UNIVERSITY OF TARTU
Faculty of Social Sciences
School of Economics and Business Administration
Innovation and Technology Management Curriculum

Anna Shamritskaya

Information security assessment in a start-up

Master's Thesis (20 ECTS)

Supervisor(s): Mari Seeba
Raimundas Matulevičius

Tartu 2022

Information security assessment in a start-up

Abstract:
Information security currently generates a significant coverage and discussion in media worldwide. Even relatively few security breaches affect vast numbers of people, making it one of the biggest problems companies face today. As a result, more pressure is put on emerging suppliers of innovative processes and products, start-ups.
However, there is no established framework that assesses the information security of a start-up. One possible solution is to use frameworks already created for established companies, even though such frameworks do not consider the peculiarities of start-ups. **In this work, the author considers studying how to assess the level of information security in a start-up by elaborating a model which can be matched with the well-known start-up lifecycle.**
The main result of this thesis is a new model that will be a significant contribution to understanding how information security evolves at different stages of a start-up lifecycle.

Keywords:
Start-up, start-up lifecycle, information security, security requirements, ISO 27001.

CERCS: P170

Infoturbe hindamine idufirmas

Lühikokkunõte:
Infoturve tekitab praegu kogu maailma meedias märkimisväärset kajastust ja arutelu. Isegi suhteliselt vähesed turvarikkumised mõjutavad suurt hulka inimesi, muutes selle üheks suurimaks probleemiks, millega ettevõtted praegu silmitsi seisavad. Selle tulemusena avaldatakse rohkem survet esilekerkivatele uuenduslike protsesside ja toodete tarnijatele, idufirmadele.
Pole aga kehtestatud raamistikku, mis hindaks idufirma infoturvet. Üheks võimalikuks lahenduseks on juba väljakujunenud ettevõtete jaoks loodud raamistike kasutamine, kuigi sellised raamistikud ei arvesta idufirmade iseärasusi. **Selles töös uurib autor, kuidas hinnata infoturbe taset idufirmas, töötades välja mudeli, mida saab sobitada tuntud idufirma elutsükliga.**
Selle lõputöö peamiseks tulemuseks on uus mudel, mis aitab oluliselt kaasa infoturbe arenemise mõistmisele idufirmade elutsükli erinevatel etappidel.

Märksõnad:
Start-up, start-up elutsükkel, infoturve, turvanõuded, ISO 27001.

CERCS: P170

Contents

1 Introduction

Information security has been a widely discussed topic for the past years because of the ransom attacks that bring significant risks to organizations financially and reputationally. According to the UK National Cyber Security Center, there were three times as many ransomware attacks in the first quarter of 2021 as there were in the whole of 2019 [7].

Moreover, research by PwC suggests that more than half of the technology executives believe this to increase in 2022 [34]. Therefore, introducing an information security framework becomes essential because it supports the company's activities and because the law requires it.

In European Union (EU) General Data Protection Regulation (GDPR) imposes a uniform data security law on companies that have their operations in the EU. So that each member state no longer needs to write its data protection laws and they are consistent across the entire zone. It allows authorities to impose fines of up to €20 million or 4 percent of worldwide turnover for the preceding financial year—whichever is higher ([15]).

Moreover, in the EU, the National Information Security directive is in force ([28]). It promotes security measures and boosts EU member states' level of protection of critical infrastructure. In other words, it improves the information security of operators in sectors that provide essential services to our society and economy. However, Cybersecurity acts that would require all firms to follow specific standards in the field are yet to come. Nevertheless, it is still vital for any business to follow an information security framework and evaluate how effective its measures and controls are.

Unfortunately, most studies regarding compliance to data protection are about big tech giants and established firms. Little or no attention is paid to start-ups. Therefore, start-ups can find themselves thrust into the complex world of managing a business threatening ransom attack. Tools and guidelines should be developed to minimize the risks and reduce the harm.

Thus the study aims to improve the development process of the start-up by gaining insights into information security and its development throughout the start-up lifecycle. The author believes that the information security assessment model would be critical to evaluating the readiness of a start-up in terms of information security. Moreover, it can become one of the tools to prepare the start-up to scale up its operations.

1.1 Research Questions

The main research question **MRQ** is "How information security is developed throughout the start-up lifecycle?". To answer it thoroughly the following four research questions were created.

The first research question addresses the stages of start-up lifecycle. **RQ1** "What are the main stages in the start-up lifecycle?". The main aim is to understand how start-up develops and what challenges and activities are associated with each stage of its lifecycle.

RQ2 "How ISO 27001 controls are related to start-up lifecycle?". This research questions focuses on understanding how different start-up challenges and activities are associated with security controls. Thus allowing to map them together and get clear picture on the information security topics that start-up should focus during its development process.

RQ3 "How development of information security controls can be followed?". To answer this research question, author creates information security maturity model to follow the development of the controls at different stages of the start-up lifecycle.

RQ4 "What information security themes are essential at each stage of a start-up lifecycle?". This research question focuses on proving that some of the information security themes are essential at different stages of the lifecycle.

RQ5 "How to assess information security as a whole in a start-up?" The goal of this research question is to bring clarity whether it is possible to develop an information security assessment model.

1.2 Thesis structure

As for the structure of the thesis, **Section 2** covers RQ1 and RQ2. In Section 2 author presents the current view on the start-up definition, how it evolved over the past decades and what the current view on the start-up lifecycle is. Moreover, author presents information security standard, ISO 27001, to give an understanding why it is relevant to start-ups and what common practices exist. Finally, author makes a connection between ISO 27001 controls and start-up activities or/and challenge at each stage.

Section 3 focuses on elaborating RQ3 and RQ4. First, author presents the available information security maturity models and, then tailors a new one for the purpose of this study thus answering RQ3. The model is derived from the literature review. To understand how information security controls are developed throughout the start-up lifecycle, author creates a survey that evaluates lifecycle stage and maturity of different information security controls. This allows to group the controls into broader topics thus answering RQ4.

Section 4 contains the methodology and data collection method to validate that some information security themes are essential at certain lifecycle stages. This in turn allows author to create an overall information security assessment model and thoroughly answer RQ5.

Finally, **Section 5** discusses limitations of the study, concludes the thesis by providing answers to the main research question and defines the vector for future work. The following Diagram 2 illustrates the key activities of this work, it is presented to provide a sufficient and detailed overview of the workflow.

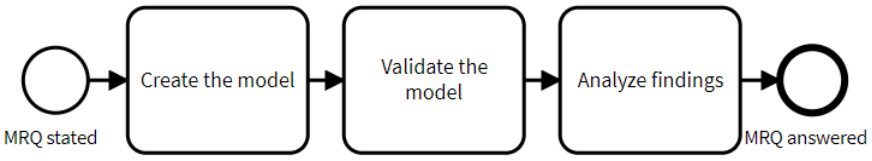

Figure 1. Overview of key the activities of the research

2 Start-up lifecycle and ISO 27001 standard

This section provides answers to **RQ1** "What are the main steps in the start-up lifecycle?" and **RQ2** "How ISO 27001 controls are related to start-up lifecycle?". To have an overview of activities that took place in order to answer research question, the Figure 2 was compiled.

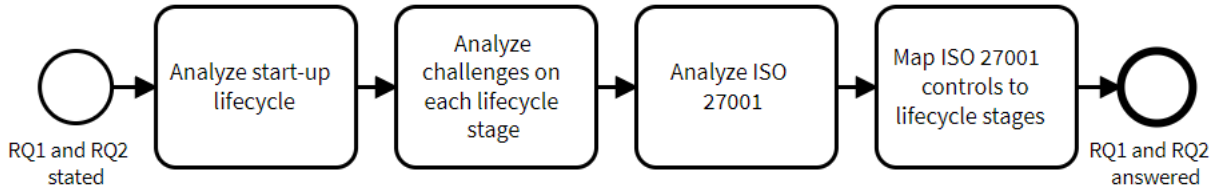

Figure 2. Overview of key activities for Research Questions 1 and 2

2.1 Start up and its lifecycle

2.1.1 Definition of a start-up

In this section, the author presents an overview of existing start-up definitions. It is important to note that there is no one unique definition of that concept. Various authors look at it from different angles and depict their understanding of the term depending on diverse factors. Nevertheless, all of them agree that start-up as a concept is related to entrepreneurship and innovations. Moreover, start-up usually refers to firms at the first stage of their operations.

To begin with, Cockayne [9] sees it as *type of firm or working practice* that brings economic growth to the region and is usually driven by technology and knowledge-based forms of entrepreneurship. His definition emphasizes the advanced technology and new, unique or innovative ways of work that the firms undertake. However, Cockayne [9] considers start-up as a difficult to define concept that is mainly used in academic and mainstream papers related to the digital media and technology-based regional economic development.

The view that start-ups are critical in introducing technologies to the market because of their disruptive power that allows continuous economic growth is shared by many authors that do not necessarily focus their research on the definition of the start-up. [14, 10]

Marwick uses start-up to name big and successful, already established firms, for instance, Google, Facebook, or Airbnb [26]. Marwick's view contradicts the view of other authors that describe start-ups as non-profitable establishments that only started their operations [14]. However, Marwick brings out an interesting point that there is a tautology between start-up and venture capital (VC) that comes from the way one can define a company by the way it is financed [26].

Ries, in his book "The lean start-up" [35] describes a start-up as a company that creates something new under the conditions of complete uncertainty. This definition goes along with what Cockayne brings out in his paper; both authors emphasize that technology and innovation are essential with regard to the start-up concept [9], [35].

Nevertheless, Ries [35] does not mention anything about several factors that are mentioned in other papers [33, 30, 22], for example, size of the firm, its financial stage, maturity, sector or industry. This concept definition is considered broad, but it still depicts the main idea.

Important to note that start-ups on their own are not capable of building innovation due to the lack of experience, size, and resource limitations; they depend on various external actors [8]. This brings the author of this paper to conclude that one of the critical indicators of a start-up could be the co-creation of value.

In OECD [30] start-up is considered as a part of a creative disruption which tightly connected to the concept of entrepreneurship. A Start-up company is considered a supplier and driver of innovation, productivity, and growth that generates new workplaces and brings new ideas to the market. There is an emphasis on the maturity that is defined by *young* meaning that the authors of [30] define start-ups as firms that just started operating or are on the stage of the idea.

A more comprehensive definition of a start-up can be found in a paper by Kollmann, and others [22] where the following factors are taken as the main determinants of the concept:

- Less than ten years
- Innovative technology and business models;
- Significant growth

These aspects help differentiate start-ups from established companies and provide valuable insights to understand the fuzzy concept better. One of the emphasis is on regional development, and the authors of the paper clearly state that their study cannot be fully representative of all European start-ups [30]. Nevertheless, their notion reflects the understanding of most of the authors previously mentioned, which makes it entirely accurate.

All in all, in the past decade, more and more people are talking about start-ups, but still, there is no one concrete definition that could cover it all. Many factors do impact the concept and how it is used. However, most of the authors agree that the term is tightly connected to entrepreneurship, advanced technologies, and innovations. It is explained by the understanding that start-ups usually bring new and sometimes disruptive ideas to the market. Definitions discussed in this section are not exhausted and are provided for the reader to better acquaint oneself with the concept.

2.1.2 Start-up lifecycle

In this section author of the paper introduces different perspectives on the start-up lifecycle models and gives a brief introduction to each stage. Moreover, the main issues and challenges for each stage are identified.

To begin with, various business lifecycle phases are proposed in the literature. To be more specific three major stages were identified for a start-up lifecycle: **creation, development and market phase** [33, 23, 14]. As with the definition of a start-up, the lifecycle concept, the boundaries that divide stages from one another are not so definite. However, these phases provide a roadmap of the path that start-ups usually follow when maturing.

