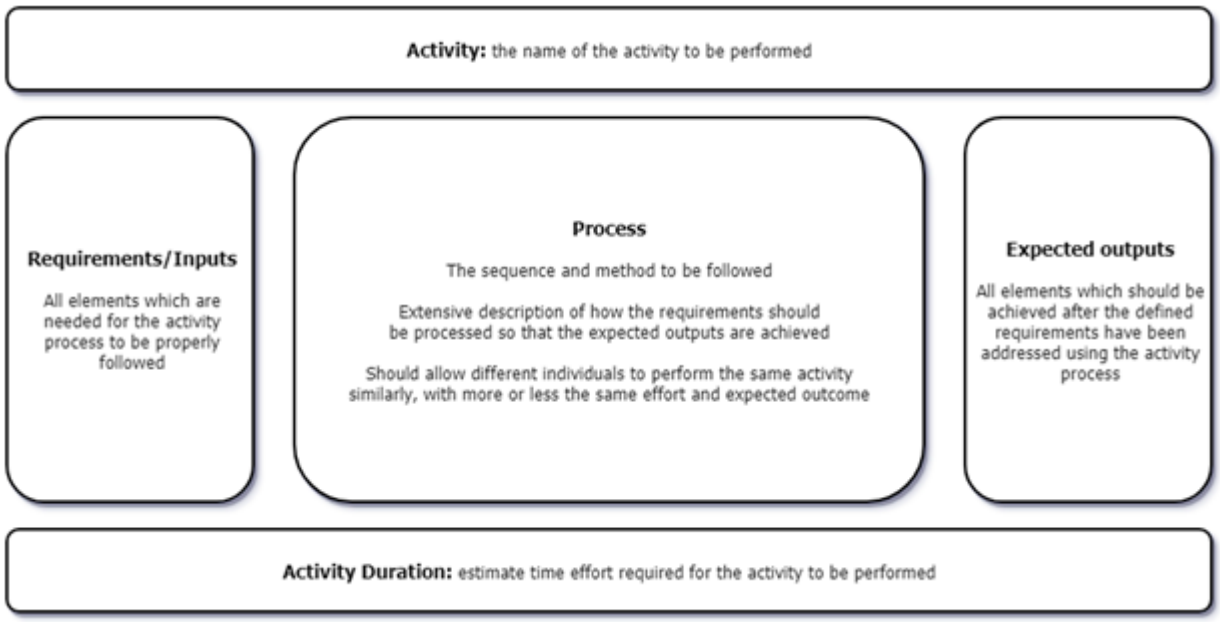

Figure 2 - Standard service process documentation structure proposal

As explored above (Figure 2), a structured way to establish and document service process activities can turn out to facilitate individuals' work and increase service quality performance, through increased process consistency and reduced variability. A process which is structured

this way could be used across all service processes within an organisation, so that all processes follow the same structure and line of thought. If the whole documentation an organisation has is reported equally, following the same principles and presented the same way, not only will it be easier for individuals to cycle between processes with reduced adaptation time, as it will also be easier for newcomers (new collaborators, interns, clients, etc.) to understand these processes and to heavily reduce their required learning cycle.

Taking Strongstep's case study as an example, an improvement opportunity was identified and addressed using the above-mentioned approach. This improvement opportunity which was identified at Strongstep will surely be relatable to many SMBs. Therefore, a generic description of how this opportunity was assessed is presented, followed by the identification of its main goal, finishing up with an explanation on how this opportunity was addressed together with Strongstep.

The main issue which was meant to be tackled using this approach was the fact that internally, the company's ISO 27001 consultancy service process (as well as the remaining service processes) were not documented using the same structure, template, and a consistent work sequence. For each of Strongstep's processes, a different template was used to document the process, which then followed a different line of thought for each of the processes. Therefore, having started by focusing on improving the ISO 27001 consultancy service process, the same methodology was used across several internal processes as to reinforce work standardisation and documentation consistency. The major goal to be achieved through this transformation was to facilitate the interpretation and use of process documentation, especially when involving newcomers or external users, plus to facilitate the creation and adoption of new documentation and/or new processes.

Together with Strongstep, a new process template was developed. This template followed the structure of the proposed approach and was implemented in processes which had been untouched for a long time and were documented differently, starting by the ISO 27001 consultancy service process (Figure 3).

