jamk.fi

Risk management strategy formation for an ICT startup entering the Russian Market

Mark Mattayev

Bachelor's thesis
May 2017
Business Administration
International Business Programme

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Mattayev, Mark	Bachelor's thesis	May 2017
	Number of pages 62	Language of publication: English
		Permission for web publication: x

Title of publication Risk management strategy formation for an ICT startup entering the Russian Market
Degree programme – International Business
Supervisor(s) Saukkonen, Juha
Assigned by Trulyprotect Oy

Startup companies in the field of ICT can easily scale their services internationally with an intangible service or product. Nonetheless, the exposure to risk and uncertainty become an ever growing concern that must be managed in order to operate successfully in a target market. In this study, the author who is the General Manager of a cyber security company called Trulyprotect in Finland, focused on identifying, categorizing and rating various risk factors while entering the Russian market in order to form a proper risk management strategy. The Russian market was chosen due to its market size, favorable change in cyber security legislation and increased awareness of the corporate sector for the need of simiral offered solutions.

In the literature review section the author defined the main key terms in the research, followed by a theoretical background of enterprise risk management, market entry mode, PESTLE and SWOT analysis, risk evaluation and strategic risk management.

The research method applied in the study was qualitative with an exploratory approach. Through surveys, semi-structured interviews of twenty participants and observations the author collected primary data that aimed at forming a risk management strategy based on the predetermined objectives of the company in the Russian market and its context. The collected secondary data further assisted in identifying the most relevant risk factors and methods of risk treatment.

The findings of the research indicated specific risk types and elements based on primary and secondary data on the grounds of ISO 31000 framework for enterprise risk management. In the results and analysis section a risk management strategy was proposed that would assist the company in its endeavors to efficiently enter the Russian market.

Keywords (subjects) Enterprise Risk Management, ICT startups, Internationalization Risk, Russian Market
Miscellanous

Table of contents

1 Abstract....3

2 Background and motivations....4

3 Literature review – Theoretical background....6

3.1 Definition of Risk....6

3.2 The Risk Management Process....7

3.3 Risk Types....13

4 Research Methods and Implementation....22

4.1 Research Method....22

4.2 Research implementation....23

5 Results and Analysis....27

5.1 Establishing the Context....27

5.2 Identified Risk Types and Elements....38

5.3 Risk Analysis and Evaluation....44

5.4 Risk Treatment....45

5.5 Conclusion....49

5.6 Research Quality....50

5.7 Further research recommendation....52

6 Discussion....53

7 References....55

8 Appendicies....59

Figures

Figure 1 Ernst & Young (2010) “Risk appetite. The strategic balancing act”....7

Figure 2 ISO 31000 Risk Management Principles....9

Figure 3 Russian Market competitiveness, World Economic Forum 2016....29

Figure 4 SWOT analysis for the Russian Market....32

Figure 5 Market Elements Risks Map Summary....43

Figure 6 Trulyprotect's objectives for the Russian Market....45

Tables

Table 1 Risk Evaluation Table (Global CCS Institute, 2017) 11
Table 2 Barriers ranked by SMEs using the top ten ranking method (OECD, 2009) 14
Table 3 Finance Risk in the Russian Market - Part 1 17
Table 4 Finance Risk in the Russian Market - Part 2 18
Table 5 Operations Risk in the Russian Market 19
Table 6 Strategic Risk in the Russian Market 20
Table 7 Information and Technology Risk in the Russian Market 21
Table 8 Finance Risk type and Elements, Respondents 39
Table 9 Information and Technology type and Elements, Respondents 40
Table 10 Operations Risk type and Elements, Respondents 41
Table 11 Strategic Risk type and Elements, Respondents part 1 42
Table 12 Strategic Risk type and Elements, Respondents Part 2 43
Table 13 Risk Evaluation Table (Global CCS Institute, 2017) 44
Table 14 Stage 1 Objectives, Risks and Treatment Strategy 46
Table 15 Stage 2 Objectives, Risks and Treatment Strategy 47
Table 16 Stage 3 Objectives, Risks and Treatment Strategy 48
Table 17 Stage 4 Objectives, Risks and Treatment Strategy 49

1 Abstract

Startup companies in the field of ICT can easily scale their services internationally with an intangible service or product. Nonetheless, the exposure to risk and uncertainty become an ever growing concern that must be managed in order to operate successfully in a target market. In this study, the author who is the General Manager of a cyber security company called Trulyprotect in Finland, focused on identifying, categorizing and rating various risk factors while entering the Russian market in order to form a proper risk management strategy. The Russian market was chosen due to its market size, favorable change in cyber security legislation and increased awareness of the corporate sector for the need of similar offered solutions.

In the literature review section the author defined the main key terms in the research, followed by a theoretical background of enterprise risk management, market entry mode, PESTLE and SWOT analysis, risk evaluation and strategic risk management.

The research method applied in the study was qualitative with an exploratory approach. Through surveys, semi-structured interviews of twenty participants and observations the author collected primary data that aimed at forming a risk management strategy based on the predetermined objectives of the company in the Russian market and its context. The collected secondary data further assisted in identifying the most relevant risk factors and methods of risk treatment.

The findings of the research indicated specific risk types and elements based on primary and secondary data on the grounds of ISO 31000 framework for enterprise risk management. In the results and analysis section a risk management strategy was proposed that would assist the company in its endeavors to efficiently enter the Russian market.

Topic

Risk management strategy formation for an ICT startup entering the Russian market

Key words

Enterprise Risk Management, ICT startups, Internationalization Risk, Russian Market

2 Background and motivations

The exploration of Russia as a potential market for expansion followed after the Russian and Finnish Chamber of commerce published an article that was called ”Information security booming in Russia” (FRCC 2016) which invited Finnish companies to offer Cyber security solutions in Russia due to new changes in legislation. The positive approach in the article did not mention, however, the various hazards and downfalls of entering such a market. Moreover, there were not many ICT companies from Finland entering the Russian Market.

There was one instance of a Finnish cyber security company named Blancco that entered the Russian market put pulled out due to various reasons (Infosecurity Russia, 2012). These all made the Russian market interesting enough to research and promote. However, the recognition that it is fairly risky had always been a topic of discussion of experts in the field. As a result, I was motivated to study and research the risk management strategy that can be implemented to manage the potential losses and gains as we enter the market.

While there is a wealth or research and information regarding general risks of doing business in Russia it was important to narrow down and identify the unique problems that a Finnish ICT startup that sells to Medium to Large size organizations might face while entering the Russian market. This type of information was not readily available as there have not been traceable cases of Finnish cyber security startups entering the Russian market in the past decade.

The Russian market is the biggest trade export for Finland and, therefore, it was an attractive market to explore, despite the multitude of hazards entailed in operating in such a volatile environment. After my first visit to Russia in January 2017, I compiled a comprehensive company report titled *”Entering the Russian Market”* that was 32 pages long. There I recommended that the

next step should be a study of the risks involved in the Russian market which is the purpose of this research paper.

Research Questions

The main three research questions that function as the backbone of the entire research paper are as follows:

1. What are the risk types that are the most relevant for Trulyprotect entering the Russian market?

2. What practical elements need to be considered most within these risk types?

3. What is the most viable risk management strategy for Trulyprotect entering the Russian market?

Based on these guiding questions the interview and survey questions were formulated.

3 Literature review – Theoretical background

In this chapter I will examine the theoretical background of the main key terms of this research paper. First, I will define the concept of risk from a multidisciplinary perspective. Then I will describe in detail the process of Enterprise Risk Management and its significance to an organization for strategy formation. Afterwards I will present company specific risks for Trulyprotect alongside with special risks in the Russian market from the literature and internationalization risks. Finally, I will present the choice of Market entry mode model which is an inseparable part of the study which defines the scope of our intended business activity.

3.1 Definition of Risk

Numerous are the definitions of risks within various fields, yet among other definitions the ISO 31000 for Enterprise Risk Management definition was selected for the purposes of this research paper. Based on the ISO website the International Standards Organization creates documents that provide requirements, guidelines, specifications or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. (ISO 2017.) According to the standard, risk is the ”Effect of uncertainty on objectives, whether positive, negative or any deviation from the expected. The impact can be short, medium and long term” (AIRMIC 2010, 4).

In other fields, such as Insurance and Event Management *risk* is defined as ”the uncertainty concerning the occurrence of a loss and variability of future outcomes” (Rejda 2008, 3-17). Furthermore, two main generic risk types are presented in the literature to explain the source of risk: Absolute and Speculative risks. Absolute risk is defined as *”the possibility of loss and no possibility of gain”* while Speculative risk is defined as *”the possibility of loss and the possibility of gain”* (Silvers 2008, 4). The latter is associated with the desire of the risk taker to engage in a business conduct that entails a possibility

to generate a positive cash flow while the other has merely negative consequences such as the burn down of a manufacturing facility.

Within the context of investments and portfolio management, risk ”is recognized as to convey the possibility of losses and gains” (Walker 2013, 2). This generic definition does not include the elements of variance of returns and volatility as portfolio beta, yet ”the investor does consider expected return a desirable thing and variance of return an undesirable thing” (Markowitz 1952, 77-91). Consequently, an investor must utilize risk management strategies to remain within the risk target range (Figure 1) to keep desirable rates of returns while not exceeding his own predetermined risk tolerance and risk capacity levels (Ernst & Young 2010). For instance, diversification, which is the mixture of a wide variety of investments within the same industry to balance losses and gains from poorly and well performing companies, is often used to reduce unsystematic risk (Investopedia 2017b).

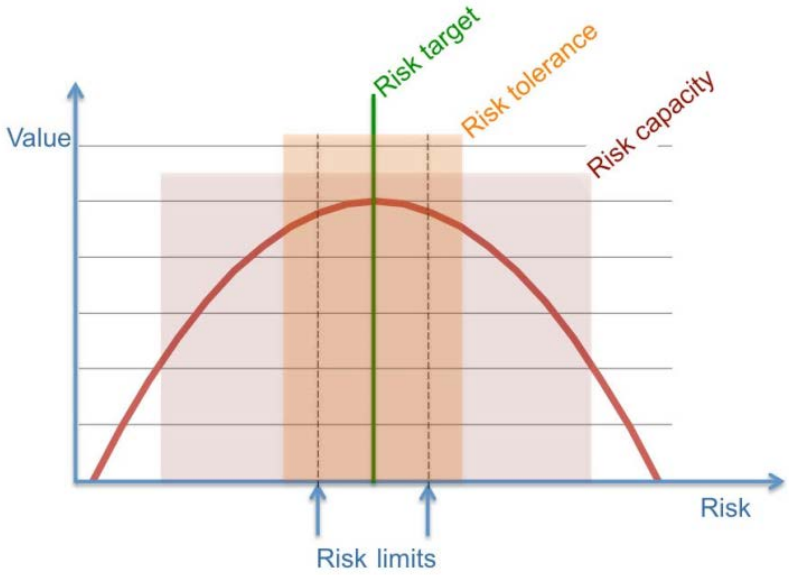


Figure 1 Ernst & Young (2010) “Risk appetite. The strategic balancing act”

3.2 The Risk Management Process

A risk management process is not merely a list of steps an enterprise must take in order to safeguard themselves from potential losses but, moreover, it is

a fundamental procedure by which a strategic management can be applied based on the risk capacity, business context and objectives. For such a process to be useful, an organization must apply it systematically with a dynamic feedback process that would correspond to the changing nature of the business environment. For instance, the sanctions that were imposed on Russia in 2014 by the EU constitutes a radical shift in the risk limits a company can handle, thus the risk management strategy must be reconstructed. (AIRMIC 2010, 6)

Based on the designated framework for risk management process laid by ISO 31000 (Figure 2) a detailed description will be presented in the subchapters for each one of the steps in the progression. Within the framework several critical steps were diagnosed to handle risk effectively step by step (AIRMIC 2010, 4-14). These are:

Establishment of context in which both internal and external factors that affect the company are considered.