Another important aspect is that some authors argue that after the *market phase or growth stage* start-ups enter one more stage, maturity or market exit, after their status of a start-up is no longer valid [33]. Finally, the start-up lifecycle is not a linear process; in order to stay lean and mature the product or service, start-ups have to go through the stages more than once [35].

Some authors identify the very first stage of a start-up lifecycle as ideation, pre start-up, or early seed [23, 31]. It is a stage before the first major one, creation. The founder has an idea already

and seeks to explore its feasibility; most of the efforts are on developing the idea that might solve a significant customer need. This stage is defined as well by the search of the market, customers, partners, distributors, and competitors [31]. It is also a formative stage where the founder has to prepare for the future steps; the start-up is yet to generate the value and revenue but already has a market hypothesis to test.

As for the key challenges that start-ups face during this stage, they all are summed up by one concept of uncertainty, to be more specific: lack of skills, lack of team and its structure, no confirmed commitment, and no product/service.

When initiating start-up development, entrepreneurs have to act in unpredictable settings, they lack the necessary knowledge about the external environment, and their actions are usually based on intuition [38]. Setting directions and maintaining the focus, being clear about the goals, and staying realistic are the factors that are perceived as primary. Nevertheless, founders do not see legal regulations or information security requirements to play a significant role at this stage [40].

The next stage is creation; transition to the stage is usually defined by prototyping the solution into a minimal viable product (MVP) and advancing the initial business model into a feasible one [31]. Additionally, more profound market research is conducted. It is also a time when start-ups grow in terms of people; if in the early stage, it is a one-person show, now multiple people share responsibilities and have a primary division of the roles [23].

The critical challenges are leadership and team alignment, financing of the future company, and the creation of MVP [40]. Moreover, the following issues are there to solve by the founder and the team as well [40]:

- position the product/service in the market;
- maintain internal communication smooth;
- maintain growth;
- build the organization and the management teams;
- build financial capability;
- develop an internal work culture;
- manage risks.

This list is not exhausted, and there could be start-up-specific challenges as well, but it captures in essence that the creation stage is the next step from the ideation and involves even more uncertainty and risk. However, to the best of the author's knowledge, the information security risks are not emphasized at these stages.

From this stage, start-ups are slowly moving to the next one, development. When entrepreneurs construct a solid business model, test it, and refine the prototype through building several MVPs, first customer data flows occur. It is the time when both product and market validation occurs [33, 25]. Therefore, the team is challenged by dealing with strategic decisions, and operational process management [33]. Another issue at this stage is scaling in terms of adding resources to scale the business profitably [23]. This goes along with the study by Wang and others [40], who mentioned the following challenges to be the major: building the product, customer acquisition, funding, leadership & team alignment, and business model.

To conclude, the development stage is only different from the first two stages of the start-up by having less uncertainty since the product or service has a tested prototype ready to go to the market. Nevertheless, it is essential to emphasize that legal and security concerns are still not considered crucial [40]. The start-up at this stage has acquired financing and customers and has a bigger team. Thus, their responsibility to protect the idea or the data gathered grows.

One of the final major stages is defined as becoming an efficient and profitable entity; it is sometimes referred to as the growth or market stage [31]. The main focus is on scaling operations, processes, and systems; they become moderately formal and systematic. Therefore allows to identify the most optimal model for planning the strategy, product improvement directions, and commercialization [38, 14]. The start-up attempts to build strong connections with customers, penetrate the market and diversify the offer [31, 33].

The major challenges is to make a consistent return on the investments made by the founders or investors. Therefore such challenges as legal and security get more attention. The founders start to understand the importance of securing their organization to avoid wasting or losing money on those issues when scaling in the future. Other aspects are establishing market leadership and stay competitive[25].Customer acquisition, product-market fit, and scaling are becoming increasingly perceived as the key challenges by the team [40].

Moreover, the start-up should be able to demonstrate success and can clearly state their requests in terms of what they lack, be it financing or lack of expertise in a given domain. The risk of failure is much lower; the start-up is much more credible at this stage. Several opportunities arise for organizational change or shift of power. [31]

Some authors argue that the market stage is not final, and after the market exist should come; end the cycle of being a start-up and become a working and profitable entity.

A more profound and holistic view of the start-up lifecycle could be found from StarupCommons.org, where start-up has three key stages formation, validation, and growth. However, the model is divided into sub-stages that better explain what processes occur and when. The framework is excellent to use when communicating the stage of the start-up to investors or mentors because it is widely known and accepted (Look at Figure 3)

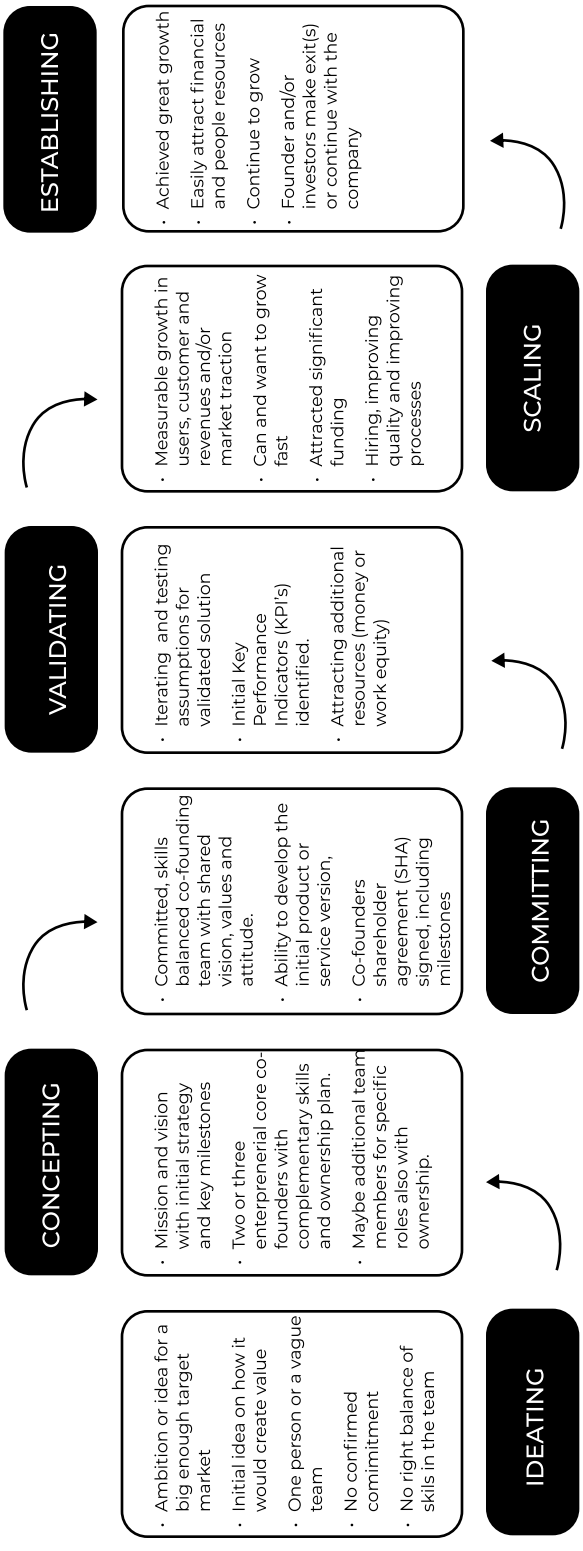

Figure 3. Start-up Lifecycle stages and key activities.
Source: adapted from www.startupcommons.org

To conclude, three main stages are usually identified in the literature, but some authors include two additional, pre-start-up and market exist, to the list. This does not change the essence of the maturing process that is perceived to be non-linear for start-ups, thus allowing to be agile and lean. The following Figure 4 is the synthesis of challenges and risks discussed above at the start-up lifecycle stages.

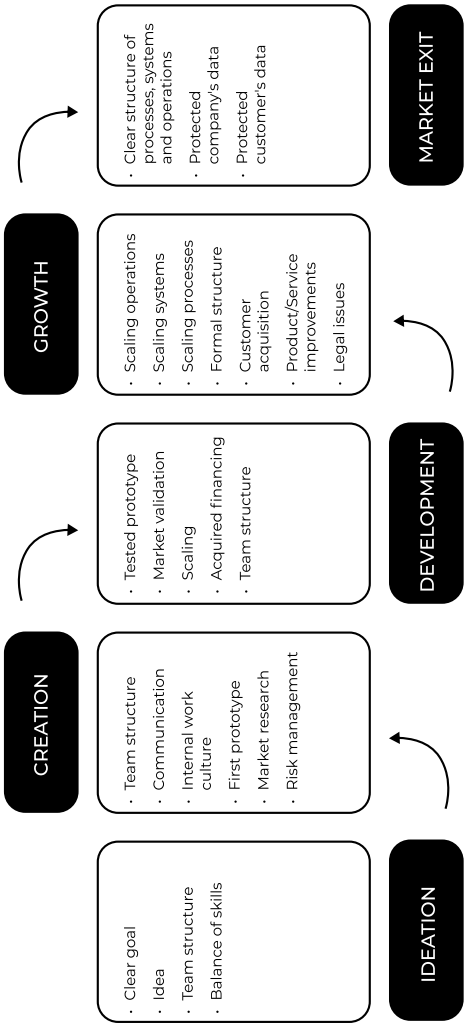

Figure 4. Start-up Lifecycle stages and associated challenges.

2.2 Connection between ISO 27001 and start-up lifecycle

2.2.1 Family of standards ISO 27000

To begin with, various security standards aim at the different aspects, be it cybersecurity or information security. Nevertheless, the aim of the standards is usually the same, to ensure that information within the company is protected and used as intended. The author of this paper has chosen ISO 27001 as a framework for her research for several reasons. First, ISO 27001 is an internationally recognized standard that provides customers and stakeholders confidence that information security risks are managed properly. According to ISO Survey 2020 [20], there are around 44 500 valid ISO/IEC 27001 certificates in 137 countries worldwide, the top three countries are China, Japan, and the UK [20, 4].

Second, ISO/IES 27001 is compatible with most national security standards, for instance, Estonian E-ITS (The new Estonian Information Security Standard), which will replace the current IT Baseline Security System (ISKE) by 2024. Therefore, it is enough to employ ISO 27001 as an information security framework to follow the national requirements. [3]

Third, the standard is audible. It is necessary to meet certification requirements, and the company must also be audited by an internationally accredited certification body [19]. Moreover, the certification is given only for three years, and during that period, the company undergoes the surveillance audits [4], [19]. Finally, there are benefits of following the framework recognized by different authors [4, 29, 3, 36], [19]:

- Provide customers and stakeholders with the confidence that the information risks are managed properly,
- Receive competitive advantage,
- Improve the internal processes in the company,
- Be prepared to face information security threats

ISO 27000 family of standards includes various steps in ensuring security becomes a part of the company's culture and makes it possible to diminish or even prevent security breaches. However, the conformance is perceived by entrepreneurs and business owners as something that would require vast amounts of time, internal resources, and money; something that needs to be done for big companies, not for SMEs or start-ups [12]. There are more than a dozen standards in the family, and they all are designed to apply to any type and size of the firm, from multinational companies to SMEs, which makes it useful for start-ups as well.

In this section, the author intends to describe ISO 27001 and ISO 27002, which are fundamental for the whole family.

ISO 27001

A standardized approach, ISO 27001, makes external and internal users confident that the system they use meets a predefined level of security. However, no standard can guarantee that the system is fully unreachable to hackers under any circumstances. Certification is still optional, but one of the key aspects of following a standard is that partners are more likely to demand an elevated level of security from any firm [13].

The main focus of ISO 27001 is the specification of requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within

the organization [19]. Moreover, ISO 27001 includes Annex A. There are 114 Annex A Controls, divided into 14 categories (controls are denoted further in the work as A.x.x.x). A valuable way to understand Annex A in ISO 27001 is to think of it as a catalog of security controls. The company selects the applicable ones based on the risk assessments, informed by particular risks.