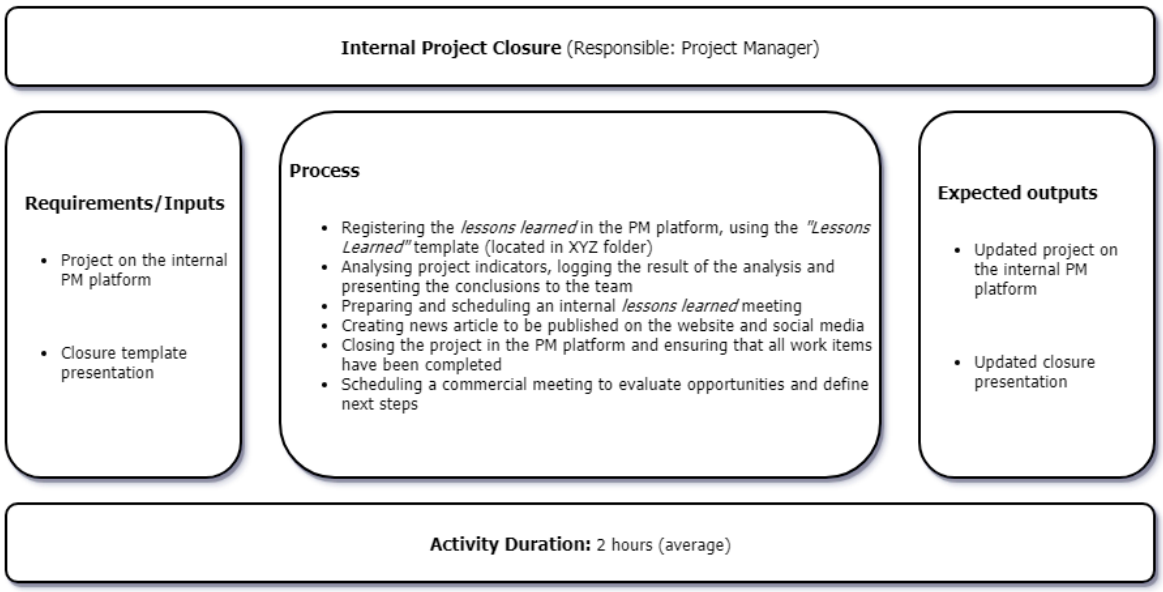

Figure 3 - Application of the proposed service process documentation structure to the Internal Project Closure activity of the ISO 27001 consultancy service process

As previously mentioned, besides having process documentation for each of the services the company provides (including the ISO 27001 consultancy service), Strongstep also has these processes documented in the company's internal project management platform. In this case, an improvement opportunity had been identified regarding the fact that the process documentation and the processes that were documented and followed in the project management platform had considerable discrepancies. This meant that, for example, a newcomer that would join Strongstep and use its process documentation to learn about the processes and their stages would end up with a completely different view on how the process works when compared to how they are handled. To address this improvement opportunity within the scope of work standardisation, the ISO 27001 consultancy service process which is used within the internal Project Management (PM) platform was updated. Changes were made wherever necessary so that the process available in the PM platform would follow the same stages, activities, and principles as the process available in the organisation's documentation. Since the identified issue could also be verified in other service processes apart from ISO 27001, the same principle was applied to two of the other internal processes.

Considering the consistency gains which the proposed work standardisation approach aims at providing, it is set to be expanded to the remaining processes of the organisation and to be used in the future when the need to document new processes (or change existing ones) surges. The goal is to ensure that all of Strongstep's processes are documented using the same template, following the same structure, and using the same line of thought, while maintaining coherence with the processes followed in the internal PM platform. These measures will not only make it easier for newcomers to learn and begin performing these processes optimally sooner, as they will also facilitate project management and increase service quality and effectiveness through increased process consistency.

5.2 Process improvement: a PDCA approach to customer feedback

The PDCA cycle is a part of the lean management philosophy and one of its main requisites for continuous improvement of people and processes. Also known as the Deming cycle, this tool was made popular in the 50s as a method for enhanced quality control. PDCA is a four-stage iterative model for carrying out change, aiming at improving products, services and processes and helping people avoid recurring mistakes. The model's name stands for Plan, Do, Check and Act.

Within the reality of SMBs, the introduction of models such as the PDCA can help these small organisations structure and simplify the process of continuous improvement. Considering the case of Strongstep, an improvement opportunity had been identified regarding exploring how the company could use client feedback to improve aspects of its consultancy services, such as the workshops' content and order, the documents to be filled in by the client, and so on. To tackle this improvement opportunity, a PDCA-based approach is here proposed, focused on adapting the model to the market of consultancy services where companies such as Strongstep operate.

As to properly assess the concerns of companies such as Strongstep, the stages of the PDCA model have been defined as following:

1. Plan
    a. Plan what needs to be done – take small steps towards a low failure risk plan

b. What is the main problem to be solved?

c. Which resources are needed to solve the identified issue?

d. What is the best possible solution for fixing the problem within the available and viable resources?

e. What are the main goals of the plan?

2. Do

a. Implement the changes, keeping in mind that unexpected problems may surge

b. Alpha implementation before full release

c. The higher the degree of standardisation, the higher the chance of success

3. Check

a. Clarify the initial plan – audit plan execution

b. Did the initial plan work as intended?

c. Find what went wrong – perform root cause analysis for problems

d. Use problem identification and analysis to mitigate future occurrences

4. Act

a. Actions depend on the result of the previous stage

b. Positive outcome – Standardise and stabilise the effective changes

c. Negative outcome – begin new iteration of the cycle

d. Adjustment phase which allows a better baseline to be achieved for the next iteration

e. Ideal result – better process

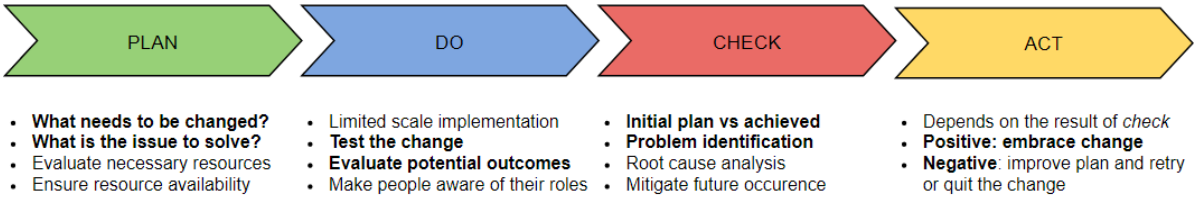

Figure 4 - PDCA approach to turn customer feedback into process improvement

Having broadly defined what matters the most in each stage of the PDCA cycle (Figure 4), the improvement opportunities identified at Strongstep may now be addressed. As previously mentioned, most the company's clients provide feedback during meetings and after the projects' closure. An example may be feedback that Strongstep received which indicated that the workshop lecture process and the related documentation were too extensive, therefore making it harder for the expectations to be fulfilled from the client side. Among other feedback received from clients, these are the type of subjects which this PDCA approach aims at tackling. The core idea is that the scope of the PDCA model can be adapted so that the

company can iteratively plan, implement, review, and adjust changes based on feedback and *lessons learned*.