Risk Identification establishes the type of exposure category of the organization to different risks and uncertainties. In this step an answer to the question "*What may happen and why?*" should be found. The types of risks used within this study are: Finance, Operations, Information Technology and Strategic risk (Moller 2011, 35)

Risk Analysis refers to the procedure that results in forming a risk profile that attaches a significance to each risk. This step should answer the question "*What are the consequences of the risk?*" in order that the PESTLE and SWOT analysis tools can be used (AIRMIC 2010, 8)

Risk Evaluation determines the probability and severity of the risk that may occur within the context and objectives the company operates in. A risk rating matrix is applied to make a prioritization of risks. In addition, these risks can also be quantified to the level of loss exposure for every risk element. (AIRMIC 2010, 8-10)

Risk Treatment is the stage in which a choice of action is selected to handle a certain risk element. There are primarily four risk management strategies: Avoidance, Acceptance, Mitigation/Reduction and Transfer (Walker 2013, 35).

Risk Monitoring and Review is the last stage in the framework in which the efficiency of the chosen strategy is estimated and reviewed. In case there is poor performance the definition of context, risk identification and risk ranking and treatment can be modified.

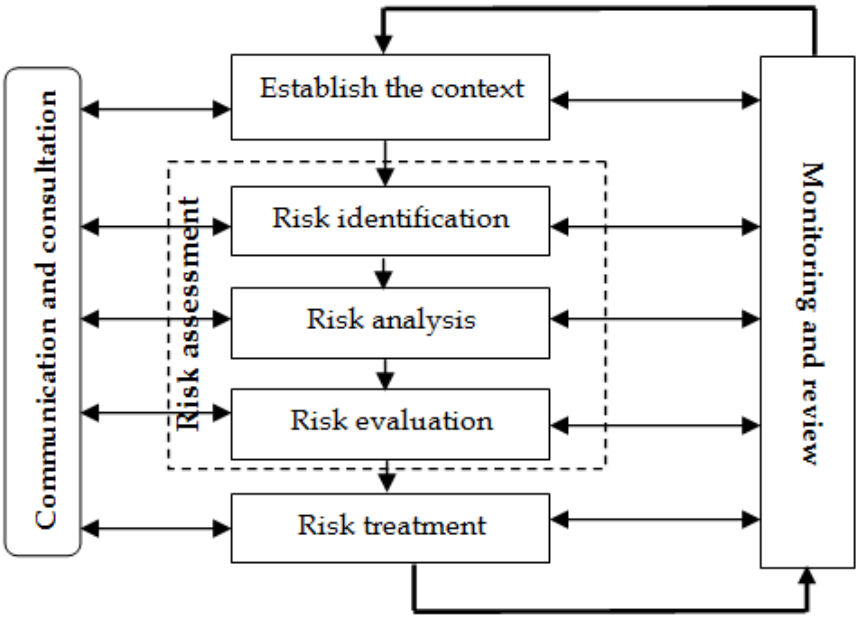


Figure 2 ISO 31000 Risk Management Principles

Forming a Risk Management Strategy

Based on the principles and framework of Enterprise Risk Management the formation of the risk management strategy is mainly dependent on the context in which the company operates, the objectives it sets, the main identified risks it might face, quantifying and assessing the risks' probability and severity and then choosing the proper strategic tools to treat the various risks.

Establishing the context

The first step in forming a risk management strategy is to define the context in which the company operates (Dorfman & David 2013, 10-14). Such tools can include PESTLE and SWOT analysis which will be used in the results chapter to define the context in which Trulyprotect operates. PESTLE analysis ”is a concept in marketing principles which is used as a tool by companies to track the environment they’re operating in or are planning to launch a new project/product/service” (Pestelanalysis 2017). It is a mnemonic which in its expanded form refers to as P for Political, E for Economic, S for Social, T for Technological, L for Legal and E for Environmental.

SWOT analysis is a framework tool that stands for strengths, weaknensses, opportunities and threats that a company faces while making a critical business decision. (Irwin 1969.)

Risk Identification

The growing popularity of enterprise risk management frameworks contributed to the wider variety of risks’ identification and categorization. It can be argued that the most important step in the formation of a risk management strategy is the accuracy of the identified risk elements. Therefore, it is pivotal to pinpoint which risks may have a stifling and how it can be treated. The means of obtaining an accurate map of risks can be achieved through a combination of secondary and primary data from within the organization and outside the organization to increase the validity and reliability of the risk elements. (Dorfman & David 2013, 16-17.)

Risk Evaluation and Analysis

In other chapters the context in which the company operates will be laid down in the form of PESTLE and SWOT analysis, while the risk types and elements identification will stem from the primary and secondary data collected and

categorized. In this subchapter I will introduce the tool that would assist in ”risk evaluation” and ”risk treatment”.

Risk evaluation is critical to the proper understanding of how the probability of occurrence of a certain risk element would correlate with the severity of an impact over the company as illustrated in Table 6 (Global CCS Institute 2017).

		Consequences				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood						
5	Almost certain	High	High	Extreme	Extreme	Extreme
4	Likely	Moderate	High	High	Extreme	Extreme
3	Moderate	Low	Moderate	High	Extreme	Extreme
2	Unlikely	Low	Low	Moderate	High	Extreme
1	Rare	Low	Low	Moderate	High	High

Table 1 Risk Evaluation Table (Global CCS Institute, 2017)

Based on this table the risk elements are inserted according to the estimation of their potential consequences from a scale of 1 to 5 and the likelihood of occurrence from 1 to 5. Risk elements have four levels of risk rating; low, moderate, high and extreme. These ratings are then calling upon a specific strategic approach.

According to the Global CCS institute, the meaning of the terminology of likelihood can be defined in numeric terms as follows; Rare – 5% chance of occuring, Unlikely – 20%, Moderate – 50%, Likely- 80% and Almost certain with 95% chance of occuring. Likewise, the definition of “Insignificant” consequences mean that it can be absorbed through normal activity, while “Minor” means it is an adverse event which can be absorbed with some management effort. Then “Moderate” risk means that it is a serious event which requires additional management effort. A “Major” risk refers to a critical occurance that requires extraordinary management effort. The most

hazardous consequence is “Catastrophic” which means that it is a disaster with a potential to lead to collapse.

Risk Treatment

Treating loss exposure in a knowledgeable and informed manner is critical for the success of the risk management process. The following are possible strategies that appear in the framework of ISO 31000 and ERM:

Risk avoidance is one of the strategies to control risk. The direct definition of risk avoidance includes a situation where ”a certain loss exposure is never acquired for, or an existing loss exposure is abandoned”. For instance, flood losses can be avoided by not building a new plant of a floodplain. (Rejda 2008, 45.) In other words, if the perceived risk is greater than the perceived risk tolerance, then there is no reason whatsoever to include the risk as part of the plan. If avoidable, then it is preferable to choose a different solution, such as building a plant in a more expensive area but less prone to floods.

Despite the clear advantages of risk avoidance, there are a few disadvantages. It is not always possible to anticipate and control certain high severity risks. Such could be, for instance, the premature death of a high ranking company executive. Another disadvantage is the indirect nature of some risks that are part of a larger context and cannot be separated from other core operations. As an example, a paint factory can avoid losses from manufacturing paint, but once it does it there will be an immediate cease of the value production of the business and it will close down. (Rejda 2008, 45.)

Risk Transfer “refers to a wide range of techniques that the risk manager can apply to shift the financial responsibility of losses away from his or her organization and onto a third party” (Dorfman & David 2013, 51-52). There are three transfer risk categories; *Risk Bearing Financial Institutions*, such as insurance companies which cover certain risks for a predetermined fee. *Contractual Transfers*, which, simply transferring the underlying risk into a third party within a given contractual arrangement, for instance, once the

goods of a certain manufacturer have left the inventory, they are transferred to the carrier of the good. *Transfers involving limited liability*, which means that under the law of a limited liability company, an owner, unless explicitly agreed otherwise, does not guarantee or use his own assets to recover from bankruptcy. (Dorfman & David 2013, 51-53.)

Risk Reduction/ Mitigation "refers to the measures that reduce the severity of a loss after it occurs" (Rejda 2008, 46). Such a strategy can be used, for instance, when a credit card has been lost or stolen, by blocking the card user from executing any transactions until it is found. Moreover, even if some transactions had occurred, transfer risk may apply to credit card companies who use insurances to recover the stolen money. In this fashion the reliability of the credit card company is kept positive. Understanding the frequency of occurrence of a certain specific risk element may contribute to using risk reduction strategy.

Risk Accpetence is mainly utilized in small insignificant risks that occur rarely or moderately and have a low level of consequences. These could, for instance, be the sudden illness of a second IT support expert who cannot attend a sales meeting. The probability is rather low and the consequences are not significant, since there is already one available. Dedicating time and money resources to mitigate such risks once occurred does not justify the added value that would rise in case a third backup IT expert would attend the meeting since one would usually suffice. (DBP management 2014.)

3.3 Risk Types

In this chapter various types of risk with their special characteristics will be reviewed such as Internationalization risk, specific risk, born global risk and general Russian market risks that were split into four main risk types; operational, information and technology, finance and strategic risks.

Internationalization Risks

The process of internationalization entails an increase in the risk capacity a firm must be willing to undertake. Economic, political, environmental, legal, technological and cultural differences may have an adverse effect over the adaptation process into a new foreign market. Such possible adaptations are well narrated by a report published by the OECD (2009) called: "*Top Barriers and Drivers to SME Internationalization*". In the report ten main barriers were found and ranked particularly for small to medium size businesses as seen in Table 2.