ISO 27002

The general application of ISO 27002 is as a guideline for information security standards and information security management practices, including selection, implementation, and management of controls taking into consideration the organization's information security risk environments. It is a code of practices that outlines mechanisms to be adopted under the provision of the ISO 27001 [20], [16].

ISO 27002 includes 14 aspects (control clauses) that companies must look at when implementing ISMS: Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and environmental security, Operations Security, Communication Security, System acquisition, development and maintenance, Supplier relationships, Information security incident management, Information security aspects of business continuity management, Compliance.

It is essential to understand that these control clauses will become more critical and evolve while the start-up develops. For instance, the Policy for information security is a living document that would reflect the current and projected environment of the company and its business strategy. Thus it should be reviewed after each stage of the start-up to add more details.

2.2.2 Ideation stage and ISO 27001 controls

To connect the start-up lifecycle stage and ISO 27001 controls, the author first briefly describes the key challenges elaborated previously (see subsection 2.1.2) and then explains what control could match them. It is important to note that several assumptions were made to make the connection more coherent.

The first assumption is the growing level of expertise in a start-up moving along the lifecycle. As for the level of expertise, the learning curve theory was employed; with the idea that the more founders work for the start-up, the better they get at resolving challenges [42].

The second assumption is growing financial resources. As the start-up matures, various funding options become available; in the early stage, the main financing option is family and friends; later on, capital funding is considered the primary source, be it equity or debt financing. Therefore, the maturer start-up is, the more financial resource it has, and thus, money can be spent on the gradual implementation of security controls [27], [32].

The Ideation stage is associated with the following challenges: define a clear goal and direction, idea, team, and what skills will be needed in the future. Therefore questions of what information, resources, and assets are needed to achieve the goal, how new information is used, whether it should be protected, and if yes, then how, who has specific responsibilities over various aspects should be raised on the team's meetings and discussed thoroughly.

However, at this stage, most of the security controls are excessive and do not add value to the start-up's future. Nevertheless, protecting against the loss of the data (A.12.3) and ensuring that the information that is involved in daily processes is appropriately protected is crucial. It allows the team not only to design their first security policies but understand what they work with and how sensitive it is (A.8.2).[6]

The development of a product or service is challenging. To ensure that the process is not interrupted, the development, testing, and operational environments should be separated; this brings agility to the processes and reduces the risks of unauthorized access or changes to the final product or service (A.12.1.4).

Team structure and management were noticed as the critical challenges at the Ideation. Therefore, ensuring that the team does not bring any additional risks to information security is crucial. Team has to be aware of their information security responsibilities in order to do so it is advised to allocate specific roles to the members (A.6.1.1). Allocation of roles establishes the management framework and guides others when they have any requests.

Alternatively, in case of any incidents, everyone should be aware of whom they can approach with their issue to resolve it in an effective manner. If the team works with sensitive data, screening of people who could have access to it should be conducted to secure the data (A.7.1.1). Moreover, access control would protect data from unauthorized view. Securing the credential by different means should be in place already at the early stages to create fundamentals for implementing future security controls [6].

Communication within the team is one of the most significant challenges. Choosing how the information is transferred and what systems and devices are in use all have to deal with preventing unauthorized access (A.9.4). Another method is network security management. It is early for a start-up to deal with all the controls in security control clause A.13 but making sure that the WIFI that is used by the team is adequately secured is one small but effective step toward information security [6].

Access control, information classification, backup, and communication security are crucial to consider even at the early stage.

2.2.3 Creation stage and ISO 27001 controls

The second stage of the start-up is associated with the following groups of challenges: a place of work, communication, internal work culture, and risk management. The place where the team meets and works together collaboratively is supposed to have suitable communication devices, including methods for securing remote access. Since start-ups do not usually have their own office at this stage - it is crucial to secure a non-traditional work environment (A.6.2.2). To secure the environment, one should consider providing the team with their own network service and allowing only authorized users to access it (A.9.1.2) [6]. The team members need to be aware that the physical security of the devices that hold sensitive data about the product or service they are developing is critical. Depending on the resources and assets obtained by that point, the implementation phase of the control A.11.1.3 will be different.

As was noticed, communication is critical, but who the team contact in case of any incidents is even more critical. Appropriate contacts with relevant authorities would mitigate the risks and improve the knowledge of security information (A.6.1.3). Moreover, contacts with specialists or interest groups should be maintained, thus learning best practices, staying up to date, ensuring understanding of security environments, and sharing information about new technology, threats, and practices (A.6.1.4) [6]. However, the management should require all team members to apply information security practices that were created throughout the first and second stages of the start-up (A.7.2.1).

Internal work culture relates to values and traditions that make a business unique. If one of the

main principles is to keep the customer's data protected, team members should be aware of how to protect the start-up systems. Confidentiality and password management are two concepts that would make life easier for the team, ensuring that authentication information is not shared with anyone who is not supposed to have access. Using a strong password or passphrase is a relatively easy measure to prevent unauthorized users from accessing or disclosing information (A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2). The Creation phase is the time when a start-up implements its password management system ([6]) that would ensure the quality of passwords (A.9.4.3).

Nevertheless, physical security of the equipment is also necessary; users should not leave unattended equipment without appropriate levels of protection (control 11.2.8). An excellent practice to manage the assets on the table and organize the way of work would be a clear desk policy that allows agility and extra security (A.11.2.9). To help to organize the process in a start-up, development, testing, and operational environments should be separated; this control was already mentioned for the Ideation stage, but during the creation stage, the control should already be fully implemented (A.12.1.4).

The first working prototype brings more security challenges; the first project for the start-p is the creation of the prototype; therefore, it is time to practice information security and make sure that the service or product is secure (A.6.1.5).

2.2.4 Development and ISO27001 controls

The third stage of the lifecycle is Development; it is associated with the following groups of challenges: tested prototype, legal environment, market validation, scaling, acquired financing, team structure, and internal work culture.

To begin with, the tested prototype brings various concerns. The focus should stay on the integrity and confidentiality of the information used by all the systems. Therefore, policies regarding the cryptographic controls, cryptographic keys, rules for the Development, and principles of secure engineering systems should be established and thoroughly used (A.10.1.1, A.10.2.1, A.14.2.1, A.14.2.5).

It is not necessarily that start-ups fully employ all these controls at this stage. However, it is possible to get started with the controls and ensure their proper implementation with the level of expertise and financial resource. Moreover, a secure development environment should be established to test security features (A.14.2.6, A.14.2.8).

To allow continuous safe work, acceptance testing programs and related criteria must be in place for new systems (A.14.2.9). The start-up needs to create a policy that would have guidelines for dealing with security events, be it a human error or access violations (control 16.1.2) [6]. Since, at this stage, a start-up might or might not have a full-time information security specialist, it is still necessary to have a point of contact in case employees or contractors suspect information security weaknesses (A.16.1.3).

Therefore, the start-up scales more responsibilities from the legal perspective; understanding the legislation applicable to the start-up, where to seek legal advice, where the documents related to information security are stored, and how to review the requirements are aspects to consider [6]. As it was noted before, at the Development stage, the start-up already has particular expertise and financial resources; therefore, it is possible to invest money not only in growth but in legally protecting the start-up (A.18.1.1, A.18.2.2, A.18.2.3).

Scaling can be viewed from different perspectives. For instance, a start-up may have new

employees to whom the access rights are granted. Therefore it is time for the formal provision and allocation of privileged access rights. Since more people perform modifications of different kinds and the structure of the team is yet to be perfect, the following questions should arise whether it is possible to access, modify or use the systems without detection and authorization, whether there are conflicting duties for some members of the team, how the rights are restricted and controlled (A.6.1.2, A.9.2.2, A.9.2.3). [6]

Another perspective is in terms of the systems the start-up has, and it might be the case that there is a need for extra facilities to keep up with the growth pace (A.17.2.1). It was already noticed that the security by design approach is the key to the efficiency and effectiveness of security requirements. Therefore, establishing healthy internal work culture is one of the priorities. Moreover, media might become a part of processes. Thus, understanding how to deal with it (should it be removed, unrecoverable, where the track of removed items is kept) is crucial to reaching the overall security (A.8.3.1, A.8.3.2, A.8.3.3).

The next step is understanding key aspects of the environment where the work is conducted, the configuration of the network, the way the information is transferred, agreements with external parties regarding the information transfers, the security of data exchange, and the way systems are configured and installed, and the way backup is done (A.12.1.1, A.13.1.3, A.13.2.1, A.13.2.2, A.14.1.2, A.13.2.3).

The disruptive events happen at all stages. However, up until now start-ups would not have enough resources to establish risk management policies that would allow not only to deal with the ad-hoc events but, in the first place, prevent them (A.17.1.1, A.17.1.2, A.17.1.3).

2.2.5 Growth and ISO 27001 controls

As it was noted in previous sections, the growth phase is about scaling, be it systems, operations, processes, or teams. Thus controls that could potentially cover those topics were mapped to this stage. For instance, physical and environmental security controls (A.11) should be taken into account at this stage if star-up wants to prevent unauthorized physical access, damage, and interference to their information and information process facilities. It is important to note that these controls would only apply if the start-up has a place of operations, be it rented or owned.

Moreover, the key control to ensuring correct and secure operations of information processing facilities is Change management (A.12.1.2). The change processes should be controlled in the particular team has to:

- identify and record the most significant changes;
- plan and test the changes to be;
- assess the impact of potential changes;
- communicate changes.

Scaling might mean new suppliers; therefore, information security should be considered in this regard as well (A.15). A.14 has clear guidelines to ensure that systems during this phase are enhanced. It suggests that information security becomes a part of information systems across the entire lifecycle [6]. Moreover, most of the controls necessary for fulfilling clause A.14 can be

applied using cryptographic controls (A.10). Some of them should have been realized in an earlier stage of development.

As it was mentioned, people are key to all processes. Therefore, controls dedicated to legalizing the relationships within the start-up are necessary at this stage (A.7.3, A.7.1.2, A.7.2.2, A.7.2.3, A.13.2.4). A growing number of employees means more concerns about security for a start-up; thus, reviewing the users' access rights, removing and adjusting them, and restricting or controlling the use of utility programs are the controls that should take place and be developed thoroughly during this stage (A.9.2.5, A.9.2.6, A.9.4.4). [6]

In the previous stage of a lifecycle, the work on how to deal with information security events had to start; however, more work needs to be done during the development stage because of all the internal challenges mentioned earlier in this paper (A.16.1.4, A.16.1.5, A.16.1.6). The control (A18.2.1) is related to compliance with how the clauses approached, managed, and if they are implemented according to the standard.

2.2.6 Market exit and ISO27001 controls

The last stage of the start-up lifecycle is Market exit. As it was noted in the previous sections of the paper, it is associated with the following challenges: clear structure of the processes, systems, and operations, protection of customers and company's data. The research has shown that it is when start-ups start thinking about security controls because of the legal obligation [6], [40].

The author's assumption for this stage was that the start-up is mature enough to maintain supplier relationships; therefore, there is a need to regulate them. Thus, controls that belong to A.15 are associated with this stage. Moreover, another assumption that was made is that by this phase, the start-up should be able to fully implement most of the controls so that the exit to the market is safe in terms of information.

2.3 Answers to Research Questions 1 and 2

In this Section we defined the start-up lifecycle model and reviewed the challenges associated with each stage to answer the question "What are the main steps in the start-up lifecycle?" (**RQ1**). This question was broken down into two sub-questions.

What are the main stages in the start-up lifecycle? - Five stage were defined: Ideation, Creation, Development, Growth and Market Exit. **What challenges are associated with each of the start-up lifecycle stage** - Challenges were reviewed and Figure 4 was compiled to answer this question.