Within the reality of Strongstep, the PDCA cycle is set to be used every time a project finishes. The feedback collected throughout the project development should be documented and kept in the project's files, just as the project's *lessons learned* which is one of the last stages of every service Strongstep provides. Then, the collected feedback should be used prior to the application of the PDCA model, serving to define a baseline for the first stage of the model. Having the collected feedback as baseline for the application of this approach, the PDCA cycle may then begin:

1. Plan – define what needs to be done. In this first stage, the client feedback should allow the company to identify the main issue(s) to be solved. It should be compiled and analysed so that improvement opportunities can be spotted. Then, the company should evaluate which resources are needed to tackle each opportunity, sorting out which are already available internally and which are viable to be made available. Essentially, this stage should output an answer to the question "W*hat needs to be changed?"*.
2. Do – implement the changes in another project that follows the one that originated the feedback. This should serve as an alpha implementation, to test the change, evaluate potential negative outcomes and collect change feedback both internally and from the client side. People should be made aware of what their roles and responsibilities are within the change, so that its success rate can be increased.
3. Check – seek to understand to what extent the initial plan corresponded to what was actually achieved. As a result, problems should be identified, and their root cause should be analysed. Having this learning stage in mind, the risk for future occurrence of similar issues should be mitigated. This stage should allow an early understanding of whether the change was or not worth it.
4. Act – the actions which may be necessary strongly depend on the result of the previous stage. If the result is positive and indicates that the change was mostly successful, the organisation should seek to stabilise and standardise these changes, incorporating them in the process and acting according to them from then on. If the result is negative, the company can choose to either begin a new iteration of the cycle (if there is still potential positive outcome from the evaluated change), or simply discard and treat the change as non-valuable.

Through this process, the company should be able to pick client feedback, define what can be changed and how the change can be achieved, test the proposed change, perform adjustments, and identify issues, and decide whether the change should be made permanent or discarded. Even though the process was developed with the goal of improving Strongstep's ISO 27001 consultancy service process, it should be extended to any internal process the company has.

As the diagram below shows (Figure 5), the iterative process which is here proposed consists of the four stages of the PDCA model, to which has been added an initial stage of feedback gathering and collection to create a baseline for the application of the model. This process is meant to help Strongstep improve its internal processes, but also to potentially be useful for any other SMBs running similar businesses in successfully implementing a PDCA approach for continuous improvement. It should allow organisations to handle the feedback they receive in a structured way, testing hypothesis and improving processes over time.