Rank – Weighted factor	Description of barrier
1	Shortage of working capital to finance exports
2	Identifying foreign business opportunities
3	Limited information to locate/analyse markets
4	Inability to contact potential overseas customers
5	Obtaining reliable foreign representation
6	Lack of managerial time to deal with internationalisation
7	Inadequate quantity of and/or untrained personnel for internationalisation
8	Difficulty in matching competitors' prices
9	Lack of home government assistance/incentives
10	Excessive transportation costs

Table 2 Barriers ranked by SMEs using the top ten ranking method (OECD, 2009)

These elements will be served in the identification of risk types in the analysis and discussion chapters.

Market entry mode

In this study of the internationalization process defining the proper entry mode to the Russian market is critical for the realization of the risk scope Trulyprotect is exposed to while entering. Thus, an entry mode to an international market outside Finland requires an understanding of the possibilities that are available, for instance, based on Brassington & Pettit (2000) framework. Among many other options the entry can range between;

exporting, franchising, contracting, licensing, subsidiaries, joint venture, strategic alliances and direct investment. Each one of the options would depend on “contribution of know how” and “level of ownership” as illustrated in figure 3 “comparing different entry mode options”.

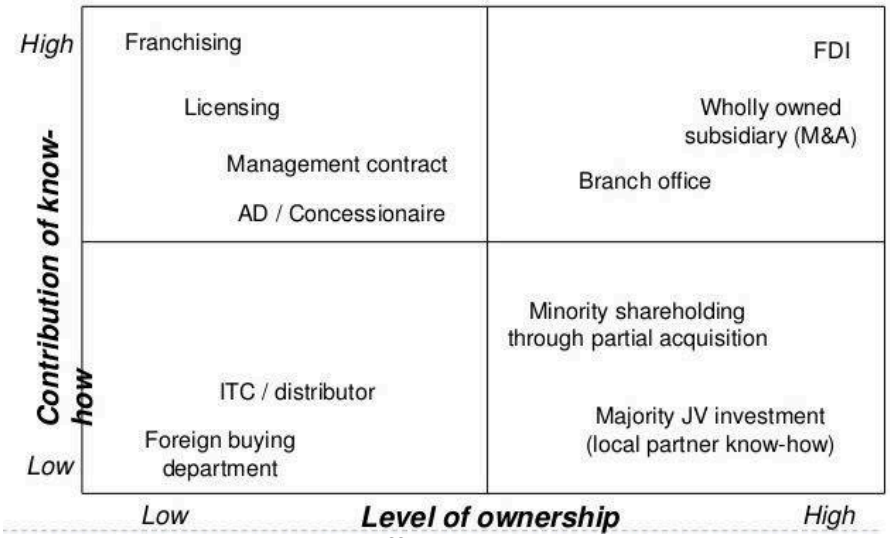


Figure 3 Comparing different entry modes. Charur, 2012

For the purposes of this research paper the scope of entry is only focused on two main possibilities for the short term of the next two years of operations which are: low “level of ownership” with either low/ high “contribution of know how”.

As a result, our most relevant options are narrowed down to the following business models:

Licensing: Granting legal permission to a second party to utilize the intellectual property owned by the licensor for a designated compensation without controlling power over second party. (Charur 2012.)

Distributor: a contract between channel partners that stipulates the responsibilities of both parties. The agreement is usually between a manufacturer or vendor and a distributor. The distributor is granted the right to sell the goods under certain specific conditions. (Rouse et al. 2017.)

Franchising: Granting legal permission to a second party to use the business model, brand, and operations process for a predetermined fee. The franchiser exercises control over the franchisee. (Diffen 2017.)

Specific risks

According to Investopedia (2017a), Specific Risk is one that "affects a very small number of assets. Specific risk, as its name would imply, relates to risks that are very specific to a company or small group of companies." This type of risk is the opposite of an overall market risk. (Investopedia 2017a.) These special risks to our company are described in the following passages.

Born Global Risk

Our company can be defined as "Born global" which means any company that starts their international activities immediately from their birth (Andersson 2004, 851-875). As such there are certain risk elements that we are exposed to versus companies that focus first on the local market and then incrementally expand to other markets overseas. One of the major risks a Born Global company faces is that they "tend to be relatively small and have far fewer financial, human, and tangible resources as compared to large multinational enterprises" (Stoyan 2012).

General Risks in the Russian Market

Unlike many Western countries, risks involving business operations in Russia have their own unique characteristics (Honkanen & Mikluha 1998). The book *"Successful management in Russia"*, authored by Matti Honkanen and Arja Mikluha (1998) dedicates an entire chapter to the risks of doing business in the Russian market. Since the authors are Finnish it is highly suitable for our context and despite the fact that it was written almost two decades ago the risks that are laid down in the book are highly valid for Trulyprotect's risk

management strategy formation. In the book I found a wide range of different risk elements that are suitable for an early stage market entry strategy either through licensing or distributors. These risks are summarized in Tables 2-7.

Finance Risk in the Russian Market

Finance Risk is a category of risks that include attributes in the fluctuation of value that is determined by the financial markets. In addition, the internal cost structure of the sold services or goods and obtained credit by the company are all related to finance risk exposure. (Dorfman & Cather 2013, 27.)

Risk Element	Details	Proposed Solution	Page
Regulatory Reporting Risk	There is no bank secrecy in Russia. All information in any back in Russia is possible to obtain. Authorities can demand access	Foundation documents, licenses and permissions are not trade secrets. Therefore this risk must be accepted as part of the financial risk	121
Foreign Exchange Risk	Some currencies may experience convertibility issues. There might be a requirement for an import or export passport on foreign currency payments	By using Roubles as payment currency in import operations to Russia Western companies may avoid the Russian currency regulation and charges connected with currency exchange	142
Currency Risk	Companies which are registered in Russia, including Western companies' subsidiaries, are required to convert 50% of their freely convertible currency earnings into Roubles through the domestic currency exchange market	An exemption from this rule is the provision concerning supplier credit in excess of 180 days.	142

Table 3 Finance Risk in the Russian Market - Part 1

Risk Element	Details	Proposed Solution	Page
Taxation Risk	Double tax treaties are signed between Russia and many Western countries yet there is a restriction on the amount of repatriation of profits, and possibility for additional paper work related to the travel of cash across borders to the tax authorities in each country	It is possible to pay dividends to nonresident shareholder abroad provided all taxes are duly paid. In addition, it is possible to use service or management agreements	146
Capital Avialiability Risk	A nonresident Western company that is not registered with the Russian tax authorities is not able to open a Rouble account in Russia	An investment account must be open. Moreover it is required to receive a license from the Central Bank allowing payments in foreign currency	143
Non Payment Risk	Almost 80% of transactions occur in as pre payment terms of yet in some in some case there are requirements to pay in installments	Western companies should insist on advance payment as means of compensation	148
Foreign Exchange Risk	All sales inside the Russian Federation by resident a legal entity must be made in Roubles	It is possible to acquire a special license that permits doing so yet it is time and resource consuming	143

Table 4 Finance Risk in the Russian Market - Part 2

Operations Risk in the Russian Market

Operations Risk is any risk that prevents a firm from conducting its normal scope of operations. Usually the risk elements within this category are attributed to inadequate internal processes, internal systems failure and human or management errors. (Dorfman & Cather 2013, 27.)

Risk Element	Details	Proposed Solution	Page
Regulatory and government complince	Licenses, permissions and certificate requirements. There are 35 different organization controlling companies activity	The lawyer of the company should provide an accurate estimate of future expenses, and operate according "to the book" in Russia	111-112
Litigation	Sanctions can be imposed on Western companies. Penalties for instance of up to 50% of the delivered good to the plaintiff	In consumer protection context, signing a contract as a non resident of Russia can assist as it is not probable a customer will sue in a western country	113

Risk Element	Details	Proposed Solution	Page
Crime	Organized crime. 6,000 criminal groups. Do money laundry, illegal protection of businesses and prostitution	As long as there is no permanent establishment the risk is low. Avoiding any solicitation of prostitution, drugs and alcohol.	117-118
Human Resource Risk	In the majority of cases, personal interests of Russian employees are more important than the company's interest. Thus an employee may move to another company in case offered merely a few hundred Euros higher salary	Understanding how to develop relations in Russia is critical since they play a major role in Russia is than in Western countries. Loyalty can be achievedthrough friendships.	149
Process Execution Risk	The Bureaucracy in Russia is much heavier than Western countries. Officails will charge higher fees from Westerners compared to locals	Sending a local lawyer to deal with paper work who knows the court room well.	124
Supply Chain Risk	Finding a reliable partner is a complex task. Many partners may seem right on the first meeting, yet may underperform significantly	Using the partners of one's friend in the West. The process of choosing a good partner should be thorough and well reasoned.	124
Supply Chain Risk	Limitation of agents and distributor's rights are more limited in Russia. Terminological differences also occur in law definitions	Russian distributors must be kept under control through supervision. No distributor exclusvie rights should be given.	126

Table 5 Operations Risk in the Russian Market

Strategic Risk in the Russian Market

Strategic Risk is related to the manner a firm is positioning itself in the market with respect to their competitors, thus obtaining a competitive advantage. Therefore, any activity that is a direct or indirect result of strategic rivalry in the marketplace is regarded as strategic risk. For instance, any risk that would harm the company from being competitive in the market is a strategic risk. (Dorfman & Cather 2013, 28.)

Risk Element	Details	Proposed Solution	Page
Legal and Regulatory Change	Unregulated or regulated inadequately. Often amended, poor publication. Interpretation may differ by governmental institutions.	Not compromising on the quality of legal advisors. Should be English speaking	110 -111
Patent/ Trademark	There is no stipulation that restricts the use of the name of a company. Sometimes there are 10 companies with the same name	A western company must register it's trademark and patent at patent authorities of the Russian Federation	115
Industry Risk	Most of Russian companies are not able to insure any risks and some of them are just collecting premiums	Despite the fact that Western insurance companies are not allowed it is advised to find a some subsidiary such as AIG and Allianz	121-122
Industry Risk	Russian banks may not be reliable as Western banks. At times may not work with SWIFT connections. Nonethless they are cheaper, faster and more flexible	A first bank account for a new company should be Russian since opening an account is one of the most time consuming processes. Later on a possibility to work with a Western bank is an option	126
Corruption	Bribing and "Speed money" which is bribing for speeding up processes within organizations, mostly governmental are widely used to gain competitive advantage in the marketplace	conformity to the local standards may help in the short term, yet it may hit back as a reputational loss on the long run	151

Table 6 Strategic Risk in the Russian Market

Information and Technology Risk in the Russian Market

Information and Technology Risk is defined as any threat that may rise a result of using information technology systems such as computers and networks and any information processing regarding the different company activities. (Business Queensland 2016.)