Then Section answered **RQ2** "How ISO 27001 controls are related to start-up lifecycle?". Based on several assumptions, growing level of expertise and increasing financial capabilities with each next stage of a lifecycle, it is possible to connect activities and challenges of each start-up lifecycle stage with information security controls. This section described how to incorporate security and privacy into each stage of a start-up lifecycle. Moreover, how to scale information security within the start-up as it grows.

3 Development of Information security in a start-up

3.1 Maturity model and Information security themes

Information security requirements have become a complex concept that includes technical terms and standards that are difficult to understand for someone new to the field. Therefore, it is uneasy for start-ups to be aligned with overwhelming information security requirements and follow up on their development. This Section provides answers to **RQ3** "How the development of information security controls can be followed?" and **RQ4** What information security themes are essential at each stage of a start-up lifecycle?. To answer RQ3 author first gives an overview of the existing maturity models and then elaborates on a new one specifically for this study. To validate the model author creates a survey, and based on its results, the author arranges information security controls into several themes by lifecycle stage, thus answering RQ4. To visually depict the activities for this section, the following Figure 5 was compiled.

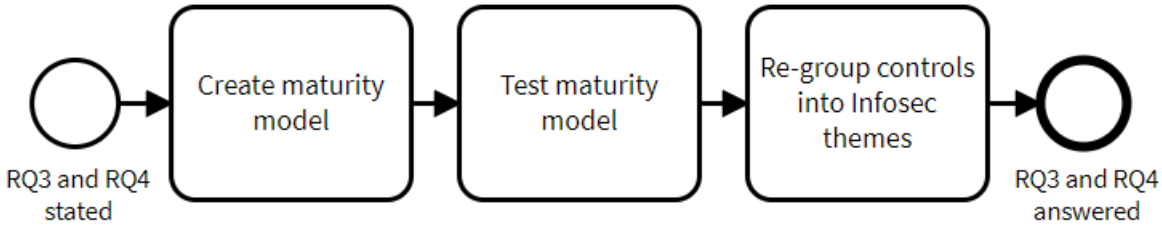

Figure 5. Overview of key activities for Research Questions 3 and 4

3.1.1 Information security maturity model

The Performance evaluation part of ISO 27001 focuses on monitoring, measuring, analyzing, and evaluating controls. ISO 27001 provides the organization with the tools to understand the information security risks. However, it does not allow the organization to measure the progress of the framework implementation, in other words, it does not show the maturity levels and information security processes capabilities. Therefore, the maturity model is needed to measure the information security process capabilities of a firm in a given state. Some of the frameworks for information security have specific maturity models, for instance, COBIT and ISF; their models are used widely for IT governance. Also, the O-ISMS3 model is particular to the management of information security. ONG C2M2 and SSE MM are used for information security frameworks such as ISO 27001 that do not have a specific maturity model.

The following models SSE CMM, ONG C2M2, ISF MM, and COBIT PAM MM, were studied, and the focus was to create the model that would be suitable for the research goals of this paper[11, 24, 18, 21].

Unlike the other maturity models, ONG C2M2 is a three-scale model that assesses ten information security domains, making it the simplest to comprehend. The domains of the model comply with the clauses in ISO 27001, which makes it compatible to use within the framework. Moreover, it correlates with NIST Framework. [24, 21, 18]

While SSE CMM, ISF MM, and PAM MM are five scale maturity models, they all have a different understanding of each level; thus, the problem of mapping the levels of maturity does exist. According to the previous research made on these models [1] some of the levels of maturity do not exist in other models meaning that there is no one-to-one mapping. For instance, SSE CMM L2 (Planned and Tracked) cannot be mapped to any levels of other maturity models. Moreover, information security areas that these models cover differ and cannot be mapped one-to-one either. For instance, "Cyber security Program Management" in ONG C2M2 is possibly mapped to several different areas in other models because it covers the aspects that were separated in other models into sections. In SSE CMM "Administer Security Controls" and "Specify Security Needs" can be compared to above mentioned part of ONG C2M2. [1, 37] All in all, models are inconsistent, and it is impossible to map the level of maturity one-to-one. The next issue is that the areas of information security that models cover are different from model to model; even though they correspond to some parts of the chosen framework, ISO 27001, it is still risky to use any of them. Moreover, the models are industry-specific, thus the purpose of use does not allow to use of any of them for current research.

Therefore, the author of the paper decided to create a model considering previously reviewed models. The main argument for creating a new model is a need to tailor a model that start-ups would easily understand at the early stages of the development. Moreover, the author considered methods and approaches to building maturity framework [2, 17], they would suggest to have five levels as the previously discussed maturity models, therefore, the decision to make the proposed maturity model a five-level scale was justified.

The author has recognized that all models follow the same pattern. The first level is to have the process or control in place; it might be partially implemented but yet should be recognized. The next level is when the control or practice is fully implemented, meaning that it corresponds to the stage of the start-up's overall maturity and covers its current needs. The third level is when control is reviewed, so an initial analysis of how the implementation process went, the result is performed, and how to improve it is clear. The fourth level is when the process is improved according to the findings of the previous analysis, the last level usually describes the process to be fully optimized. Therefore, all models follow the pattern of partially improving the process from one level to another, reaching the most optimized way of doing it. For the purposes of this research and with the knowledge that information security is not considered an issue to address at the early stages of start-up (cite), Level zero is added to the model. Level zero describes the state where the initialization of the process has not started yet; the start-up is not aware of the information security control and the need to implement it. The following figure represents the aggregation of the author's knowledge and shows the levels of the model and their characteristics. It is important to note that a set of attributes defines each level. To assign a level of maturity to a start-up, it has to demonstrate the attributes and achieve the level's capabilities. Having measurable transition states between the levels enables an organization to use the scale to:

- define its current state
- determine its future, more mature state
- identify the capabilities it must attain to reach that future state

To give a better understanding of how the maturity model evaluates the information security control, the author has compiled the following table (Table 1). The Access control policy (A.9.1.1) was

chosen for an evaluation. This control focuses on determining appropriate access control rules, access rights, and restrictions for specific users and assets that belong to them, taking into account various external and internal factors that may affect those rules in a particular manner. The control has several attributes that have to be considered when implementing it, such as segregation of access control roles, management of access rights, removal of access rights, etc. These attributes can be implemented beforehand or as soon as required. It is essential to note that two principles are directing this control: need-to-know basis, when access to information is granted to the person who needs to perform the tasks, and need-to-use basis when access to processing facilities is granted to the person who needs to perform the task.

Finally, Appendix B was compiled as synthesis of the Section 2.2 and the Section 3.1.1. A maturity level was assigned to each information security control at different start-up lifecycle stages. Appendix B is a subjective vision of how information security controls could develop based on the knowledge gained throughout the research.

Table 1. Maturity model

Level	Name	Characteristics	References	Example
Level 0	Plan to work on it soon	Practices are not performed.	[18], [21],[1]	Start-up is aware of the Access control policy (A.9.1.1) and the need to implement it.
Level 1	Partially implemented	Initial practices are performed but maybe ad-hoc.	[18], [21],[1]	The policy is in the process of implementation, it has some relevant aspects but not all of them, for instance, it covers security requirements of business applications but not removal of access rights. However, the removal of access rights guidelines undergoes discussions.
Level 2	Fully implemented	Practices are performed, documented, and complete or more advanced than at Level 1.	[1], [37]	The policy is in place and corresponds to the level of the start-up overall maturity.
Level 3	Fully implemented and reviewed	Practices are performed and guided by policies. The effectiveness of activities is evaluates and tracked.	[24], [21],[18]	The policy is in place, it was reviewed and the missing elements are identified. For instance, start-up has been growing and now need to introduce the privileged access rights, this should be denoted and implemented.
Level 4	Fully implemented, reviewed and continuously improved	Practices are improved, more complete or advanced than at Level 3.	[24], [21],[18]	After the revision, start-up continuously improves access control policy and adds new elements to it as soon as they appear.

3.1.2 Information security themes and start-up lifecycle

Section 2 mapped information security controls with activities and challenges of each lifecycle stage. The author created an Infosec survey to prove that start-ups consider information security throughout their lifecycle. The survey structure closely follows the format of the ISO 27001 standard; it was made so to include as many Infosec controls and reflect the idea of the standard. To be more precise, the survey consists of the following topics: Security requirements, Management directions for information security, Organization of information security, Human resource security, Asset management, Acess control, Information classification, Cryptography controls, Physical and environmental security, Operations security, Compliance, and Communication security. Questions from the blocks of Asset management, Cryptography controls, and Physical and environmental security were only asked if the start-up fulfills the requirements. For instance, questions related to cryptography only asked if a start-up has a formal written policy on the use of cryptography controls. However, the first set of questions addressed the start-up lifecycle stage and the demographics of the start-up, in Table 2, one can find how the stage is defined, it is the synthesis of the knowledge gained in Section 2.

Table 2. Defining start-up lifecycle stage

Lifecycle Stage	Team	Financing	Idea	Market acquisition	Years of operations
Ideation	1-3 ppl	Friends and family	There is only idea	No market acquired	0-1 y.o
Creation	4-10 ppl	Crowdfunding	Initially validated idea	No market acquired	1-2,5 y.o
Development	10-20 ppl	Pre-seed or seed, angel investors	First prototype	Early adopters	2,5-4 y.o
Growth	20-50 ppl	Angel investors and/or Venture capital	Minimal Viable product	Found first customers	4-5 y.o
Market Exit	50+ ppl	Self financing, IPO	Product/Service is developed	Market is acquired	5-10 y.o

Overall, the survey included 73 questions (See Appendix A).

Estonia was chosen as a target country due to the high number of start-ups in the region and high level of start-up ecosystem development ([39]).

The survey was distributed via numerous online channels (Facebook, Instagram, and LinkedIn).

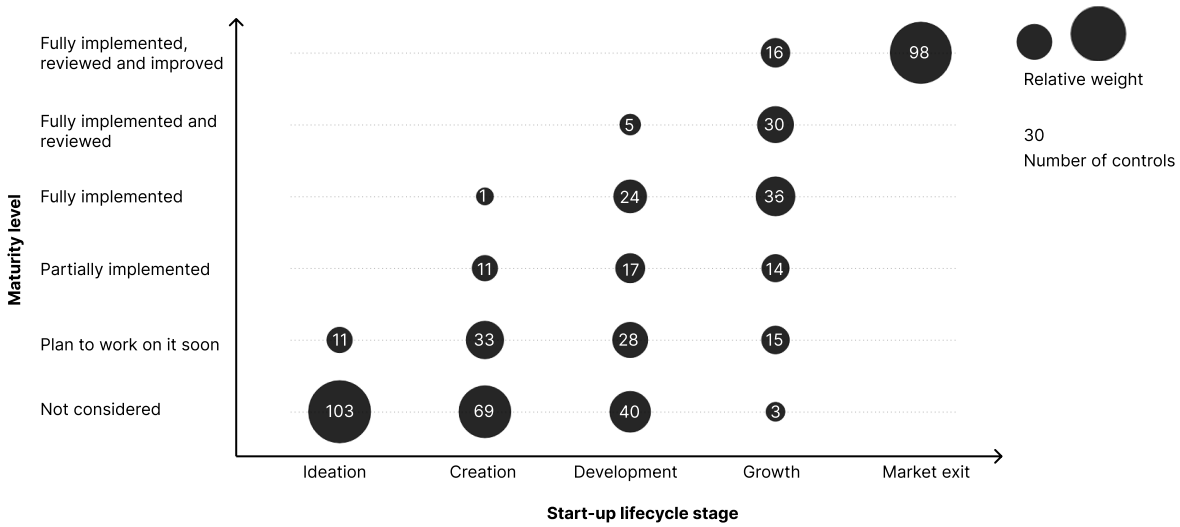

Figure 6. Number of information security controls by start-up lifecycle stage and maturity

Moreover, the author contacted different incubators (Prototron, WiseGuys, Tartu Science Park, IdeaLab) to reach start-ups at varying levels of development.