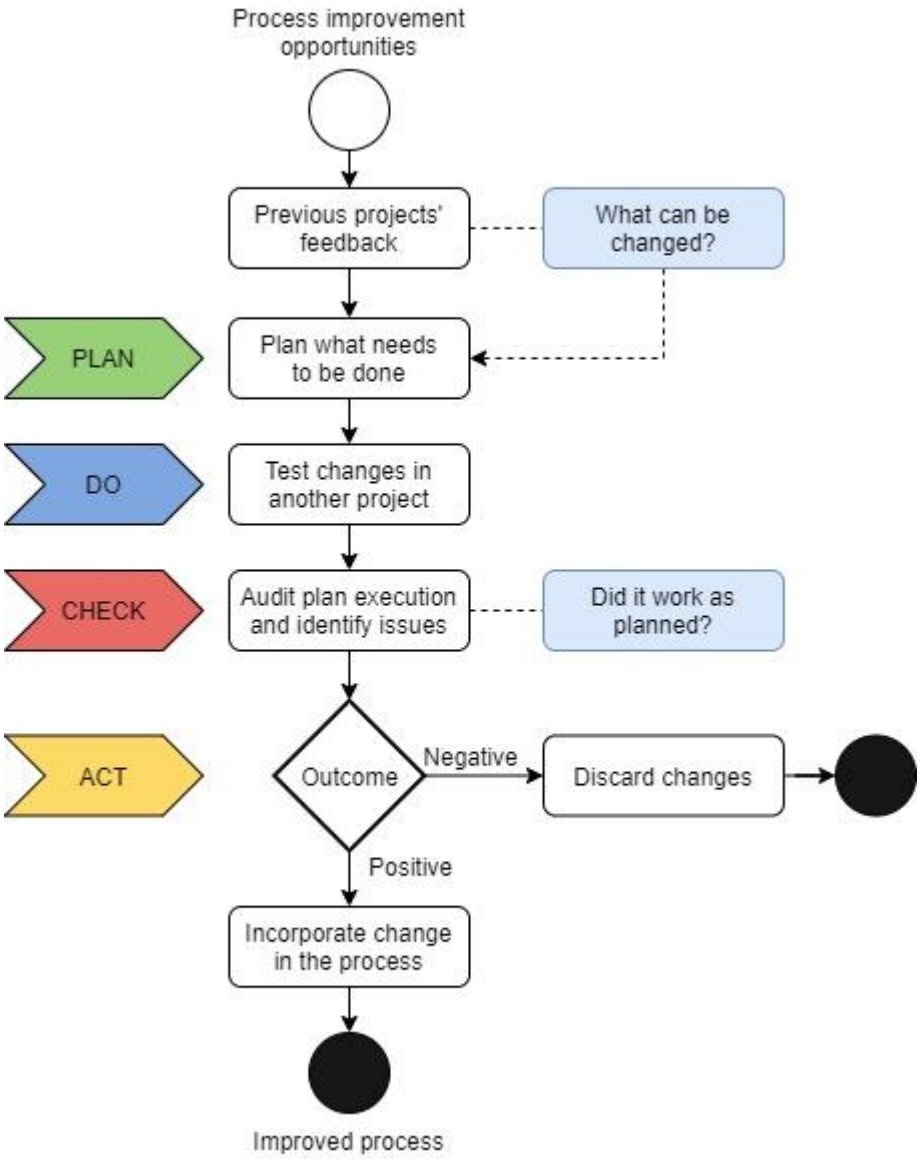

Figure 5 - Incorporation of the proposed PDCA model approach in the improvement opportunity treatment process

5.3 Knowledge *pull* to optimise planning by eliminating non-value-added activities

As mentioned earlier in this thesis, an improvement opportunity had been identified at Strongstep regarding the workshop sessions which the company lectures when providing ISO 27001 consultancy services. The training sessions involved in this consultancy service consist of eight separate workshops, which are the same across all clients, having their presentations suffering only minimal adaptation changes from one client to another (such as including the clients' logo). In this chapter, an approach on how Strongstep may perform these sessions in a more efficient way is proposed, described in such way that other SMBs working in similar markets may also benefit from it.

To properly address this improvement opportunity, the concept of *pull* has been introduced as the ability to produce and deliver the expected levels of service based on customer demand. This means that:

1. The preparation of training sessions should only happen when a client project requires so (following a lean *just-in-time* logic);
2. The way these training sessions are delivered should be adapted to the reality of each client organisation, based on their "competence demand" – here defined as knowledge demand *pull*.

The main addition that this approach presents to the generic lean concept of *pull* is that the demand should also drive the content and the scheduling of the workshop sessions, and not only the preparation process. Its main goal is not only to introduce a *pull* approach to workshop planning, but to also base this activity on a waste reduction philosophy.

Since the ISO 27001 consultancy service Strongstep provides includes a total of eight workshop sessions, this study proposes that Strongstep develops an awareness and maturity questionnaire for each of the workshop subjects. By using this questionnaire, Strongstep should be able to test their clients prior to the beginning of the sessions, thus being able to understand in which maturity level their clients are regarding each of the workshop subjects. As the workshop sessions are conducted in the presence of several individuals from the client side, it is important that for each workshop subject, all individuals which are planned to be present in a certain session are presented with this questionnaire prior to the session itself. Then, Strongstep should analyse these results to conclude which changes may be necessary to make the sessions viable or to downsize the sessions when applicable. Some examples of conclusions that may be drawn according to the results:

1. Most of the participants have average knowledge regarding the subject, therefore the workshop can be light weighted and beginner concepts/exercises may be discarded;
2. Some participants have average knowledge of the subject, while others have none; considering that these participants are most likely part of the management board of the company or have roles related to the certification process, it is very important that the most complete version of the workshop is lectured, so that all participants can be on the same page. The same conclusion should be taken in case all involved participants have no knowledge regarding the subject;
3. All the participants have deep knowledge regarding the subject, covering most interest areas and understanding most related concepts; since these individuals are deeply aware and informed on this subject, the workshop session should be downsized to include only crucial theoretical information, allowing straight advance to other components of the certification process (such as filling documents, creating policies, and so on).

The major goal of this approach is that Strongstep can adapt the content and duration of each workshop to the knowledge and maturity that the client-side participants have on the subject, potentially resulting in major time efficiency gains. This is heavily related with the lean pillar of eliminating waste, since the objective is for Strongstep to provide only the necessary service level for the workshops' objective to be achieved, reducing the content/duration of its workshops when the competences of the audience make it viable. As result, the same workshop outcome should be achieved – client knowledge, awareness, ability to develop the documents which are necessary for the certification – through a quicker and more efficient

process, since time wasted on content which would not add value to the participants (thus to the process) would be eliminated.

To further explain how this can be achieved, let us imagine that one of the involved workshops regarded Information Security Awareness. Having the subject in mind, the company should then develop a questionnaire with questions that would allow the client participants' knowledge on the topic to be tested. These questions could, for example, include:

1. While browsing your e-mail, you pressed a link that took you to an unknown page and started the download of a file. What should you do?
    a. Delete the file, close the page, and move on with your work.
    b. Contact the IT department immediately.
    c. Open the file to figure out what it is.
2. Which entities are under risk of suffering attacks from hackers?
    a. Companies who manage customers' payment information.
    b. Banks and finance institutions.
    c. All companies and individuals are at risk.
3. One of your co-workers sent you an e-mail requesting that you click a certain link. What should you do?
    a. I trust the person who sent me the e-mail, so I will click the link.
    b. If the e-mail message was harmful, it would have been blocked or flagged as potentially dangerous.
    c. Call the sender and verify whether they sent the message or not.