Risk Element	Details	Proposed Solution	Page
Employee Safety Risk	Valuable and costly staff members who are sent as expatriates may face sicknesses, accidents and even death	Western companies sending personnel on business trips to Russia should always do life, accident and sickness insurance	123
Performance Measurment	Contacts may not bare the same significance for Russian companies as Western. A Russian company punish over provisions for non performance, they may not comply to an agreement.	Drafting an agreement with an experienced lawyer. Moreover, it is not wise to conclude any contract, without the General Director signing it himself. Otherwise it may not be valid at all.	123
Taxation Risk	Extremely complex taxation system with often provisions that contradict each other. Drafting and budgeting is sometimes almost impossible	Choice of accounting firm with a Western parent company through a referral. Also validate they work within your field of business sector	139
Financial Reporting Risk	The tax office carries out various continuous inspections; regular, extraordinary and special. These may stifle normal flow of operations	If the company operates "by the book" and reports suspiciously huge amount of profits or other extraordinary activities these can be avoided	140-141

Table 7 Information and Technology Risk in the Russian Market

4 Research Methods and Implementation

This chapter will present the multiple data collection methods as well as the overall research structure and how it was implemented.

4.1 Research Method

The structure and methodology that was chosen to construct the research was determined after defining the research topic, exposure to preliminary secondary data and defining the business objectives of the company. Reviewing previous studies based on the keywords revealed that the more keywords are combined, the less relevant and scarce the results are (Table 7).

Term	Results
Risk	19,595
Risk management	13,752
Risk management strategy	8,283
Risk Management IT Russia	2,071
Risk management strategy Russia	1,794
Risk ICT Russia	316
Risk management strategy Russia ICT	296
Risk Russia cyber security	76
Risk management strategy Russia cyber security	70

Table 8 Results of main keywords in Thesus database, 2017

Since the topic of forming a risk management strategy for an ICT company in the Russian market was not well researched, the approach that was undertaken during this study was based on an Exploratory method. According to Saunders & Lewis (2012), “This type of research is not intended to provide conclusive evidence, but helps to have a better understanding of the problem. The researcher ought to be willing to change his/her direction as a result of revelation of new data and new insight” (ibid.). Following this method I was able to form a non biased opinion about the prospects of the company to

effectively form a strategy that would reduce the risk or choose not to enter the market.

Once concrete research questions were defined a Qualitative approach was chosen due to the rich nature of possible data collection. A qualitative approach as opposed to quantitative allows the collection of rich non numerical data (Saunders et al., 2009 p.151).

4.2 Research implementation

During the period of the research study I visited Russia three times in January, March and April 2017 to conduct interviews for a total of 21 days both in Saint Petersburg and Moscow. The main purpose of the visits was getting a comprehensive understanding of the Russian IT ecosystem and supply chain. In order to plan a long term market entry strategy meeting with as many relevant stakeholders was critical.

By the end of the business trips I met with two business incubators (Ingria and Skolkovo), two major IT universities in Saint Petersburg (GUAP and ITMO), three Finnish government export support organizations (Finpro, Jykes and Finnish Russian Chamber of Commerce), the Israeli Embassy in Moscow, three Russian system integrators, two marketing agencies, two Finnish – Russian consulting firms, four accounting and law firms out of which one was based in Finland, three IT business directors, two directors of an IT association, two non IT Finnish businesses that were operating in Russia and two representatives from JAMK that were involved with the Russian market and of course the President of Trulyprotect. In total, as many as 29 companies, organizations and businesses both in Finland, Russia and Israel.

Secondary data

The secondary data that was gathered functioned as the foundation for the research questions and literature review. For the theoretical background as

many as nine books related to risk management were used as well as seven professional journals about the export business to Russia.

Similarly, online articles and publications were an important source of information due to the dynamic field of Cyber Security and the Russian market. I reviewed at least fifty articles related to the key words defined in this thesis. Moreover, for the proper formation of the thesis, I also carefully read five closely related thesis topics that were published in recent years in Finland and worldwide.

The Survey

The respondents that were carefully chosen had vast experience in their field of expertise; therefore their input was essential in the formation of an accurate understanding of risk elements and a risk management strategy.

The survey was chosen as a tool for orientation for further discussion and interview with the respondents. In the survey there were four open ended questions that comprised of the following questions:

1. What general risk factors exist for ICT startups
2. What unique risks are there in the Russian market unlike in other countries?
3. What financial risks are there for a cyber-security startup doing business with big companies in Russia?
4. Which risk in your opinion is the most critical? And how is it possible to reduce or eliminate this risk?

Question number three included a direct use of financial risk which is a part of the ISO 31000 risk management framework. This was due to the preconceived notion before the research study that such a risk type is the most significant one in the Russian market. However, as the survey results were collected it was evident that the Reputational and Marketplace risks are the most relevant.

Consequently, the focus of the interviews was on these risks rather than the Financial Risk.

The survey was sent to 23 respondents, out of which 12 directly replied to the survey before the meetings, while eight respondents preferred to fill in the survey together while I was making notes during the interview. Three respondents were not able to respond due to their busy schedule and sensitivity of the subject.

Semi Structured Interviews

All of the interviews were conducted in a semi structured form and were exactly the same questions as were in the survey with the expectation of obtaining deeper knowledge. Semi structured interviews are comprised of open ended questions and it allows further probing on subjects that contribute to the exploration process of the theme. Unlike a questionnaire the semi structure interview format allows the respondent to form his own unique answer, thus enriching the subject that is being researched (Teijlingen 2014, 15-23). The setting of the interviews was usually at the office of the respondents. The interviews were not recorded but notes were taken during the interview or immediately after while the information was still fresh. For both surveys and interviews the respondents were provided with a complete anonymity.

Participant Observation

Being a participant observer was an inseparable part of the research process. Due to the fact that I had been the General Manager of the company in Finland for two years, I was deeply involved in the different operations and management activities. This gave me the possibility to obtain tacit knowledge that is not readily available in books and other sources of information. The “insider” knowledge contributed to the depth of engagement I had during the business meetings in Russia and my overall comprehension of Trulyprotect’s strategic development. The literature defines participant observation in a way

that it "combines participation in the lives of the people being studied with maintenance of a professional distance that allows adequate observation and recording of data" (Fetterman 1998, 34-35).

5 Results and Analysis

The following results will aggregate the secondary and primary data through PESTLE and SWOT analysis and the results from surveys which are presented in the form of a table.

5.1 Establishing the Context

In order to establish the context and understand the unique environment in which Trulyprotect plans to operate a PESTLE and SWOT analysis were conducted.

PESTLE Analysis

The PESTLE framework will assist in evaluating the market which we wish to enter into. In this case the Russian market will be approached from various angles to understand what environment we plan to operate in.

Political

The international tensions between the US/EU and Russia have been emphasized through the nationalistic approach Russia has taken in their politics related to information technology and, particularly, data protection.

The Russian government increases its budget to support its political agenda and, therefore, is located fourth among top 6 cyber armies in the world. Igor Korotchenko, editor-in-chief of National Defense magazine, said Russia increased the financing of cyber security programs after 2010 when American and Israeli secret services dealt a severe blow to Iran's nuclear sites during the Stuxnet Operation. (RBTH 2017)

Russia's cyber army hacks a spot in the Top 6

	Annual financing in millions of dollars	Number of cyber troops
U.S.	7,000	9,000
China	1,500	20,000
UK	450	2,000
Russia	300	1,000
Germany	250	1,000
North Korea	200	4,000

Table 9 RBTH website, January 2017

Economic

The political situation has had a negative effect on Russia's economy in the form of imposed sanctions. *The Russian economy shrank by 3.7% in 2015, while real disposable income fell by 10%* (World Economic Forum 2016). The Ruble has depreciated, oil prices have decreased, unemployment has risen and the growth rate has declined. Nonetheless, Russia attempts to attract foreign direct investments from various sources particularly from Eastern countries such as China. This direction according to the International Monetary Fund (IMF) may prove that Russia's economic condition was less severe than previously thought, and the economy is expected to return to growth, unless oil prices plunge again.

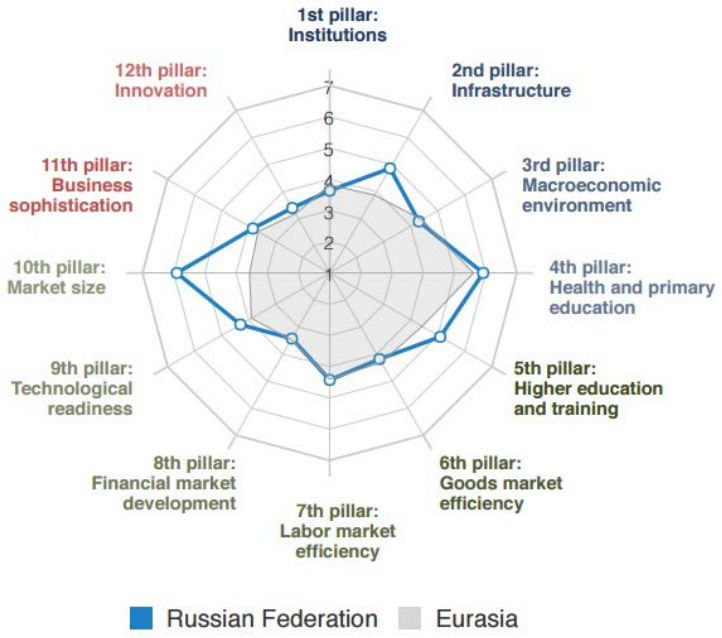


Figure 3 Russian Market competitiveness, World Economic Forum 2016

There is a strong tie between economic performance and cyber security. For instance, in early December 2016 the FSB said foreign cyber attacks were planned against Russia's banking sector. The foreign hackers' goal was to create a crisis in Russia's credit-financial system, force companies to file for bankruptcy, and cause Russian banks to lose their licenses. (RBTH 2017). Since there is a major concern for such a scenario, Russia is tightening its cyber belt around itself and invites new tech companies to solve these issues.

Another form of economic support for new Tech providers is tax incentives. The Russian Government continued introducing federal tax incentives aimed at attracting investments into Far East regions, green field projects. Moreover, regional authorities continue to compete with each other introducing new property tax and profit tax benefits, thus allowing for many possible tax and non-tax incentives to be granted at regional level. (Deloitte 2016)

Moreover, Russia rose two places on the index to 43rd. The report (World Economic Forum 2016) pointed out that this was partly due to better scores on education and innovation, in addition to an improved domestic business environment and less negative business sentiment than expected (ibid.).

Social

The Russian society has shown resilience facing the deterioration of the economic conditions. According to Scaramucci, Russians would eat snow if they had to survive. And so, for me, the sanctions probably galvanized the nation with the nation's president (SOTT 2017).

During my stay in Russia it was evident from my discussions with private individuals that the support of Putin has been rising and any social uprising against any controversial laws, such as anti privacy, will gain support from the majority of the society to insure the interests of Russia in the region.

In addition, the government is actively seeking to silence any possible uprising through social media networks, as happened in the Arab spring. This may be viewed as a negative move by the government from the human rights perspective. On the other hand, from the perspective of governance stability and sustainability it may, in fact, be positive allowing for a possibility to safely export our services into the Russian market without the threat of regime instability such as in Syria.