In total, the author received eleven answers to the survey. The distribution by the start-up lifecycle stage was the following two start-ups at the Ideation stage, three start-ups at the Creation stage, two start-ups at the Development stage, two start-ups at the Growth stage, and one start-up at the Market exit stage. Start-ups that participated in the survey belong to FinTech, CyberTech, and Consumer Products and Services branches. The dominating business model adopted was Business to Business.

These answers allowed the author to map the information security controls to the lifecycle stages, and with the knowledge gained in Section 3.1, the author has created Figure 6. Three main conclusions from Figure 6 are that start-ups at the Ideation stage do not consider most of the information security controls and only plan to work on specific controls. None has been implemented yet. However, the situation changes within the Creation stage. As was already mentioned, commitment plays a crucial role in the Creation stage. Thus start-up is ready to partially or fully implement several controls. Moreover, the awareness of information security increases as many controls have a level of maturity "Plan to work on it soon". The process itself, according to Figure 6, is linear; controls move to the next level of maturity at each stage of a lifecycle. By the growth stage, 16 information security controls reached the highest level of maturity, Level 4. Therefore, only 98 controls reached Level 4 at the Market exit stage. Nevertheless, this Figure 6 does not give a sense of what areas are covered during the start-up development.

For this purpose, controls were regrouped into new or similar themes as in ISO 27001. The following themes emerged: Communication security, Data Privacy, Software security, Cryptography, Incident response, Equipment security, Identity and Access Management, Operations security, Compliance, Privacy, Human Resource security, Security management, and Supplier relationships.

Table 3 was elaborated to highlight information security themes at each stage of a start-up lifecycle.

Table 3. Essential Information security themes by start-up lifecycle stage

Lifecycle Stage	Theme
Ideation	Communication security, Operations security, Identity and access management
Creation	Software security, Privacy
Development	Incident response, Human Resource security, Data Privacy,
Growth	Compliance, Equipment security, Cryptography
Market Exit	Supplier relationships

Identity and access management, Communication security, and Operations security were considered essential by [6] and start-ups participated in the survey. Eight out of eleven participants started working or implemented those controls on the early stages see Table 3).

Supplier relationships, Cryptography, and Equipment security carry redundant features and cause more complexity rather than security. [6], only two start-ups out of eleven started implementing these controls, and their lifecycle stage was Growth and Market exit(see Table 3).

3.2 Answers to Research Questions 3 and 4

In this Section, author created Maturity model for start-ups to employ. Therefore, RQ3 "How development of information controls can be followed?" is covered by the model (see 6).

Moreover, this Sections covered RQ4 "What information security themes are essential at each stage of a start-up lifecycle?". To answer this question the survey that evaluates the start-up lifecycle stage and maturity of different information security controls was created.

The information gathered was developed into the model (see Figure 6). The main idea of which to show the development of the controls during the start-up life. The model is high level and has no differentiation by information security topics however, it shows that most of the controls should start being developed already at the Ideation and Creation stages (for instance, controls related to Access management and Privacy).

Nevertheless, survey results allowed to regroup information security controls into new twelve information security themes and create Table 3 which shows essential information security topics at each stage of a lifecycle.

4 Validation

This section focuses on validating Table 3 and creating an information security assessment model out of it. Thus, answering RQ5 "How to assess information security as a whole in a start-up?". For validation purposes, author conducted nine interviews with different start-ups to get in depth information about the approaches used by them to build up information security layers. First, methodology and data collection are introduced. Then findings are described.

4.1 Methodology and data collection

In the following section, the author of the paper introduces the way interview plan was crafted, what method of data collection is used to fulfil the research aim, the framework for the analysis of the acquired data, and the primary data overview.

Firstly, deductive approach was adopted. The hypothesis that is derived from 3.1.1 that information security controls are implemented depending on the stage of start-up lifecycle, they have certain maturity framework and at each stage of the start-up lifecycle controls are at the certain maturity level. From the literature review, there was no opportunity to see the pattern because such studies were not made before. However, author conducted a survey to grasp the concept and create the model (see Figure 6).

Secondly, the method of gathering the data chosen is web-based one-to one interviews. The method was chosen as the most common research method, qualitative method dominates in this kind of research [37]. Semi-structured interviews make it possible to collect more details and accurate answers [41]. Finally, the sampling method that is in use is purposive sampling. It means that participants of the research were chosen in a strategic way, so that people participating in the semi-structure interviews were relevant to the research. Meaning that they have enough expertise and knowledge to make adequate and relevant conclusions. However, this kind of the sampling does not allow to generalise to a population [5]. Overall, 9 interviews were conducted from 20 to 90 minutes. The following Table 4 is the representation of the sample.

Table 4. Overview of research participants

Start-up id	Industry	Stage of start-up lifecycle	Founders have experience
1 Startup A	Business software & HR	Development	Yes
2 Startup B	Business software	Growth	Yes
3 Startup C	EdTech	Development	Yes
4 Startup D	EdTech	Growth	Yes
5 Startup E	Communication	Market exit	Yes
6 Startup F	Communication	Ideation	No
7 Startup G	FinTech	Growth	Yes
8 Startup H	Culture	Creation	No
9 Startup I	Consumer products and services	Ideation	No

In order to conduct interviews, the plan was crafted. It has 14 core themes that are derived from the analysis of ISO 27001 standard (see Appendix A). Moreover, the standard itself and findings from the Figure 4 were the basis fro making up interview questions; the initial version of the interview was given to a co-founder of Start-up A who has relevant experience and expertise for research. His7her review and comments on the interview question prompted the author of the paper to re-think the structure of the interview and questions included. Moreover, irrelevant question were excluded and changes to the structure were made. Overall, the purpose of the interview was to discuss information security topics and map them to different stages of the start-up lifecycle.

The interviews were held in English, each interview started with a short introduction to the topic and introduction of the model created by the author (see Figure 6). The first part of the interview included question about interviewees' understanding of the information security concept, clarifying questions on information security standards and their use for start-ups. The second part of the question were developed to identify the start-up lifecycle stage, therefore questions were based on Section 2. Third part of the interview was a retrospective for mature start-ups, understanding their actions towards information security and current overview of the actions for start-ups at early stages. Fourth part of the questions focused on the current actions for mature start-ups and future actions for early stage start-ups. Fifth group of questions was a closing part to check if any information was missing and if the interviewees had any other questions not addressed during the interview.

4.2 Findings

The preliminary assumptions based on the survey results (see Figure **??** were that at early stages of a start-up lifecycle vast majority of information security controls are not considered by the start-ups as points of development. Moreover, based on Table 3 the main information security topics are Communication security, Operations security, and Identity and access management. However, the results from the interview give a more extensive picture (see Figure 7). The results suggest that not only three themes mentioned before should be considered at the Ideation stage of a start-up lifecycle. Compliance, most commonly to General Data Protection Regulation (GDPR) was mentioned by two out of nine start-ups.

Figure 7. WordCloud Ideation.

Moreover, Software security and Privacy was mentioned by start-ups with extensive prior knowledge and experience. Meaning that founders that had start-ups before, or had work experience tend to develop more information security themes from the Ideation stage than their counterparts with less experience. Finally, the main focus for the Ideation stage as noted by Start-up A, Start-up B, Start-up E and Start-up G should be on

- define data capabilities to protect,
- determine systems to protect,
- determine people with access to the system to protect.

One discrepancy, between the survey and the results presented in Figure 7, Operations security was not mentioned by any of the start-ups participated in the interviews, as a theme for early stage rather for later stages of the development. This might be explained by the fact that the most growth happens at the Development stage of a start-up lifecylce and therefore this theme was assigned there.

Survey resulted in two themes being critical for the Creation stage of the lifecycle, this view was validated by the answers provided by the interview participants (see Figure 8). Moreover, Operations security and Identity and Access management(IAM) were mentioned by seven out of nine and five out of nine start-ups respectively. Explaining their choice by the need of having proper Backup plan at this stage since founders are getting committed to the idea and more documentation, elaboration of the idea appears. Moreover, the installation and configuration of the systems fall under Operations security, and becomes an important information security control because founders looking for the tools to create solution.

Figure 8. WordCloud Creation.

The next interesting theme that was mentioned by Start-up C and Start-up D, their industry is EdTech, the supplier relationships. This theme was brought up because they are heavily dependent on the counterparts therefore non-disclosure agreement or any other types of agreement related to the secure transfer of information are essential for them. Several start-ups brought up Human Resource security as being important at this stage, it was mainly because those at the Creation stage started looking for new team-members therefore they had to sign employment agreement. Important to note that at first, not all start-ups considered employment agreement as an information security measure. Finally, the main focus for the Creation stage as noted by Start-up C, Start-up D and Start-up G should be on:

- determining the operating systems to support,
- reviewing terms and conditions with suppliers and vendors,
- removing all shared accounts and providing each participant with individual account,
- implementing a password manager,
- implementing multi-factor authentication on all cloud infrastructure.

As for the Development stage of the start-up lifecycle, Incident response, Human Resource security and Data Privacy were denoted essential by the survey participants. However, neither Human Resource security nor Data Privacy were not mentioned by the interview participants, this might be due to the reason that they have attached these topic the the earlier stage of the lifecycle (see Figure 9) .

Figure 9. WordCloud Development.

It is important to note once again, that majority of interview participant had extensive experience and knowledge in information security area as well as it was not their first start-up. Therefore, they might start considering some of the Infosec themes earlier. Incident response was noted as the most important at the Development stage, explaining it by having the first prototype and testing the market fit therefore the product or service appear on the web and need extra layers of protection.

The second most important information security theme at this stage is Operations security. It was mentioned again by several start-up because the most development of the product and the creation of the first test version are happening at this stage, therefore such controls as event logging, protection from malware, control of operational software and management of technical vulnerabilities become increasingly important to consider and fully implement.

Furthermore, Privacy was mentioned by five out of nine start-ups. By Privacy they mainly considered the the privacy of internal processes and how protected the data on the company are, for instance, the financial statement, employee contracts and their personal data. This was brought up because usually at the Development stage, start-ups are scaling in terms of people therefore additional attention is needed to cover this aspect.

Equipment security is a theme that is brought up for the first time at this stage. It was mentioned by Start-up C and Start-up E that at the Development stage they have acquired company's equipment, laptops, and that they started thinking at that time how to approach in terms of information security.

Finally, the main focus for the Development stage defined by Start-up A is :

- make sure your devices are secure,
- focus on protecting data,
- turn on available security controls on your cloud provider,
- document as much as possible.

The next stage is Growth, survey resulted in the following information security themes: Compliance, Equipment security and Cryptography. The first two themes has already been discussed and taken into consideration earlier by the start-ups participating in the interviews. The most important information security theme considered by the participant was Security management. This is related to the activities of the start-up at this stage; since the Growth stage is about scaling of systems, processes, and operations, therefore formal documentation of them is necessary.

Figure 10. WordCloud Growth.

Human resource security is brought up at this stage once again because new people are involved in the start-up therefore, more consideration should be given to that topic (Start-up G and Start-up E). Moreover, if some people has already left the start-up, it is useful to check whether they still have access right to any system.

Compliance is becoming more important at this stage because start-up gets involved in relationships with external systems therefore, it should be able to recognise what Industry and Government standards and regulations are applicable to it and how to follow them.

Furthermore, Cryptography at first was not noted by mature start-ups as a separate information security topic. They would mention using built-in solutions rather than creating their own cryptography controls.

Finally, the main focus for the Growth stage suggested by start-ups is:

- review relevant regulations to comply with,
- create a guidelines for new member regarding the way information security is treated in the start-up,
- add a security section to the product or service website,
- review and improve previously created information security policies.