Having the questions defined, the company should then define a standard to evaluate the results of the test. This standard should allow Strongstep to qualify the maturity level of the participants regarding the subject (for this example, Information Security Awareness). Based on this example, the answers could be evaluated as following:

- **Maturity level 0:** either none or one answer were correct.
- **Maturity level 1:** two answers were correct.
- **Maturity level 2:** all answers were correct.

Having the participants' subject maturity properly classified, Strongstep would then be able to conclude which type of operation would be necessary for the workshop to be prepared. Still taking the previous example into account, the three scenarios which were initially approached may be verified. Firstly, a scenario where most of the participants have been evaluated with maturity level 1. This means that these individuals may not dominate the subject, but they have an acceptable level of awareness about it, possibly lacking a few crucial aspects. Since they already have a decent amount of knowledge on the subject, the Information Security Awareness workshop could be slightly downsized, excluding beginner concepts and/or exercises which will most likely not add value to these average-scored individuals. On the other hand, let us pick a scenario where while some individuals were evaluated with maturity level 1, others have been evaluated with maturity level 0. This means that while some of the participants will already be aware of some of the topics discussed in the workshop, others will

need the most beginner-friendly version of the training session, as they feel very uncomfortable with the subject. In this case, the full version of the workshop session should be used, so that all participants can be provided a similar level of knowledge and awareness on the subject. Third and last, the "best case scenario" in terms of efficiency and time savings: all individuals scored maturity level 2 in the test, meaning that they all got all answers right. Since these questions covered the relevant topics of the workshop and the participants are fully aware of how they should be addressed, the workshop session can be heavily reduced to include only crucial information, thus allowing quicker progression into further stages of the certification process. While these 3 scenarios do not cover all possible combinations of the involved variables, they should be broad enough to serve as a guideline for proper understanding and use of the approach.

Once the knowledge and awareness tests have been conducted and evaluated for every participant regarding the eight involved workshop subjects, the second issue may be addressed. Here, the main goal is to define how these workshop sessions should be scheduled, in terms of the scheduling order. For workshop scheduling, a much simpler approach is proposed, to complement what was previously explored. While still using the three above mentioned scenarios as consequence of knowledge and awareness test evaluation, the drawn conclusions will be applied to structure the workshop order. Having this in mind, three primary criteria for subject ordering were developed:

1. Workshops which have been approached under conclusion type 3 (major downsizing and simplification) should be lectured in first place, so that the work pace can start softly to facilitate client adaptation and help motivate the participants;
2. Workshops which have been approached under conclusion type 1 (minor downsizing, beginner aspects discarded) should be lectured in second place; since the participants have already been involved in simpler and less time/effort consuming tasks, it will now be easier to progress to slightly more complex sessions and tasks;
3. Workshops which have been approached under conclusion type 2 (full workshop version, as complete as possible) should be lectured in last place; having performed simple tasks first and slightly harder tasks next, it would then be easier to move on to the hardest stage.

The idea around these scheduling criteria is that the first contact which clients have with the workshops and related deliverables is as simple as possible, so that they can slowly embrace the process and fit their working habits to the reality of the process itself. Once they start feeling more comfortable with a different way of working, it could potentially be easier for them to embrace and feel motivated to complete harder tasks, as they will already feel like a part of the project. Having been able to complete these tasks, it would be expected that the participants would be much more receptive to the final and most complex category of subjects and tasks. As they would already have been exposed to introductory subjects and allowed to more deeply explore subjects that they previously had very basic knowledge in, the introduction of completely new subjects can be softened.

The approach explored in this chapter presents a solution on how Strongstep can simultaneously address two improvement opportunities that had been identified during the beginning of this project. Based on the lean concept of *pull* and the generic idea of waste reduction and elimination of non-value-added activities, this approach was developed to allow Strongstep to reach higher levels of time and effort efficiency in its workshop sessions' content and scheduling. Regardless of having been developed with the reality of Strongstep

and its services in mind, this approach may prove to be useful for other SMBs which may operate in similar markets and/or provide services which may involve sessions of a similar nature.

5.4 Waste reduction approach to workshop output documents

Previously in the project characterisation chapter, an improvement opportunity regarding the documents which Strongstep requires their customers to fill after each workshop was briefly introduced. When providing ISO 27001 consultancy services, Strongstep has a set of documents which are presented after each workshop as *expected outputs*. These templates are meant to allow the client company to properly fulfil the requirements of the ISO 27001 standard. As previously mentioned, these templates received feedback from clients, who frequently felt overwhelmed by the amount and complexity of the documentation which they were required to develop. Internally, consultants who manage and operate ISO 27001 projects have agreed that this consultancy service involves too many templates, which could easily be reduced to a much smaller number. This would facilitate their work, but also the clients' job when striving to fulfil the requirements of the norm. This improvement opportunity is heavily related to one of lean's most important principles: identifying value and eliminating all non-value-added activities. Since the main issue lies on the existence of unnecessary documentation, the present approach will relate these two aspects, proposing a solution for Strongstep to address the issue by focusing on value-adding activities.

To properly address this issue using a lean thinking approach, a proper definition of *waste* under the context of the issue is needed. Given the nature of the improvement opportunity, *waste* is here defined as:

1. Amount of documentation:
    a. Scenario 1 – The required documentation includes documents which may not be strictly needed to fulfil the requirements of the norm.
    b. Scenario 2 – The required documentation includes documents which are equivalent to other documents that the client organisation has already built internally.
2. Scope of documentation:
    a. Scenario 1 – The required documentation includes documents which may not be applicable to the reality of the client organisation.
    b. Scenario 2 – The required documentation presents separate documents to fulfil requirements of similar nature.