Technological

Some nations are better prepared than others to deal with damaging cyber attacks from criminals, terrorists and rogue nations. Data experts have ranked the vulnerability of 44 nations to cyber attacks. The United States ranked 11th safest, while several Scandinavian countries (Denmark, Norway and Finland) ranked the safest. China, India, Russia, Saudi Arabia and South Korea ranked among the most vulnerable. (Sciencedaily 2016.)

Russia holds the 69th place out of 128 countries in the global Innovation ranking which may imply that their technological development is not the highest in the world. Therefore, our solutions may be suitable for their market needs. (WIPO 2016.)

Legal

A new wide set of laws have been introduced lately that usher in a new era of intense focus on data collection from individuals and new cyber security standards to keep the West at bay. New laws such as described below are meant to provide tighter regulation of data. Subsequently, the business opportunities for cyber security companies are growing (SVKK 2017).

New Laws list (Jdsupra 2017):

- Federal Law No. 374-FZ on Amendments to the Federal Law on Combating Terrorism and Certain Legislative Acts of the Russian Federation with respect to Establishing Additional Measures for Combating Terrorism and Ensuring Public Safety of July 6, 2016

- Federal Law No. 244-FZ on Amendments to Parts I and II of the Russian Federation Tax Code of July 3, 2016

- Federal Law No. 475-FZ on Amendments to Article 105.14 of Part I and to Part II of the Russian Federation Tax Code of December 28, 2016

5.1.1.1
Environmental

Environmental changes may have tremendous effect on the demand level of our cyber security services. Both the global warming, the availability of pure water supply, the level of pollution and other environmental concerns can potentially increase the need for our products.

Global warming plays a strategic role for Russia as it counts on the slow climate change in the North Pole to the degree it would be used as a future trade route. As of today Russia has already established a military zone in the area as expressed in an article titled *"Russia Launches Biggest Arctic Military Expansion Since Fall Of USSR"* (Zerohedge 2017). Since the military expands in this region, additional focus on cyber security would have to be considered

by the army, thus making the Russian government allocate additional funds for such long term projects.

As air pollution becomes more and more a substantial concern world wide the use of autonomous cars will increase as a future trend. The Russian elite would be willing and able to afford themselves these types of cars as mentioned in an article called: *"Sales of luxury cars in Russia up 6.5% in 2016"* (Litovkin 2017). Our developments can prevent intrusion and remotely break into such autonomous vehicles. This is, of course, not only specific to the Russian market, but it has global implications which can then be relevant for this market.

SWOT analysis

Below is a SWOT analysis for the Russian Market based on the feedback I received from the meetings and my own conclusions.

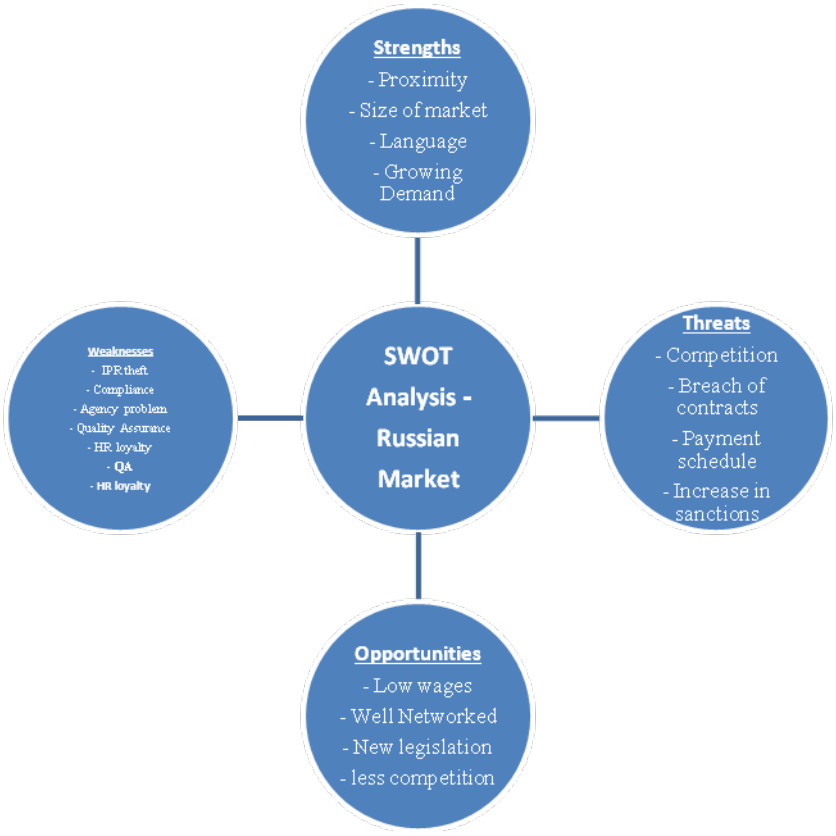


Figure 4 SWOT analysis for the Russian Market

Strengths

- Proximity: The proximity to Saint Petersburg and Moscow is a great advantage. Within five hours one can arrive there. It is almost the same driving length as to Helsinki from Jyvaskyla. This reduces possible agency issues. The time difference is also only an hour which makes business meetings possible with ease unlike doing business in USA, China, Japan or other far reached countries.

- Size of market: Merely the size of Saint Petersburg covers the whole population of Finland. Moreover, the Russian cyber security market is expected to grow from $1.82 billion in 2013 to $2.89 billion in 2019, at a CAGR of 7.30% for the period 2013 to 2019 (Micromarketmonitor 2017). This constitutes a significantly bigger market than the one in Finland.

- Language: Unlike many other Finnish companies, our advantage is that I am able to communicate well in Russian. During the trip I conducted well over 35 business meetings in Russian and was able to create trust between the parties and receive support. This strength should not be undermined since should I have spoken in English the market would not have welcomed me as it did. In addition, the translation of the website to the Russian language was significantly important as it demonstrated the Russian partners that Trulyprotect is serious with its intentions and willing to adapt to meet the customer's needs in the region.

- Growing Demand: The Finnish Russian Chamber of commerce has published and article titled *Information security booming in Russia*. In the article it was stated that Information security is one of the most popular ICT topics in Russia. Local companies have an increasing demand for information security solutions because of cyber threats and new data localization measures. (SVKK 2017.) I contacted the author of the article, and he indeed arranged a meeting for me with a local integrator the following week.

Weaknesses

- IPR theft: Russia is said to be among the top countries with the most significant concerns regarding insufficient [intellectual property rights] protection or enforcement or actions that otherwise limit market access for persons relying on intellectual property protection (Furgchtgott-Rott 2017). Thus, the greatest concern for international companies is protection from such theft routinely. Due to these facts, Trulyprotect must hedge against sending the source codes to Russian integrators and perhaps extend only binaries and hire local Israeli Russian work force to keep our IPR at bay.

- Compliance: Adhering to our own corporate culture and management discipline may be extremely relevant when conducting international projects. An agency problem is not only specific to the Russian market, although it may be overemphasized there as the attitude to labor and ethics vary between the Finnish and the Israeli approach. With regards to compliance should Trulyprotect chose to have a local branch and legal entity in Russia, it can have a clear tasks, goals and performance evaluation on a monthly basis to make sure that the tasks are fulfilled.

-Quality Assurance: Despite the fact that the Russian programmers are considered highly professional due to advanced education system (ITMO, GUAP and others), there might still be disparity between programming technique and the productivity level of Russian employees. These may, therefore, project on the overall quality of the product and service resulting in poor delivery and possible damage to our brand image.

- HR loyalty: Based on feedback I received from Finnish experts on Russian market export, new recruits like getting trained by international companies but they are not loyal and are willing to move on to a new position once offered 100 Euros more by a competing company. A possible solution could be having a Vesting agreement based on shares and bad leaver case for two years including a low compensation for work (400 Euros).

- Long sales cycles: Due to the complexity of our product and the large size of the companies we address the sales cycle is rather long. This may of course be a rewarding process for big lucrative contracts if the sales process is successful; however, there is no guarantee whatsoever that a strong sales lead will eventually end up as sales contract. Moreover, according to an article about risks associated with long sales cycles (Gibson 2017) there are various risk elements such as: poor customer targeting and profiling, misunderstanding the buying process, lack of customer information and bidding and winning contracts that cannot be materialized (Gibson 2017).

Opportunities

- Low wages: According to Glassdoor (2017) the average salary of a developer in Moscow region can be about 1,200 Euros while as a programmer with a similar skill set may cost around 5,000-7,000 Euros. This is a whooping difference of up to 6 times of wages of a developer in Israel or in Finland. The opportunity is obvious. Low wages yet not lower quality necessarily. This also correlates with various discussions I had with experts in the field in Russia.

- New legislation: Higher standards for Cyber Security in Russia have been recently enforced by new information security laws. For instance, in the summer, a measure known as Yarovaya's law was introduced, which requires Russia's telecoms and internet providers to store users' data for six months and metadata for three years. (Soldatov & Borogan 2016.) This new legislations among others is calling upon the increase in demand for data protection services which Trulyprotect can provide for Telecommunication companies for example.

- Well networked: In my recent activities I invested much in forming a robust network by meetings with, Finpro, East consulting, Finnish Russian Chamber of commerce, JYKES, Gazprom, Rocla, IT manager Journal, Ingria, ITMO, GUAP universities and others. I believe I have established a well-articulated

network that can support a creation of value chain in Russia from legal business entity formation through accounting services, marketing, programming, integration, sales support and customer satisfaction. This opportunity should not be taken for granted, as it is also dependent on the availability of these partners at this moment, which may not be the case in the future.

- Less competition: During my discussion with Olga Popova, she mentioned that various ICT companies had pulled out of Russia since the Russian attitude has become stricter towards US companies. It is also possible to find a testimony for that in an article titled *Russia Tightens Grip on Tech Infrastructure, Cuts Ties With US Firms (*Advox.globalvoices 2016). One of the main statements in the article read that this policy aims to pull US companies out of Russia's technology ecosystem, a move that would presumably provide greater protection from surveillance born out of cooperation between US firms and US intelligence agencies, as well as the removal of a American leverage point in the event of further sanctioning. (ibid.)

The fact that some US companies are pushed out does not mean that a Finnish company would have the same treatment. I would even say that the contrary is true. During the meeting with Dr. Rabin from GUAP he mentioned that they are more than open to cooperate with Finland based companies.

Threats

- Competition: Big companies that might re-enter the market once sanctions are lifted off may reduce profit margins. In addition, at the moment various system integrators are scanning for new partners and are eager to replace other partners that quit the market.

- Breach of contracts: one must ensure that our partners actually comply with agreements. This may be a tedious process and exhausting financially if companies should violate agreements. In many cases the enforcement of

punishment over violation of contracts may not be sufficiently severe to deter any criminal activities.