As for the Market exit, all nine start-ups agree on the point that it is time to review what was done before and improve it. By that stage, no more new information security topics should appear and it was suggested to elaborate those that lack attention on the previous stages.

After analysing the interviews the following assessment table was created. It was suggested that at each stage of start-up lifecycle

4.3 Answers to Research Question 5

To answer **RQ5** Table 5 was elaborated where information security themes are shown at stage of a lifecycle and the stage of their development according to the maturity model created in Section 3. It is possible to assess the information security maturity of a start-up as whole however, it has its limitations and considerations.

Table 5. Information security assessment model for each stage of a start-up

Lifecycle Stage/-Maturity Level	Ideation	Creation	Development	Growth	Market Exit
Level 1	Privacy, Compliance	Data privacy	HR security	Equipment security, Cryptography	
Level 2	Communication security, IAM, Software security	Operations security	Compliance	Privacy, HR security, Security Management	
Level 3		Communication security, IAM, Software security	Incident response, Operations security, Data privacy	Compliance	
Level 4			Communication security, IAM, Software security	Operations security, Data Privacy, Incident response, Compliance	
Level 5				Communication security, IAM, Software security	Privacy, Data privacy, HR security, Compliance, Incident response, Operations security,Security management, Equipment security

5 Thesis summary

This thesis gives an overview of the Information security framework for start-ups. The work resulted in the Information security assessment model for start-ups that can be used as a reference of when to approach certain information security topics. The model contributes to the explicit understanding of the information security and its process in start-ups. Three main conclusions were made:

Conclusion 1 The way information security is approached in start-ups depends on the expertise and previous experience of the founders. The more experience founders have, earlier they start build foundations for the information security controls.

Conclusion 2 Even though ISO 27001 controls can be mapped to the start-up lifecycle stages, such framework can be used as a reference only. Each start-up participated followed its unique way of developing depending on various external factors.

Conclusion 3 In some case start-up were not aware that they were using information security controls.

Conclusion 4 There are other contributing factors except from the founders expertise that should be researched further, for instance industry and financial capabilities.

5.1 Limitations

Even though the topic of InfoSec is widely discussed for the past years, author still encountered limitations considering the literature in hand. As mentioned in the introduction, there are very few academic studies available regarding the information security in start-ups and maturity level of it. Most of the available non-academic papers about the topic are white-papers or technical documents or specifications. Due to this, the research is limited by performing the research only on available literature.

The second limitation is the sampling method and number of participants. With the current setup the conclusions cannot be generalized to public. Therefore, the validation of the results might have low accuracy. Due to this, another validation approach might result in a different model, by selecting different region or/and sampling method, for instance.

5.2 Answers to research questions

This thesis research questions were:

MRQ "How information security is developed throughout the start-up lifecycle?"

RQ1 "What are the main stages in the start-up lifecycle?"

RQ2 "How ISO 27001 controls are related to start-up lifecycle?"

RQ3 "How development of information security controls can be followed?"

RQ4 "What information security themes are essential at each stage of a start-up lifecycle?"

RQ5 "How to assess information security as a whole in a start-up?"

Research question 1 was answered in the Section 2.1.2 with creating a Figure 4. The answer to research question 2 was given in the Section 2.2, where controls were mapped to the stages via challenges and activities of the stage.

The Maturity model (see 1) was created in the Section 3.1.1 to answer research question 3.

To validate maturity model and re-group controls into new information security themes, survey was created. Thus, research question 4 was answered in the Section 3.1.2.

Section 4 was focused on validating the information security themes by means of interviews and creating Information security assessment model (see Table 5). Therefore, research question 5 was answered in the Section 4.

5.3 Conclusions and future work

This type of research of the information security in start-ups is a first and hopefully a basis for future work. The future version with such reference model would be to see if the model is applicable to start-ups from other regions and how does this model contribute to the general understanding of the information security. By no means this model is complete but the author hopes that this inspires other to do research in this field, bring awareness of information security and develop more frameworks for start-ups to use.

References

[1] Sultan Almuhammadi and Majeed Alsaleh. "Information Security Maturity Model for Nist Cyber Security Framework". In: *Computer Science & Information Technology (CS & IT)*. Academy & Industry Research Collaboration Center (AIRCC), Feb. 2017, pp. 51–62. ISBN: 978-1-921987-62-5. DOI: 10.5121/csit.2017.70305. URL: http://airccj.org/CSCP/vol7/csit76505.pdf (visited on 03/29/2022).

[2] Campbell Australasian Conference on Information Systems Bruce, Association for Information Systems, and Australasian Chapter, eds. *Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005), November 30 - December 2, 2005, Sydney, Australia*. English. OCLC: 225646832. Sydney: Australasian Chapter of the Association for Information Systems, 2005. ISBN: 978-0-9758417-0-9.

[3] Information System Authority. *Cyber Security in Estonia 2021*. 2021. URL: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.

[4] Chloe Biscoe. *ISO 27001 certification figures increase by 20%.* Sept. 2017. URL: https://www.itgovernance.co.uk/blog/iso-27001-certification-figures-increase-by-20.

[5] Alan Bryman and Emma Bell. *Business research methods*. 3rd ed. Cambridge ; New York, NY: Oxford University Press, 2011. ISBN: 978-0-19-958340-9.

[6] Chris Castaldo. *Start-up secure: baking cybersecurity into your company from founding to exit*. Hoboken, New Jersey: Wiley, 2021. ISBN: 978-1-119-70073-9.

[7] National Cyber Security Centre. *Annual Review 2021*. Tech. rep. National Cyber Security Centre UK. URL: https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf.

[8] Henry Chesbrough and Adrienne Kardon Crowther. "Beyond high tech: early adopters of open innovation in other industries". en. In: *R and D Management* 36.3 (June 2006), pp. 229–236. ISSN: 0033-6807, 1467-9310. DOI: 10.1111/j.1467-9310.2006.00428.x. URL: https://onlinelibrary.wiley.com/doi/10.1111/j.1467-9310.2006.00428.x (visited on 03/14/2022).

[9] Daniel Cockayne. "What is a startup firm? A methodological and epistemological investigation into research objects in economic geography". In: *Geoforum* 107 (2019), pp. 77–87. ISSN: 0016-7185. DOI: https://doi.org/10.1016/j.geoforum.2019.10.009. URL: https://www.sciencedirect.com/science/article/pii/S0016718519302970.

[10] Alessandra Colombelli and Francesco Quatraro. "Green start-ups and local knowledge spillovers from clean and dirty technologies". en. In: *Small Business Economics* 52.4 (Apr. 2019), pp. 773–792. ISSN: 0921-898X, 1573-0913. DOI: 10.1007/s11187-017-9934-y. URL: http://link.springer.com/10.1007/s11187-017-9934-y (visited on 03/14/2022).

[11] Pamela D. Curtis and Nader Mehravari. "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure". In: *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. Waltham, MA, USA: IEEE, Apr. 2015, pp. 1–6. ISBN: 978-1-4799-1737-2. DOI: 10.1109/THS.2015.7225323. URL: http://ieeexplore.ieee.org/document/7225323/ (visited on 04/18/2022).

[12] Cath Everett. "Is ISO 27001 worth it?" en. In: *Computer Fraud & Security* 2011.1 (Jan. 2011), pp. 5–7. ISSN: 13613723. DOI: 10.1016/S1361-3723(11)70005-7. URL: https://linkinghub.elsevier.com/retrieve/pii/S1361372311700057 (visited on 03/29/2022).

[13] Edward H. Freeman. "Holistic Information Security: ISO 27001 and Due Care". en. In: *Information Systems Security* 16.5 (Nov. 2007), pp. 291–294. ISSN: 1065-898X, 1934-869X. DOI: 10.1080/10658980701746478. URL: http://www.tandfonline.com/doi/abs/10.1080/10658980701746478 (visited on 03/29/2022).

[14] Nobuya Fukugawa. "Is the impact of incubator's ability on incubation performance contingent on technologies and life cycle stages of startups?: evidence from Japan". en. In: *International Entrepreneurship and Management Journal* 14.2 (June 2018), pp. 457–478. ISSN: 1554-7191, 1555-1938. DOI: 10.1007/s11365-017-0468-1. URL: http://link.springer.com/10.1007/s11365-017-0468-1 (visited on 03/14/2022).

[15] GDPR. *General Data Protection Regulation (GDPR).* Tech. rep. 2018. URL: https://gdpr-info.eu/.

[16] Constantine Gikas. "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards". en. In: *Information Security Journal: A Global Perspective* 19.3 (June 2010), pp. 132–141. ISSN: 1939-3555, 1939-3547. DOI: 10.1080/19393551003657019. URL: http://www.tandfonline.com/doi/abs/10.1080/19393551003657019 (visited on 03/29/2022).

[17] The Departament of Internal Affairs Te Tari Taiwhenua. "Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)". In: *Departament of Internal Affairs on behalf of the New Zealand Government* (2014). URL: https://www.digital.govt.nz/assets/Documents/Privacy-Maturity-Assessment-Elements-and-Attributes.pdf.

[18] ISACA. *Control Objectives for Information and Related Technology (COBIT)*. URL: https://www.isaca.org/resources/cobit.

[19] ISO. *Information technology – Security techniques – Information security management systems – Requirements:* URL: https://www.iso.org/standard/54534.html.

[20] ISO. *The ISO Survey of management system standard certifications - 2020 - explanatory note*. Sept. 2021. URL: https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_and_overview_on_ISO_Survey_2020_results.pdf?nodeid=21899356&vernum=-2.

[21] Joint Task Force Interagency Working Group. *Security and Privacy Controls for Information Systems and Organizations*. Tech. rep. Edition: Revision 5. National Institute of Standards and Technology, Sept. 2020. DOI: 10.6028/NIST.SP.800-53r5. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (visited on 04/18/2022).

[22] Tobias Kollmann et al. *European Startup Monitor 2016*. English. OCLC: 964395485. 2016. ISBN: 978-3-938338-17-9.

[23] Marc König et al. "Different patterns in the evolution of digital and non-digital ventures' business models". en. In: *Technological Forecasting and Social Change* 146 (Sept. 2019), pp. 844–852. ISSN: 00401625. DOI: 10.1016/j.techfore.2018.05.006. URL: https://linkinghub.elsevier.com/retrieve/pii/S0040162517316943 (visited on 03/14/2022).

[24] Ngoc T. Le and Doan B. Hoang. "Can maturity models support cyber security?" In: *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*. Las Vegas, NV, USA: IEEE, Dec. 2016, pp. 1–7. ISBN: 978-1-5090-5252-3. DOI: 10.1109/PCCC.2016.7820663. URL: http://ieeexplore.ieee.org/document/7820663/ (visited on 04/18/2022).

[25] Arthur Marcon and Jose Luis Duarte Ribeiro. "How do startups manage external resources in innovation ecosystems? A resource perspective of startups' lifecycle". en. In: *Technological Forecasting and Social Change* 171 (Oct. 2021), p. 120965. ISSN: 00401625. DOI: 10.1016/j.techfore.2021.120965. URL: https://linkinghub.elsevier.com/retrieve/pii/S0040162521003978 (visited on 03/14/2022).

[26] A.E. Marwick. "Status Update: Celebrity, Publicity, and Branding in the Social Media Age". In: *Status Update: Celebrity, Publicity, and Branding in the Social Media Age* (Jan. 2013), pp. 1–36.

[27] Nir Eyal. "Angel or Devil: Who's Really Investing In Your Start-Up?" In: *Harvard Businss Review* (Nov. 2013). URL: https://hbr.org/2013/11/angel-or-devil-whos-really-investing-in-your-start-up.

[28] *NIS Directive*. Tech. rep. 2016. URL: https://www.enisa.europa.eu/topics/nis-directive.