The abovementioned categories of *waste* may not be simultaneously verified. Across different projects and different client organisations, different scenarios of non-value-added activities regarding requirement documentation may be present. Regardless, the fact that the same templates and the same documentation structure is required to each customer (with low to null degree of customisation) can be seen as the root cause for these types of waste to be verified in first place. Therefore, to properly apply a waste reduction approach to this process, it is necessary that each project is analysed under this scope, prior to the beginning of the requirements documentation process. This analysis should allow the client organisation to be evaluated according to factors such as:

1. Internal documentation which may be equivalent to some of the typically required documents;
2. The reality of the client organisation, which may generate the need to simplify the process or allow certain documents to be discarded due to not being applicable;
3. The ability of the client organisation to take advantage of information which is already available internally, potentially changing its display form and/or adapting it to fulfil a certain requirement without having to build a new document from scratch. This may be applicable when, for example, a company has a platform for asset registry, but does not have a formal asset inventory.

Using the first three previously defined scenarios of waste under the scope of this issue and considering the individual analysis of each project, the company may then be able to identify which documents (from its whole set of traditionally required documentation) are not necessary for a certain client to fulfill the requirements of the standard. As for the last waste scenario presented, the outcome should be slightly different. Since this scenario may be verified whenever the required documentation includes separate documents which address similar requirements or pieces of the same requirement, the proposed "waste treatment measure" is that Strongstep merges these documents, as their scope should not justify the existence of multiple documents. Having these documents merged, two main benefits are expected. First, since multiple documents would have been merged into one, document components such as the edit log and the index would be present only once, thus facilitating the filling process and reducing documentation size (increasing efficiency when building the documents). Second, this approach tackles a more psychological aspect of the process – customers' perception of *work to be done*. Being required to develop a smaller number of documents, the clients are expected to feel less overwhelmed by the work they are expected to do – even if, in theory, it is just as much as before – thus potentially feeling more motivated and delivering results quicker. An example of this scenario may be taken from one of the client sessions which was observed as source of input for this thesis. When explaining how they managed to conciliate their job at their organisation with the work they were required to fulfill the requirements of the ISO 27001 certification process, one of the organisation's clients mentioned that they would dedicate each piece of their time to get a certain number of documents done. Theoretically, this means that if this person decided to put time into 2 of these documents per week, and they were required to build 10 documents in total, it would potentially take them 5 weeks to have everything done. On the other hand, if these documents were studied and it was concluded that three pairs of two documents could be merged into one, only 7 documents would be needed. This means that while the content itself could be the same, this individual could potentially have the same information documented in one and a half weeks less, simply over the fact that the number of deliverables they were expected to develop would have been shortened.

To make it easier for the proposed lean-based approach to be understood and put into use, a process diagram was built as a visual representation of all involved steps (Figure 6):