- Payment schedule: Based on an article called *Market Monitor - ICT industry – Russia* (Atradius 2017) the following was stated: Depending on the level in the supply chain and market leverage of businesses, payment duration in the industry ranges from 30 days to 120 days. Non-payment notifications have increased in 2015, and this negative trend is expected to continue in the coming months. (ibid.)

- Increase in sanctions: The Russians have a real urgency to get back to normal economic relations and get these sanctions removed (CNBC 2016). However, despite the warm attitude of Donald Trump and Putin to restore relations there is always a chance that the sanctions would deepen. So much so that the Ruble would keep devaluing, unemployment would rise, the GDP would fall and local companies, which would in turn hinder our growth, will not pay local integrators such as Trultyprotect's partners.

- Delivery failure: Due to the lack of workforce and capacity, if Trulyprotect take up many projects it might not be able to deliver the projects. Otherwise, even if outsourced there is an exposure of revealing our code to external developers which is a significant threat to our intellectual property.

- Cyber Security sector: As a Cyber Security Company, Trulyprotect faces a unique set of risks unlike other companies within the IT sector. For instance, in an article written by Amir Kotler (2016) it was stated that "42% of cyber security companies surveyed report lack of demand for their product in the market. Start-ups fail for the most practical of reasons - assembling the wrong team for the project 23% and stronger competition 19%. Running out of money is rarely the root cause for failure, but only a symptom". (Kotler 2016.)

Due to the sensitivity of the field of cyber security, such companies face a higher barrier of market entry due to the orthodoxy of commercial markets.

Such is also the experience of Trulyprotect in its penetration efforts in the Finnish market.

5.2 Identified Risk Types and Elements

After collecting all the surveys and interviews and organizing them in a chart I searched for risk elements and risk types. The coding used for the results were symbol “R” for Risk and a following number of the risk. For instance, “R1” means Risk number 1. In addition, the coding for Respondent number was “Res” with the addition of a number, thus “Res 1” means respondent 1. Regarding the findings, all in all there were 30 different risk elements that were recognized based on the framework of four risk types of Finance, Operations and Strategic, Information and Technology risk which correspond to the ISO 31000 framework (Moeller 2011, 35).

The most noticeable difference in the risk types is the fact that there are significantly more elements that are relevant for the Russian market from the operational and strategic risks rather than Information and Technology risk and finance risk. The following tables present a summary of the highlights found in the results from different respondents:

Finance Risk type and Elements

The risk of finance elements that were found can be analyzed through various characteristics of risk types Table 8. For instance, “Foreign exchange risk”, “capital availability” and “duration risk” can be referred to as an internationalization and speculative risk. As a result, these risks can be handled by avoiding entering an international market or choosing a market entry mode that would minimize these risks. Other risks such as “default risk” and “budgeting risk” are not related to internationalization; they may be referred to as absolute and general business risks since the consequence of such risks will always be negative and are a result of poor general management.

Symbol	Risk Element	Quotes from respondents
R1	Foreign Exchange Risk	Res 18: "The Ruble is currently low compare to what it used to be before the crisis. If the situation gets better, development costs would be higher. Fluctuation of currency caused many Finnish companies to pull out of the Russian market due to loss of profitability"
R2	Duration Risk	Res 20: "Finland is not a good place for sales, for every 400 visits in Finland you will have 1 that will succeed, it is not a profitable move , Sweden is better for sales. Finland would get you desperate. Now is a good time to go to Russia, because when you establish yourself there, when it opens up you will have both of your feet there. Russians are loyal, if they are good people, but the bad ones are bad people"
R3	Default Risk	Res 12: " Your startup company may default on payments to other providers in case you don't manage your cash flow well"
R4	Capital Availability Risk	Res 2: "Russian markets with your cyber security start up, I think that you might enter into problems with getting the money (payments) out of Russia"
R5	Budgeting Risk	Res 5: "Very often project managers do not have elementary financial and management competencies, the lack of which leads to negative consequences. Errors in the start-up budget calculations."

Table 8 Finance Risk type and Elements, Respondents

Information and Technology Risk type and Elements

There were not many risk elements in this category; although "Taxation risk" is an absolute risk that must be avoided and an Internationalization risk, since it occurs due to the internationalization process. "Information access risk" is a general Russian market risk that will affect any company in any industry that operates in Russia, meaning that this is not a specific risk that Trulyprotect is especially susceptible to, being a Finnish cyber security startup with limited resources. This risk also affects small to medium companies as well as large companies. The main difference is with the resources each one employs to find a solution for this risk.

Symbol	Risk Element	Quotes from respondents

R6	Taxation Risk	Res 4: "Determining who pays the Value added tax can be critical. Usually the customer who buys it pays but in software business it might be the other way around for a foreign company. There was an instance that one Finnish company realized that they had to pay the Tax at source but it was too late and they had to pay large sums which made the deal unprofitable."
R7	Information Access Risk	Res2: "I assume that market research and other services have improved in Russia, but still. How to find reliable business partners, if you do not have good and "right" contacts, it is almost impossible. You have to understand the meaning of networks in doing business in Russia."

Table 9 Information and Technology type and Elements, Respondents

Operations Risk type and Elements

Operations Risk is one of the most significant types of risks since fourteen out of thirty risk elements were found under this type. Training Failure Risk, Policy and Procedure Risk, Human Resource Risk, and Cycle Time Risk can be categorized as General business risks. While Litigation Risk in the context of the respondents' reference is related to the Internationalization risk. Partner Risk element is considered a specific risk in this instance. All the rest of the risks; Policy and Procedure Risk, Supply Chain Risk, Process Execution Risk, Non Payment Risk, Fraud Risk, Environmental Risk, Employee Turnover Risk, Crime Risk, Corruption Risk are General Russian Market Risks.

Symbol	Risk Element	Quotes from primary data
R8	Training Failure Risk	Res 9: "Some companies fail to adequately train their expatriates about the operations in a new country. This can be critical to the failure of a project"
R9	Supply Chain Risk	Res 11: "trust is everything. When you find an honest Russian you are safe, finding honest partner, this is the main risk I found."

Symbol	Risk Element	Quotes from primary data

R10	Process Execution	Res 3: "The higher level of bureaucracy in Russia leads to more expensive and slower projects" Res 9: "The lack of standards (CONVET) brings chaos into the relationship between the initiators of projects and investors, which, as a consequence, leads to a slowdown in the implementation of the start-up"
R11	Policy and Procedure	Res15: "As a rule, the risk lies in ignorance of the market, market processes and practices, due to certain unwritten rules or customs, including laws and legal practices"
R12	Partner Risk	Res 14: "It's hard for startup to make business with big companies. You need background, experience, success cases and transparent financial background behind the business" Res 17: "Local Business prefers to cooperate with Russian companies. They feel a strong distrust to foreign IT-products. Especially in the information security market"
R13	Non Payment Risk	Res 3: "a large company may delay payment for several months, Low business ethics in Russia can cause bigger companies not to pay for start-up services" Res7: "Because the need of money and references, mixed up with the nature of the business, startups are also most cheated companies. Lack of payments, some cons on contracts, etc. List is unlimited"
R14	Litigation Risk	R19: "facing lawsuit charges by another company is possible especially if you are entering a new market with high competition"
R15	Human Resource Risk	Res 3: "Participants in large company's project can have restricted competency in ICT or have lower personal motivation in participating in a project, which can negatively affect the progress and outcome of the project."
R16	Fraud Risk	Res 4: "If the director wants to scam he can establish the same company with the same full name and address and by sending a bill to clients and charging them to the name and account they created to steal from you. The payer will not notice the difference. But in your case it is not the biggest problem since there is not a lot of money anyway"
R17	Environ-mental Risk	Res 5: "From my personal point of view, laws and "way of living". If you are foreigner, you are foreigner. Everything can change overnight and there is no contract or deal that you can actually count on R15: "In parallel with the established laws, there are unwritten rules. It turns out that a law is written only on paper, and in reality the life processes follow other rules"
R18	Employee Turnover Risk	Res 3: "Specialists with the necessary technical competencies can move to other more interesting or more successful projects"
R19	Cycle Time Risk	Res 2: "The timing to enter the markets is not right. In some cases the markets are not ready for some new innovation, i.e. the window is not open yet , but it can be open after a period of time, but does the start up exist then anymore"
R20	Crime Risk	Res 8: "Unknown parties supported by public officer can overtake a company. Good example described in book written by Bill Browder"
R21	Corruption Risk	Res 16: "Bribes are often required in the Russian market to achieve progress. bribes cannot be reported in the company financial sheets"

Table 10 Operations Risk type and Elements, Respondents

Strategic Risk type and Elements

Under the strategic risk type some may be considered company specific such as Trade Barriers Risk, Customer Needs and Wants Risk, Patent/Trademark protection and Competitor Risk while others are general Russian market risks, for instance, Reputation Risk, Political Risk, Legal and Regulatory Change Risk, Economy Risk. There is only one Born Global risk in the results which is Industry Risk.

Symbol	Risk Element	Quotes from primary data
R22	Trade Barriars Risk	Res 2: "I know that there is a law in Russia about foreign investments to so called strategic business areas, one being defense. So if you are in cyber security business, that definitely is strategic area and you will face some issues with Russian government" Res 12: "Import replacement program. Applies also to software on some level"
R23	Reputation Risk	Res 9: "Branding Risk- Western markets might not like the fact you do business in Russia and might pull off" Res 7: "company with no history, with no references and "no trust that there is tomorrow" is making acquisition decision really hard for the customer. And if there's no deals, there's no business and then there's no company"
R24	Political Risk	Res 14: "the startup sphere may be limited or restricted for non-government or foreign entities"
R25	Patent/ Trademark protection	Res 16: "Technology theft. The risk is almost impossible to Avoid. Probably one should avoid business in Russia. Especially with novel technologies. Focus on Europe, USA and Pacific"
R26	Legal and Regulatory Change Risk	Res 1: "Quick and often changes in legislation" Res 8: "government and different public organizations. They can end business by some new regulation"
R27	Industry Risk	R7: "most of the customers are trying to take advantage from the startups position. They are trying to dictate terms and prices, it's not negotiation, it's dictating. And too many startups accept those situations and deals, no matter how good their product is. Of course, startups need the money and that's the main reason to accept bad deals, but in many cases those bad deals and reputation to accept "anything" will also ruin the chances of the company"
R28	Economy Risk	Res 4: "There is a significant slowdown of business from Finland to Russia. In the past I had 20 meetings when I came for one week to Finland, but now when I come there were no meetings at all! Finnish Russian trade was good in the past, people were willing to spend more, not now anymore"

Table 11 Strategic Risk type and Elements, Respondents part 1

Symbol	Risk Element	Quotes from primary data
R29	Customer Needs and Wants Risk	Res16:"Market response - As ICT start ups start at a certain phase with no market validation what so over it is difficult to predict the market response to disruptive technology."
R30	Competitor Risk	Res 1: "There are some general players in ICT market in Russia. Basically, they have strong and long term relationships with their suppliers - program builders, software implementators and etc. When new company come the market (especially from abroad) the process to including of new software to their «product portfolio» can take long time and it will be not so easy. I think not every of ICT company is ready to execute this way." Res 13: "Replicating pirated programs is very common (for example, Microsoft Office, Windows, 1C, reference and legal programs, such as Consultant plus, Garant)."