[29] Janusz G. Nowak. "Information Security Management with accordance to ISO27000 Stadards: Characteristics, implementations, benefits in global Supply Chains". In: (2015). URL: https://d1wqtxts1xzle7.cloudfront.net/38067587/JGNowak_ISO27000_logistyka_2014_EN_revised-with-cover-page-v2.pdf?Expires=1648554025&Signature=RlfigpGB~SwcLPDBlSKEjI05ceGhAdPAIGaYc4NdelYLAvgn52xyCPrsRVy-UfDeSpxaN17mKnv8lWfw4q9djWlqo-O5dWzG3zvLqOJoZHrAiuAUMQIib5PvwYllummmqNz73e1b9BSJFnhQxCntsYesw~Bt5esFg0kJlUyWpsSLkb0LdrLJLR0oF4nizKY2CMORoWYPjASQJ2EArYv08ZIEpU80Bc9N9yQYlSD1WCLu63JoQ807hIJygGtxHyZC5UGkop-qzxUA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA.

[30] OECD OECD. *OECD science, technology and innovation outlook 2016*. English. OCLC: 973555250. 2016. ISBN: 978-92-64-26305-5. URL: https://doi.org/10.1787/sti_in_outlook-2016-en (visited on 03/14/2022).

[31] Jeannette Paschen. "Choose wisely: Crowdfunding through the stages of the startup life cycle". en. In: *Business Horizons* 60.2 (Mar. 2017), pp. 179–188. ISSN: 00076813. DOI: 10.1016/j.bushor.2016.11.003. URL: https://linkinghub.elsevier.com/retrieve/pii/S0007681316301252 (visited on 03/14/2022).

[32] Philipp Cornelius and Bilal Gokpinar. "Crowdfunding Can Deliver More Than Just Money". In: *Harvard Business Review* (). URL: https://hbr.org/2021/03/crowdfunding-can-deliver-more-than-just-money.

[33] Joseph C. Picken. "From startup to scalable enterprise: Laying the foundation". en. In: *Business Horizons* 60.5 (Sept. 2017), pp. 587–595. ISSN: 00076813. DOI: 10.1016/j.bushor.2017.05.002. URL: https://linkinghub.elsevier.com/retrieve/pii/S0007681317300605 (visited on 03/14/2022).

[34] PWC. *Two thirds of UK business leaders expect cyber seurity threat to increase over next 12 month*. Tech. rep. PWC, Nov. 2021.

[35] Eric Ries. *The lean startup: how today's entrepreneurs use continuous innovation to create radically successful businesses*. 1st ed. OCLC: ocn693809631. New York: Crown Business, 2011. ISBN: 978-0-307-88789-4.

[36] Francklin Rivas-Echeverria, Gloria Mousalli-Kayat, and WSEAS International Conference on Information Security and Privacy WSEAS (Organization), eds. *Advances in e-activities, information security and privacy: 9th WSEAS International Conference on E-activities (E-ACTIVITIES-10) : 9th WSEAS International Conference on Information Security and Privacy (ISP '10)*. English. OCLC: 752667549. Greece: WSEAS, 2010. ISBN: 978-960-474-258-5.

[37] Malik F. Salek. "Infromation Security Maturity Model". In: *International Journal of Computer Science and Security* 5.4 (2011), pp. 316–337. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.1617&rep=rep1&type=pdf#page=26.

[38] Jurgita Sekliuckiene, Rimgaile Vaitkiene, and Vestina Vainauskiene. "Organisational Learning in Startup Development and International Growth". In: *Entrepreneurial Business and Economics Review* 6.4 (2018), pp. 125–144. ISSN: 2353883X, 23538821. DOI: 10.15678/EBER.2018.060407. URL: https://eber.uek.krakow.pl/index.php/eber/article/view/470 (visited on 03/14/2022).

[39] Global Entrepreneurship Network Startup Genom. *Global Startup Ecosystem Report 2021*. Tech. rep. 2021. URL: https://startupgenome.com/reports/gser2021.

[40] Xiaofeng Wang et al. "Key Challenges in Software Startups Across Life Cycle Stages". en. In: *Agile Processes, in Software Engineering, and Extreme Programming*. Ed. by Helen Sharp and Tracy Hall. Vol. 251. Series Title: Lecture Notes in Business Information Processing. Cham: Springer International Publishing, 2016, pp. 169–182. ISBN: 978-3-319-33514-8 978-3-319-33515-5. DOI: 10.1007/978-3-319-33515-5_14. URL: http://link.springer.com/10.1007/978-3-319-33515-5_14 (visited on 03/14/2022).

[41] Chauncey Wilson. *Interview techniques for UX practitioners: a user-centered design method*. OCLC: ocn828670764. Amsterdam ; Boston: Morgan Kaufmann, 2014. ISBN: 978-0-12-410393-1.

[42] Winfred B. Hirschmann. "Profit from the Learning Curve". In: *The Magazine* (Jan. 1964). DOI: https://hbr.org/1964/01/profit-from-the-learning-curve.

Appendix A

Survey

1. What is the name of your start-up if you have one?
2. In what country the main activities of your start-up are?
3. What sector(s) the start-up is in?
4. What is your business model?
5. May I contact you if any additional questions arise?

5.1 Name and Last name 5.2 E-mail address

8. How many people working on the start-up?
10. How is the start-up financed?
11. How well is the idea defined? Please choose the most applicable.

- There is only idea
- Initially validated idea and value proposition
- First prototype, not yet a minimal viable product
- Minimal viable product
- Product/ service that is used by some people
- Product/ service that is on the market

12. Do you have customers?

- No market acquired yet
- Found first customer/ early adopters
- Have acquired a market segment

13. How old is the start-up?

- 0-1 years
- 1-2,5 years
- 2,5-4 years
- 4-5 years
- 5-10 years

15. Information security policies are defined and aligned with business strategy, regulations and the information security environment.

16. Each policy has an owner and is reviewed at planned intervals

17. The information security responsibilities are defined and allocated. (who is responsible for what, authorization levels and coordination are the examples)

18. No single person can access, modify and use assets without detection.

19. There is a list of authorities and their contacts in case information security incident takes place (CERT)

20. The start-up is a part of some interest groups (incubation, StartupEstonia and etc.)

21. Any type of activity in the start-up is integrated with information security goals.

22. Information security risk assessment is conducted at an early stage of the project (project for a core business process, IT, facility and etc.)

23. There is a mobile device policy (risks of working with mobile devices in unprotected environments are taken into account, for example, no one except for you can access your work email on the phone)

24. There is a teleworking policy that protects information accesses, processed or stored at teleworking sites. Teleworking refers to all forms of working outside of the office.

25. Background verification checks are performed on all candidates (verification of CV, independent identity verification and so on)

26. In the employment contract there is a section stating employees and organization's responsibilities for information security.

27. Everyone is aware about the information security policies in the start-up. (policies can be written informally)

28. There is an anonymous reporting channel to report violations of information security policies or procedures.

29. Everyone is familiar with and comply with applicable information security rules and obligations (rules and obligations can be written in informal way)

30. There is a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

31. The communication of termination responsibilities is clear (for instance, NDA agreement is signed and thus after leaving the company person cannot give out some information about the start-up)

33.There is a list of all assets (laptops, phones, usb-sticks and etc.) that are associated with information processing.

34. All the assets have dedicated owners who are responsible for their information security.

35. There are certain rules for the use of information and of assets associated with information and information processing facilities (authorization, organization of information, coordination and etc.)

36. There are procedures for handling the assets. For instance, maintenance of a formal records of authorized recipients of assets.

37. There is a formally written access policy (covers both physical and logical). For instance, security requirements for applications, management of access rights should be a part of such policy.

38. Access is only granted to the information when one needs to perform their tasks.

39. Access is grated to the information processing facilities (apps, rooms and so on) only if one needs to perform their tasks.

40. There is a formal user registration procedure (using unique IDs to enable users to be linked and held responsible).

41. There is a formal procedure to review the user access rights. (one knows to what apps, Sharepoints and so on they have access to)

42. Some people in the start-up have privileged access rights.

43. Personal authentication information is secret? (for instance, does anyone knows your password to the work laptop?)

44. There is a secure log-on procedure? (methods alternative to password, such as cryptographic means, smart card and etc)

45. There is a password management system (Bitwarden, LastPass, 1Passwordand etc.).

46. The access to the program source code is restricted.

47. Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure and modification.

48. Procedures for information labelling are identified (for instance, physical labels and metadata are common forms).

49. The start-ups uses some cryptographical means to protect the confidentiality, authenticity and/or integrity of information

51. Please choose the most relevant items for your cryptography policy:

- General principles towards the use of cryptography controls
- Level of protection is identified taking into account the type, strength and quality of the encryption algorithm required
- The approach to key management is identified
- Roles and responsibilities, e.g who is responsible for implementation of the policy, for key management
- The impact of using encrypted information

52. A formal policy on the use, protection and lifetime of cryptographic keys is developed

53. Please choose what best describes the key management policy if one exists:

- Such policy does not exist
- Secure process for generating cryptographic keys
- Secure process for storing cryptographic keys
- Secure process for archiving cryptographic keys
- Secure process for retrieving cryptographic keys
- Secure process for distributing cryptographic keys
- Secure process for retiring cryptographic keys
- Secure process for destroying cryptographic keys

55. Please choose the most applicable to your start-up. • The physical perimeter around the start-up is secure • There are physical entry controls e.g the date and time of entry and departure of visitors is recorded • Key facilities do not have access by the public • There is a physical protection against natural disasters, malicious attacks or accidents • There are procedures for working in secure areas

e.g. the personnel is only aware of the existence of secure areas on a need-to-know basis • The loading and delivery areas are isolated from information processing facilities • None are applicable

56. Equipment is protected from power failures and other disruptions caused by failures in supporting utilities (e.g. electricity, telecommunication, water supply)

57. Power and telecommunication cabling carrying data or supporting information services are protected from interception, interference or damage

58. Equipment, information or software is not taken off-site without prior authorization

59. Unattended equipment has appropriate protection (e.g. active sessions are terminated, log-off from apps)

60. Choose the activities that have a formally documented procedures how they should be done.

- Installation and configuration of systems
- Backup
- Instructions for handling errors or other exceptional conditions
- System restart and recovery procedures
- Monitoring procedures
- None of these

61. Changes to the ways of work are controlled and explicitly depicted.

62. Development, testing and operational environments are separated.

63. Backup copies of information, software and system images do exist.

64. Event logs that record user activities, exceptions, faults and information security events are produced (e.g. you know how to access GitHub logs for bug fixing)

65. Please select the most applicable to your start-up.

- Unauthorized software is not used
- Malware detection and repair software are installed and regularly updated
- There is a person who deals with malware protection on systems

66. Software is acquired only through known and reputable sources, there is no violations of copyrights

67. Personal identifiable information is private and protected as required by local legislation (GDPR)

68. Select the most applicable to your start-up.

- The start-ups approach to managing information security is reviewed by other independent organizations
- Managers review the compliance within their area of responsibility regularly
- Information systems are regularly reviewed for compliance with technical standards

69. Information transfer is secure. (FTP, SSL, VPN)

70. Networks are managed and controlled to protect information in systems and applications.

71. The Wi-Fi router you use has strong authentication setup (for instance, passphrase that is stored in a password manager).