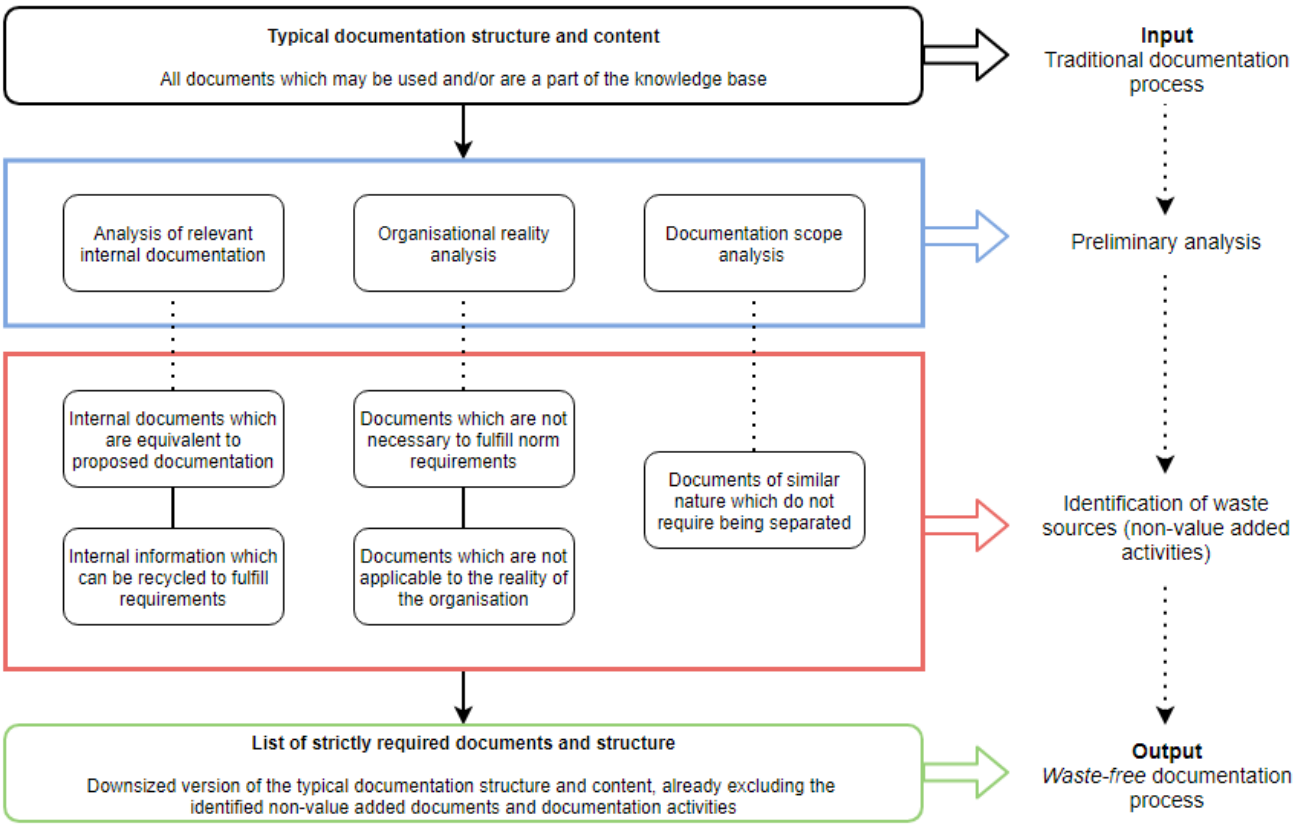

Figure 6 - Lean-based approach process to handling requirements documentation

As shown above, the main input for this approach is the documentation structure and content which the company typically presents to their customers. Taking this into account, a three-level preliminary evaluation should be conducted, analysing internal documentation of the client organisation which may be relevant for the certification process, the environment and the reality of the client organisation and the scope of the documents which are usually proposed. This analysis should aim at identifying non-value-added activities and/or components of the requirements documentation process, such as:

- Internal documents which may be equivalent to some of the proposed documentation;
- Internal information which can be recycled (adapted and/or have its display form changed) to fulfill requirements of the ISO 27001 standard;
- Documents which are a part of the typically proposed documentation but do not apply to the reality of a particular client organisation;
- Documents which are a part of the typically proposed documentation but are not strictly necessary to fulfill the norm's requirements;
- Documentation subjects which are of similar nature and/or scope but are presented in different documents.

Having identified these activities and/or components of the process which do not add value to it, the major output to be achieved is a *waste-free* documentation process, which represents a downsized version of the typical documentation structure and content, hence a more efficient version of the same process thanks to this lean thinking-based approach.

6 Conclusion and future research

This project was developed together with a software engineering consultancy company. Within the reality of this organisation, several improvement opportunities were initially identified. These opportunities were targeted and defined so that they could truly represent issues which the company has, while fitting the scope of this academic study. Having connected both the interest of the organisation in improving their processes and the interest of the researcher regarding literature contribute these improvement opportunities were addressed using the theoretical principles which guided this work.

Following what was initially evaluated, literature regarding the application of lean methodologies within the context of information security service processes is very limited. Therefore, the study aimed mainly at answering the research questions which were identified by presenting solutions which could cover both areas of interest: providing specific approaches, tailored to the improvement opportunities of the partner organisation and to their improvement opportunities, while describing them in such theoretical terms that a potential contribute to literature can be extracted from these.

The first research question which was defined is related to the exploratory aspects of this study. Seeking to understand how Information Security consultancy processes are currently handled in SMBs, conclusions were drawn primarily from two sources. In more theoretical terms, exploration was conducted through a literature review. This literature review provided insights on how these processes are currently addressed within the reality of SMBs, allowing a theoretical framing of how this happens and what methodologies are used. In second place, exploration was conducted through observing and participating in the partner organisation's daily activities related to these processes. Mainly through observation, more practical outputs were collected which provided a real-world understanding of how such organisations handle these processes. Examples of such outputs may be feedback collected directly from client organisations and the observation of people performing activities within each stage of the beforementioned processes. This second stage was crucial for the development of this project, since the single case study approach provided insights which could not be found or accounted for in literature given the high variability of services and processes which involve people.

The second research question was answered through a mix of knowledge research and field work. Having the reality of the partner organisation in mind, several improvement opportunities were identified regarding Information Security consultancy processes. Taking these into account, a set of approaches were developed and are proposed to be used to tackle these improvement opportunities. These approaches cover the application of standardised work to service processes, the handling of customer feedback through an adapted PDCA cycle, the improvement of process planning through the elimination of non-value-added activities and the reduction of waste within the consultancy service process documentation. Since the second research question was based upon understanding how lean thinking and its related methodologies can contribute for the improvement of Information Security consultancy processes, an answer can be found through an extensive analysis of the lean-based approaches which are here proposed. These root from lean thinking methodologies and some of its principles, having been adapted not only to fit the reality of the involved organisation, but also hoping to contribute to the existing literature by exploring this field of study and providing these approaches as guidelines for improvement.

From the point of view of the involved organisation, the improvement proposals (here presented as study results) tackle the improvement opportunities which had been initially identified. The company has direct interest in the results of this study, as they provide theory-based guidelines on how the organisation can assess some of its most urging issues. Since these guidelines were developed having the reality of this organisation in mind, they are presented in a way that should allow this company to explore their full potential. Nevertheless, the guidelines and approaches which are here presented have been developed and described in such way that they can be used to address issues of similar nature. By always presenting a theoretical framing in each of the improvement opportunity assessment sections, the author aimed at providing solid study conclusions which may contribute for the existing literature in this subject. In more specific terms, this thesis provides four different approaches to improving service processes, which may serve as a baseline for future studies regarding the same or related subjects.