Table 12 Strategic Risk type and Elements, Respondents Part 2

Risk Elements Map

The map below summarizes all elements in one map as follows:

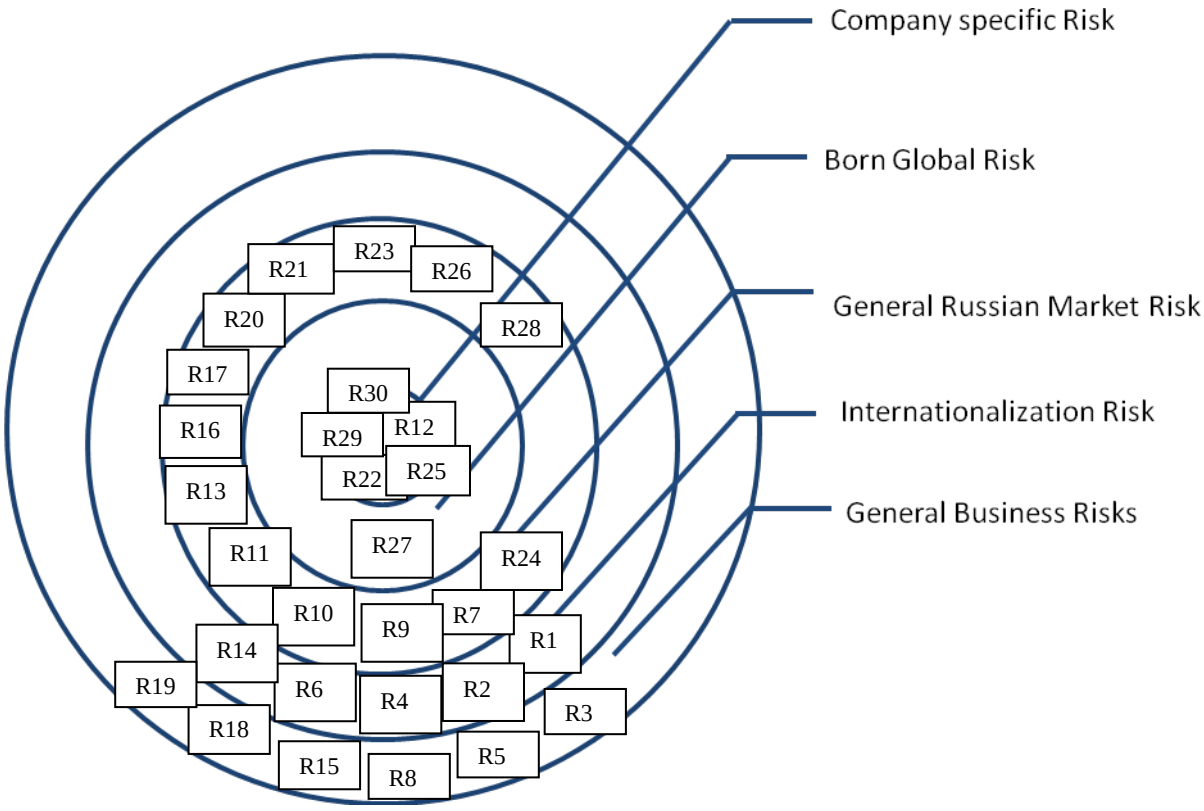


Figure 5 Market Elements Risks Map Summary

The aim of Figure 5 is to illustrate the extent to which the more the risk is moving inwards to the center of the map, the more the risk is relevant to Trulyprotect as a company operating in the Russian market. Nonetheless, the

more distant the risk from the center of the circular map the more it applies also to other businesses. In other words, should another non ICT company want to enter the Russian market they might experience similar types of risks. This is important because it emphasizes the relationship between the type of business and the risk type it may face.

5.3 Risk Analysis and Evaluation

After establishing the context, identifying the risk types and analyzing them it is now the stage in which a risk evaluation is made to find out which ones pose the highest and the lowest threat. Determining the likelihood of a risk to occur and the potential consequences were determined by based on observation of the collected data and the context by which Trulyprotect operates. For instance, R25 – Patent and Trademark protection risk was chosen to have "catastrophic" consequences with the probability of "almost certain" which means over 95% chance of occurring with a potential disaster that can lead to collapse of the business in Russia if our IPR is stolen and distributed by a big competitor.

		Consequences				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain			R11- Policy	and Procedure R22- Trade Barroars R26 – Legal and Regulatory Change	R25- Patent/ Trademark Protection R30 - Competitor
	4 Likely	R19 – Cycle Time R2- Duration	R14- Litigation R21- Corruption	R10 - Process Execution R17- Environmental R24 – Political	R28 – Economy R18- Employee Turnover R23 – Reputation R27- Industry	R13- Non Payment R29- Customer Needs and Wants
	3 Moderate		R12- Partner R9- Supply Chain R3- Default	R1- Foreign Exchange R7- Information Access	R15- HR risk	R16 - Fraud
	2 Unlikely		R5- Budgeting	R8- Training Failure		
	1 Rare		R4- Capital Availability	R6-Taxation		R20- Crime Risk

Table 13 Risk Evaluation Table (Global CCS Institute, 2017)

As seen in table 12, 2 risks are considered low, 6 moderate, 6 high and as much as 16 are considered extreme.

5.4 Risk Treatment

After categorizing the risk elements based on their level of threat, in the risk treatment part, strategic tools are applied to reduce or eliminate the damage. In order to understand which strategy to choose, concrete objectives of the company in the Russian market must be determined as made in Figure 6. Following this step, the most probable risk threats that are related to the objectives will have a proposal of a strategic step to treat it to achieve the objectives.

Objectives

The objectives of Trulyprotect in the Russian market are the following stages:

1. Finding 2-3 system integrators to cooperate with. Integrators should be large, above 1000 workers, with the capacity to provide after sale service with a call center and highly qualified.
2. Integrator should be a market leader that wins major government/ commercial tenders.
3. Together with the integrator we will incorporate our solution to the existing products of the integrator or provide a unique solution, in the corresponding markets (Defense, health tech, telecommunication, finances, infrastructure) for the end user and share the revenues.
4. If the business succeeds, an office can be established for sales and research and development of five to ten employees.

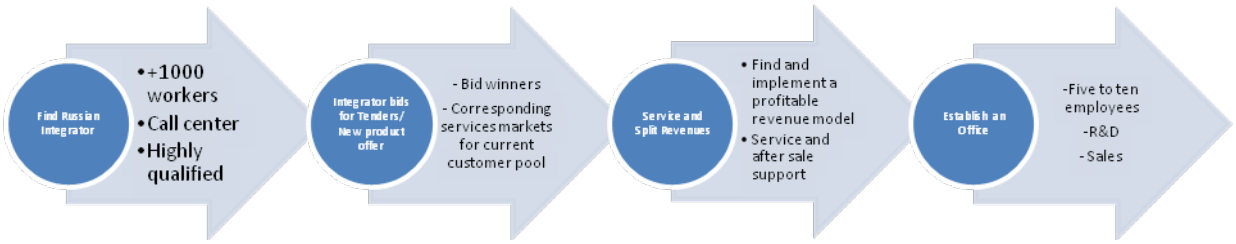


Figure 6 Trulyprotect's objectives for the Russian Market

Stage 1 Risks and Treatment Strategy

The first stage which involve low level of know how contribution and low level of ownership as an entry mode, involves mainly moderate risk outcomes which can be strategically treated with risk transfer or acceptance while extreme risk outcomes should be treated with a mitigation strategy as seen in Table 14. This entails that various preemptive measures must be put in place before these risks materialize and have their catastrophic effect. For instance, a competitor risk should be solved by naming the main competitors in the market and deciding whether to compete, form an alliance or differentiate. This strategy reduces the risk of being targeted by major competitors and labeled as a non desired competitor in the market which can result in a fierce competition over market share.

Objective and steps	Sym-obol	Risk Type	Risk Evaluation	Treatment	Solution
Finding 2-3 system integrators	R12	Partner	Moderate	Transfer	Outsource
	R19	Cycle Time	Moderate	Transfer	Outsource
	R2	Duration	Moderate	Acceptance	Tolerate
	R21	Corruption	High	Avoidance	Don't give bribes
	R5	Budgeting	Low	Acceptance	Tolerate
	R7	Information Access	Moderate	Transfer	Outsource
	R8	Training Failure	Moderate	Acceptance	Tolerate
	R9	Supply Chain	Moderate	Transfer	Outsource
Large & powerful integrator	R27	Industry	Extreme	Mitigate	Awareness and preparation
	R26	Legal and Regulatory Change	Extreme	Mitigate	Awareness and preparation
	R28	Economy	Extreme	Mitigate	Awareness and preparation
	R30	Competitor	Extreme	Mitigate	Allience, differentiation, competition

Table 14 Stage 1 Objectives, Risks and Treatment Strategy

Stage 2 Risks and Treatment Strategy

In the second stage when there are serious sales prospects and the solution is incorporated into the integrator's pool of customers there are also as in the first stage extreme risks that can terminate the business operations if not treated properly. These risks can be mitigated through various steps such as trademark coverage for patent and trademark risk. This would reduce the damage of another company using the intellectual property of Trulyprotect. This of course does not guarantee misuse of the intellectual property, yet it may deter those who attempt to do so. In addition, political risks may merely have a moderate effect on this stage of operations and the proper strategy is acceptance since there is very little that can be done in case strict bans are imposed and western companies are forced to leave. The damage at this point is not catastrophic since there were relatively fewer resources invested in the operations and development as it may possibly be in stage four.

Objective and steps	Sym-obol	Risk Type	Risk Evaluation	Treatment	Solution
Solution incorporation	R10	Process Execution	High	Mitigation	Awareness and preparation
	R24	Political	Moderate	Acceptance	Awareness and preparation
	R11	Policy and Procedure	Extreme	Mitigation	Awareness and preparation
	R22	Trade Barriers	Extreme	Mitigation	Awareness and preparation
	R25	Patent/ Trademark protection	Extreme	Mitigation	Trademark coverage
	R29	Customer Needs and Wants	Extreme	Mitigation	Continuous Marketing Research
Find projects and Form contracts	R6	Taxation	Moderate	Mitigation	Outsource

Table 15 Stage 2 Objectives, Risks and Treatment Strategy

Stage 3 Risks and Treatment Strategy

Once a contract is signed and the delivery of service is expected from Trulyprotect in stage three, there are low, high and extreme risks. These risks can be strategically approached through risk transfer and mitigation. The risk transfer as a treatment strategy, for example, can include an insurance made by Trulyprotect that can cover possible losses in case there is a litigation by a third party for underperformance or breach of contract. The insurance may cover a possible theft of hardware from the main office which might delay the delivery time or sabotage it altogether. In such cases, even if there is a loss made due to litigation, the insurance company will cover some of the damages directly or indirectly depending on the insurance terms and types.