72. There are formally documented information transfer policies and procedures (for instance, guidelines outlining acceptable use of communication facilities)

73. Only end-to-end encryption messengers are used for communications (Telegram, Signal and etc.)

Appendix B

[H] ISO security control clause	Security category	Control	Level 0	Level 1	Level 2	Level 3	Level 4
5 Information security policies	5.1 Management direction for information security	5.1.1 Policies for information security	Creation	Creation	Development	Growth	Market exit
		5.1.2 Review of the policies for information security	Growth	Growth	Growth	Market exit	Market exit
6 Organization of information security	6.1 Internal organization	6.1.1 Information security roles and responsibilities	Ideation	Creation	Development	Development	Growth
		6.1.2 Segregation of duties	Development	Growth	Growth	Growth	Market exit
		6.1.3 Contact with authorities	Creation	Development	Development	Growth	Growth
		6.1.4 Contact with special interest groups	Creation	Creation	Development	Growth	Growth
		6.1.5 Information security in project management	Creation	Development	Development	Growth	Growth

	6.2 Mobile devices and teleworking	6.2.1 Mobile device policy	Creation	Development	Growth	Growth	Market exit
		6.2.2 Teleworking	Creation	Development	Growth	Growth	Market exit
7 Human resource security	7.1 Prior to employment	7.1.1 Screening	Ideation	Creation	Creation	Development	Growth
		7.1.2 Terms and conditions of employment	Growth	Growth	Growth	Market exit	Market exit
	7.2 During employment	7.2.1 Management responsibilities	Ideation	Creation	Development	Growth	Growth
		7.2.2 Information security awareness, education and training	Growth	Growth	Growth	Market exit	Market exit
		7.2.3 Disciplinary process	Growth	Growth	Growth	Market exit	Market exit
	7.3 Termination and change of employment	7.3.1 Termination or change of employment responsibilities	Growth	Growth	Growth	Market exit	Market exit

8 Asset management	8.1 Responsibility for assets	8.1.1 Inventory of assets	Ideation	Creation	Development	Development	Growth
		8.1.2 Ownership of assets	Creation	Development	Development	Growth	Market exit
		8.1.3 Acceptable use of assets	Creation	Development	Development	Growth	Market exit
		8.1.4 Return of assets	Creation	Development	Development	Growth	Market exit
	8.2 Information classification	8.2.1 Classification of information	Ideation	Creation	Development	Growth	Market exit
		8.2.2 Labelling of information	Creation	Development	Development	Growth	Market exit
		8.2.3 Handling of assets	Creation	Development	Development	Growth	Market exit
	8.3 Media handling	8.3.1 Management of removable media	Development	Growth	Market exit	Market exit	Market exit
		8.3.2 Disposal media	Development	Growth	Market exit	Market exit	Market exit

		8.3.3 Physical media transfer	Development	Growth	Market exit	Market exit	Market exit
9 Access management	9.1 Business requirments of access control	9.1.1 Access control policy	Creation	Development	Development	Growth	Growth
		9.1.2 Access to networks and network services	Creation	Development	Development	Growth	Growth
	9.2 User access management	9.2.1 User registration an deregistration	Ideation	Creation	Development	Development	Growth
		9.2.2 User access provisioning	Development	Growth	Growth	Market exit	Market exit
		9.2.3 Management of privileged access rights	Development	Growth	Growth	Market exit	Market exit
		9.2.4 Management of secret authentication information of users	Creation	Development	Development	Growth	Growth
		9.2.5 Review of user access rights	Growth	Growth	Growth	Market exit	Market exit

		9.2.6 Removal or adjustments of access rights	Growth	Growth	Growth	Market exit	Market exit
	9.3 User responsibilities	9.3.1 Use of secret authentication information	Creation	Development	Development	Growth	Growth
	9.4 System and application access control	9.4.1 Information access restriction	Ideation	Creation	Development	Growth	Market exit
		9.4.2 Secure log-on procedures	Creation	Development	Development	Growth	Market exit
		9.4.3 Password management systems	Creation	Development	Development	Growth	Market exit
		9.4.4 Use of privileged utility programs	Growth	Growth	Growth	Market exit	Market exit
		9.4.5 Access control to program source code	Creation	Development	Development	Growth	Market exit
10 Cryptography	10.1 Cryptography	10.1.1 Policy on the use of cryptographic controls	Development	Development	Growth	Growth	Market exit

		10.1.2 Key management	Development	Development	Growth	Growth	Market exit
11 Physical an environmental security	11.1 Secure areas	11.1.1 Physical security perimeter	Growth	Growth	Growth	Market exit	Market exit
		11.1.2 Physical entry controls	Growth	Growth	Growth	Market exit	Market exit
		11.1.3 Securing offices, rooms and facilities	Creation	Development	Development	Growth	Market exit
		11.1.4 Protecting against external and environmental threats	Growth	Market exit	Market exit	Market exit	Market exit
		11.1.5 Working in secure areas	Growth	Market exit	Market exit	Market exit	Market exit
		11.1.6 Delivery and loading areas	Growth	Market exit	Market exit	Market exit	Market exit
	11.2 Equipment	11.2.1 Equipment and sitting protection	Growth	Market exit	Market exit	Market exit	Market exit

11.2.2 Supporting utilities	Growth	Market exit	Market exit	Market exit	Market exit
11.2.3 Cabling security	Growth	Market exit	Market exit	Market exit	Market exit
11.2.4 Equipment maintenance	Growth	Market exit	Market exit	Market exit	Market exit
11.2.5 Removal of assets	Growth	Market exit	Market exit	Market exit	Market exit
11.2.6 Security of equipment's and assets off-premises	Growth	Market exit	Market exit	Market exit	Market exit
11.2.7 Secure disposal or re-use of equipment	Growth	Market exit	Market exit	Market exit	Market exit
11.2.8 Unattended user equipment	Creation	Development	Growth	Market exit	Market exit
11.2.9 Clear desk and clear screen policy	Creation	Development	Growth	Market exit	Market exit

12 Operations security	12.1 Operational procedures an responsibilities	12.1.1 Documented operation procedures	Development	Growth	Growth	Market exit	Market exit
		12.1.2 Change management	Growth	Growth	Market exit	Market exit	Market exit
		12.1.3 Capacity management	Ideation	Creation	Development	Growth	Growth
		12.1.4 Separation of development, testing, and operational environments	Ideation	Creation	Development	Growth	Growth
	12.2 Protection from malware	12.2.1 Controls against malware	Creation	Development	Growth	Growth	Market exit
	12.3 Backup	12.3.1 Information backup	Creation	Development	Growth	Growth	Market exit
	12.4 Logging an monitoring	12.4.1 Event logging	Creation	Development	Growth	Growth	Market exit
		12.4.2 Protection of log information	Creation	Development	Growth	Growth	Market exit

		12.4.3 Administrator an operator logs	Creation	Development	Growth	Growth	Market exit
		12.4.4 Clock synchronization	Creation	Development	Growth	Growth	Market exit
	12.5 Control of operational software	12.5.1 Installation of software on operational systems	Creation	Development	Growth	Growth	Market exit
	12.6 Technical vulnerability management	12.6.1 Management of technical vulnerabilities	Creation	Development	Growth	Growth	Market exit
		12.6.2 Restrictions on software installation	Creation	Development	Growth	Growth	Market exit
	12.7 Information systems audit considerations	12.7.1 Information systems audit controls	Development	Growth	Growth	Market exit	Market exit
13 Communications	13.1 Network security management	13.1.1 Network controls	Ideation	Creation	Development	Development	Growth
		13.1.2 Security of network services	Development	Growth	Growth	Market exit	Market exit

		13.1.3 Segregation in networks	Development	Growth	Growth	Market exit	Market exit
	13.2 Information transfer	13.2.1 Information transfer policies and procedures	Development	Growth	Growth	Market exit	Market exit
		13.2.2. Agreements on information transfer	Development	Growth	Growth	Market exit	Market exit
		13.2.3 Electronic messaging	Development	Growth	Growth	Market exit	Market exit
		13.2.4 Confidentiality or non-disclosure agreements	Growth	Growth	Market exit	Market exit	Market exit
14 System acquisition. Development and maintenance	14.1 Security of information systems	14.1.1 Information security requirements analysis and specification	Growth	Growth	Market exit	Market exit	Market exit
		14.1.2 Securing application services on public networks	Development	Growth	Market exit	Market exit	Market exit

	14.1.3 Protecting application services transactions	Growth	Market exit	Market exit	Market exit	Market exit
14.2 Security in development an support processes	14.2.1 Secure development policy	Development	Growth	Market exit	Market exit	Market exit
	14.2.2 System change control procedures	Growth	Market exit	Market exit	Market exit	Market exit
	14.2.3 Technical review of applications after operating platform changes	Growth	Market exit	Market exit	Market exit	Market exit
	14.2.4 Restrictions on changes to software packages	Growth	Growth	Market exit	Market exit	Market exit
	14.2.5 Secure system engineering principles	Development	Growth	Growth	Market exit	Market exit
	14.2.6 Secure development environment	Development	Growth	Growth	Market exit	Market exit

		14.2.7 Outsourced development	Growth	Growth	Market exit	Market exit	Market exit
		14.2.8 System security testing	Development	Growth	Growth	Market exit	Market exit
		14.2.9 System acceptance testing	Development	Growth	Growth	Market exit	Market exit
	14.3 Test data	14.3.1 Protection of test data	Creation	Development	Development	Growth	Market exit
15 Supplier relationships	15.1 Information security in supplier relationship	15.1.1 Information security policy for supplier relationship	Growth	Market exit	Market exit	Market exit	Market exit
		15.1.2 Addressing security within supplier agreements	Growth	Market exit	Market exit	Market exit	Market exit
		15.1.3 Information and communication technology supply chain	Market exit	Market exit	Market exit	Market exit	Market exit

	15.2 Supplier service delivery management	15.2.1 Monitoring and review of supplier service	Market exit	Market exit	Market exit	Market exit	Market exit
		15.2.2 Managing changes to supplier services	Market exit	Market exit	Market exit	Market exit	Market exit
16 Information security incident management	16.1 Management of information security incidents and improvements	16.1.1 Responsibilities and procedures	Creation	Development	Development	Growth	Growth
		16.1.2 Reporting information security events	Development	Growth	Growth	Growth	Market exit
		16.1.3 Reporting information security weaknesses	Development	Growth	Growth	Growth	Market exit
		16.1.4 Assessment of and decision on information security events	Growth	Growth	Market exit	Market exit	Market exit

		16.1.5 Response to information security incidents	Growth	Growth	Market exit	Market exit	Market exit
		16.1.6 Learning from information security incidents	Growth	Growth	Market exit	Market exit	Market exit
		16.1.7 Collection of evidence	Creation	Development	Growth	Growth	Market exit
17 Information security aspects of business continuity management	17.1 Information security continuity	17.1.1 Planning information security continuity	Development	Growth	Growth	Market exit	Market exit
		17.1.2 Implementing information security continuity	Development	Growth	Growth	Market exit	Market exit
		17.1.3 Verify, review and evaluate information security continuity	Development	Growth	Growth	Market exit	Market exit
	17.2 Redundancies	17.2.1 Availability of information processing facilities	Development	Growth	Growth	Market exit	Market exit

18 Compliance	18.1 Compliance with legal and contractual requirements	18.1.1 Identification of applicable legislation and contractual requirements	Development	Growth	Growth	Market exit	Market exit
		18.1.2 Intellectual property rights	Creation	Development	Growth	Market exit	Market exit
		18.1.3 Protection of records	Creation	Development	Growth	Market exit	Market exit
		18.1.4 Privacy and protection of personally identifiable information	Ideation	Development	Growth	Market exit	Market exit
		18.1.5 Regulation of cryptographic controls	Growth	Growth	Market exit	Market exit	Market exit
	18.2 Information security reviews	18.2.1 Independent review of information security	Growth	Growth	Growth	Market exit	Market exit

18.2.2 Compliance with security policies and standards	Development	Growth	Growth	Market exit	Market exit
18.2.3 Technical compliance review	Development	Growth	Growth	Market exit	Market exit

II. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Anna Shamritskaya**,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Type Inference for Fourth Order Logic Formulae,
   *(*title of thesis)

   supervised by Raimundas Matulevičius and Mari Seeba
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Anna Shamritskaya
dd/mm/yyyy