Regarding the implementation of the proposed approaches within the organisational context of Strongstep, the scenario is optimistic. As of the end of the field study with the company, the first approach had already been applied to the ISO 27001 consultancy service process. The company considered this approach to be so valuable that it was decided that the same principle should be applied to the remaining processes of the organisation. By the end of this project, at least three of the company's consultancy service processes had already been standardised following the proposed approach. Despite not having been applied yet, the remaining approaches have been seen by the company as valuable and as potential sources of added value to their processes, thus being expected that they could be implemented in the near future.

As for expected benefits of the application of the remaining methodologies, a few points should be highlighted. It is expected that:

1. The standardised work approach to consultancy service processes can be expanded to all of the organisation's service processes, so that it can be seen as a truly standardised company in terms of work guidelines and orientation; the benefits of this achievement should be primarily internal, resulting in efficiency gains that would benefit the company as a whole.
2. The proposed PDCA approach to customer feedback is expected to help the organisation improve the quality of their services, since valuable customer feedback would be translated into improvement opportunities which would then be designed, tested, evaluated and ideally, permanently incorporated in the processes.
3. The *knowledge pull* approach is mainly focused on efficiency gains in a particular stage of the delivery of ISO 27001 consultancy services; within the scope of eliminating activities which do not add value to the process, the implementation of this approach should result in efficiency gains (internally) and in a lighter and more enjoyable perceived service experience by the clients.
4. The last of the proposed approaches tackles one of the organisations' most important issues, by simply incorporating an iterative lean-based cycle into the process of requirements documentation; this should result in major time, cost and effort savings for the organisation, as it relies on identifying sources of pure waste so that they can be eliminated from the process.

Regarding future research, the author believes that this study can potentially motivate others to develop further work regarding the application of lean methodologies to service processes. Lean as a management tool began in an industrial environment, and its application to services management and service processes still has a lot of room for improvement and for the development of methodologies, guidelines and frameworks that can help organisations make the most of the philosophy.

References

Anderson, R. (2001). Why information security is hard - An economic perspective. *Proceedings - Annual Computer Security Applications Conference, ACSAC, 2001-Janua*, 358–365.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Baker, W., Goudie, M., Hutton, A., David Hylender, C., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B., Tippett, P., Bosschert, T., Brohm, E., Chang, C., Dahn, M., Dormido, R., Van Erck, B., Evans, K., Gentry, E., Grim, J., … Neal, C. (2011). *2011 Data Breach Investigations Report.*

Boehmer, W., & Boehmer, W. (2016). Appraisal of the Effectiveness and Efficiency of an Information Security Management System based on ISO 27001.

Cavusoglu, H., M. Birendra, and S. Raghunathan. (2004a). "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," International Journal of Electronic Commerce (9)1, pp. 69-104.

Cellar, D. F., Nelson, Z. C., Yorke, C. M., & Bauer, C. (2001). The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement. Journal of Prevention & Intervention in the community, 22(1), 43e52.

Costa, P. T., & McCrae, R. R. (1992). Normal personality assessment in clinical practice: The NEO Personality Inventory. *NEO PI-R professional manual. Inc., Odessa, FL: Psychological Assessment Resources.*

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90–101.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. In *MIS Quarterly: Management Information Systems*.

Heinstrom, J. (2003). Five personality dimensions and their influence on information behaviour. Information research, 9(1), 9e1.

Hicks, B. J. (2007). Lean information management: Understanding and eliminating waste. *International Journal of Information Management*, *27*(4), 233–249.

IDG (2016). Data & Analytics Survey.

ISO (2009). ISO 27000: Information Technology, Security Techniques, Information, Security Management Systems, Overview and Vocabulary. International Organization for Standardization ISO, Geneve.

ISO (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. Handbook of personality: Theory and research, 2(1999), 102e138.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & security, 25(4), 289e296.

Maxwell, J. (2008). Designing a Qualitative Study. The SAGE Handbook of Applied Social Research Methods, 214-215.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156.

Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. *The Art of Deception*. John Wiley & Sons.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An Australian web-based study. In Proceedings of human aspects of information security, privacy, and trust (LNCS pp. 231e241). Springer International Publishing.

Pricewaterhouse Coopers. (2015). Key findings from the global state of information security survey 2016. *Turnaround and transformation in cyber security*.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. AMCIS 2006 Proceedings, 415.

Stankov, L., Boyle, G. J., & Cattell, R. B. (1995). Models and paradigms in personality and intelligence research. *International handbook of personality and intelligence*. Springer US.

Von Solms, R. (1998). Information security management (3): The Code of Practice for Information Security Management (BS 7799). *Information Management and Computer Security*, *6*(5), 224–225.

Von Solms, B. (2006). "Information Security: The Fourth Wave," Computers & Security (25) 3, pp. 165-168.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102.

Whitman ME, Mattord HJ (2009). *Principles of information security*. 3rd ed. Thompson Course Technology.

Womack, J.P., Jones, D.T. and Roos, D. (1990), *The Machine that Changed the World: The Story of Lean Production* (HarperCollins Publishers, New York, USA).

Womack, J.P. and Jones, D.T. (1996), *Lean Thinking: Banish Waste and Create Wealth in Your Corporation* (Simon & Schuster, New York, USA).

Zafar, H., & Clark, J. G. (2009). Current State of Information Security Research In IS. *Communications of the Association for Information Systems*, *24*(34), 557–596.