Mitigation strategy can be useful even with low risk outcomes. For instance, capital availability risk can be mitigated through a careful financial planning and payment of costs to holding company as “consulting "or “marketing” services instead of keeping all the revenues inside Russia and not being able to reinvest the capital in other countries.

Objective and steps	Sym-bol	Risk Type	Risk Evaluation	Treatment	Solution
Deliver service/ product	R14	Litigation	High	Transfer	Insurance
	R17	Environmental	High	Mitigation	Awareness
Receive Payment/ Move cash to Finland	R1	Foreign Exchange	High	Mitigation	Awareness and preparation
	R13	Non Payment	Extreme	Mitigation	Litigation
	R23	Reputation	Extreme	Mitigation	Public Relations
	R4	Capital Availability	Low	Mitigation	Financial Planning

Table 16 Stage 3 Objectives, Risks and Treatment Strategy

Stage 4 Risks and Treatment Strategy

In stage four after a successful sale has been executed and the first prepayments have been received there are moderate, high and extreme risks that can be mainly treated with a mitigation strategy plan to minimize the damage of a potential loss exposed activity. For instance, fraud probability reduction by a robust recruitment policy that would reduce the chance of hiring employees with a criminal background and mitigation of employee turnover risk by creating a lucrative incentivisation plan that would be beneficial for the employees on the long term.

Objective and steps	Symbol	Risk Type	Risk Evaluation	Treatment	Solution
After sales support	R3	Default	Moderate	Mitigation	Budgeting
Possibility to Establish an office in Russia	R16	Fraud	Extreme	Mitigation	Recruitment Policy
	R18	Employee Turnover	Extreme	Mitigation	Incentivisation plan
	R15	Human Resource	Extreme	Mitigation	Recruitment and workshops
	R20	Crime	High	Mitigation	Exit plan

Table 17 Stage 4 Objectives, Risks and Treatment Strategy

5.5 Conclusion

As it is evident through all stages of the objectives of Trulyprotect, the risks are treated mainly through a mitigation strategy. Since the transfer of risk through insurance is not efficient in Russia or risk transfer to other companies may reduce profitability, it is not the most preferable tool. Risk avoidance may result in not entering the market altogether and not exploiting the various existing opportunities. Risk acceptance does not apply in many cases since there are only a few risk elements that are classified as low to moderate impact

risk. Therefore, this is also not as efficient as risk mitigation which forms a premeditated layer of protection that reduces the damage of a risk exposure.

5.6 Research Quality

The research quality and ethics are of uttermost importance as it insures that the collected information, analysis and recommendations are genuine and are not affected by biased opinions which can distort the results. These are often discussed in terms of research validity, reliability and limitation of the study to ensure the reader that the results might not be applicable in other fields of research.

Validity

The choice of primary data collection was based on multiple sources from various fields, such as accounting and law firms, consulting firms, government services, export agencies, business incubators, system integrators, business partners, IT associations, marketing agencies and non ICT Finnish companies that export and operate in Russia and Finland. Such approach reduces the bias and narrow approach to risk perception by one party. The wealth of resources enhances the validity of a certain type of risk, particularly, if it was occurring repetitively from various respondents from different fields of expertise.

Reliability of data

Choice of Secondary data – classic literature in the field of cyber security may not be valid after a short period of time. Therefore, textbook sources are not as relevant as online sources that are up to date, particularly, when the subject in matter relates to new legislations, tax reforms or new cyber security regulations in Russia. Hence, the reliability of the sources might be questionable if not double checked from sources, which was the procedure in this study. This approach decreases the concern of unreliable and manipulated data.

In addition, since the risk evaluation was based on the observation of experts' assessment of probability and frequency and not statistical data of such risk occurrences, the result may be valid and reliable. However, the validity might be compromised since it might be subject to optimism bias and a conflict of interests. (Walker 2013, 8.)

Limitations of study

The limitations of the study are based on the geographical area in Russia in which I chose to focus on, which is mainly Saint Petersburg and Moscow. There are other areas that may have different types of risks. Therefore, the study mainly refers to the main business capitals of Russia which we aim to operate in. Furthermore, another limitation is access to primary data. Since the field of cyber security is highly sensitive and relevant on the level of homeland security in Russia many companies are reluctant to disclose information about the risks they face. This directly limits the quality and depth of the collected data.

Furthermore, the aspect of implementation of the strategy and monitoring, which is a part of the ERM process, was not provided in this study. Subsequently, the efficiency of the strategy was not tested, and thus providing a correlation between the strategy and positive business outcomes may not be guaranteed.

Generalizability

Part of the results in this study can be generalized, especially if it is a Finnish ICT startup regaring the risk identification. Yet the analysis and strategy formation is strictly related to the context and business sector in which the copmpany operates. Thus if it is not a Cyber Security company, some of the risk management strategies may not be generalized and since other companies might have different objectives and market entry strategy.

5.7 Further research recommendation

Having stated the abovementioned strategy for the Russian market, it may be worthwhile to conduct a benchmarking research for other post Soviet Union countries. Such countries which have low costs of doing business and rise in cyber security demands include for instance, Kazakhstan and Uzbekistan. Since they are Russian speaking countries and are not affected by sanctions from the European Union it might be a possible target market to enter while keeping the risk levels low.

In addition, I believe that it is also possible to engage in a quantitative approach that would address the ICT sector to validate certain risk types as being more significant than others on a statistical level. This would, subsequently, assist in better decision making for business problems entering the Russian market.

Finally, since the focus of the research was on the formation of a strategy based on ERM process the implementation and testing of the proposed model was not carried out. Therefore, a possible further study can focus on implementation and monitoring of the outcomes of the strategy. This would require a longitudinal research method that would test short and medium term results.

6 Discussion

The purpose of this research paper was to form a risk management strategy for Trulyprotect, a Cyber security company which is born global in nature and seeks to enter various markets. The Russian market was examined in this study from the perspective of enterprise risk management. Once the research questions were chosen, the literature review and research approach were selected, in this case a qualitative, exploratory approach was needed in order to discover the most relevant and up to date information to support a proper formation of a risk management strategy based on ISO 31000 risk management principles.

In the literature review I presented various definitions of risk and the specific one which was chosen for this paper. Later on different risk types were defined which assisted in diagnosing and categorizing the primary data in the analysis chapter. Afterwards, I defined the context through SWOT and PESTLE analysis to gain a better understanding of the business environment and objectives of the company in order to choose an appropriate risk treatment strategy following risk evaluation.

The most prevalent risk management strategy that was observed was mitigation. Thus, the overall recommendation for Trulyprotect is to attempt to achieve its objectives in the market through a thorough preparation and awareness of the changing environment in the Russian market. Despite the various risks that are present in the Russian market as implied in Figure 5, the majority of the risks are general business risks that startups face while internationalizing and might have the same level of loss exposure potential in other in countries.

Moreover, the business opportunities are currently appealing since the cost of doing business in Russia is low in comparison to European countries, the competition is rather low as Western companies are pulling out and the need for cyber security solutions such as Trulyprotect's is constantly on the rise.

The more unique risk types that are considered specific to Trulyprotect can be mitigated through outsourcing, awareness and preparation. Furthermore, Trulyprotect may choose to operate on a low risk entry mode via licensing or distributor agreements which will eliminate other possible risks that can have extreme damage over the overall operations of the company.

7 References

Advox.globalvoices 2016. *Russia Tightens Grip on Tech Infrasturcture Cuts Ties With US Firms*. Nov 11th 2016. https://advox.globalvoices.org/2016/11/11/russia-tightens-grip-on-tech-infrastructure-cuts-ties-with-us-firms/.

AIRMIC 2010. *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO.*

Andersson, S., 2004: Internationalization in different Industrial Contexts, *Journal of Business Venturing* 19, 6: 851–875.

Atradius 2016. *Market Monitor – ICT Industry – Russia.* June 16th 2016. https://atradius.fi/reports/market-monitor---ict-industry---russia.html

Brassington, F. & Pettit, S. 2000. Principle of Marketing. FT/ Prentice Hall.

Business Dictionary 2017. Exploratory Research. Accessed April 3rd 2017 http://www.businessdictionary.com/definition/exploratory-research.html.

Business Queensland 2016. *What is an information technology risk?* June 24th 2016. https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management/defined

Charur Astogi 2012. *6 international Marketing Market Selection Modes of Entry in International Markets.* slideshare.net/charurastogi/6-international-marketing-market-selection-modes-of-entry-in-international-markets

CNBC news 2016. *Trump Could Reset Russia Ties In Grand Bargain With Putin.* Dec 29th 2016. http://www.cnbc.com/2016/12/29/trump-could-reset-russia-ties-in-grand-bargain-with-putin.html.

DBP management 2014. *5 Ways To Manage Risk.* http://www.dbpmanagement.com/15/5-ways-to-manage-risk

Deloitte 2016. *Doing business in Russia*. Accessed April 10th 2017: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/tax/doing_business_inRussia_ENG_2016.pdf

Diffen 2017. *Franchising vs. Licensing.* Accessed April 11th 2017: http://www.diffen.com/difference/Franchising_vs_Licensing

Dorfman, M. S. & Cather, D. A. 2013. Introduction to Risk management and Insurance, Eastern Economy Edition. Pearson.

Ernst & Young Global Limited. 2010. Risk Appetite: The Strategic Balancing Act. Accessed April 5th 2017:

Fetterman, DM. 1998. Ethnography Step by Step (2nd Edition). Thousand Oaks, CA: Sage Publications.

FRCC (Finnish Russian Chamber of Commerce) 2016. *Information security booming in Russia*. 13.12.2016. http://www.svkk.fi/mahdollisuudet/business-opportunities/information-security-booming-in-russia/.

Furgchtgott-Rott, D. 2017. *Intellectual Property theft Biggest Crime US Economy*. The Fiscal Times. Jan 11th 2017: http://www.businessinsider.com/intellectual-property-theft-biggest-crimes-us-economy-2017-1?r=US&IR=T&IR=T

Gibson, S. 2017. *Risks Associated with Long Sales Cycle Selling*. Accessed April 3rd 2017: saleshq.monster.com/training/articles/1696-risks-associated-with-long-sales-cycle-selling.

Glassdoor 2017. *Moscow Developer Salary*. Accessed April 17th 2017: https://www.glassdoor.com/Salaries/moscow-developer-salary-SRCH_IL.0,6_IM1159_KO7,16.htm

Global CCS Institute 2017. Risk Assessment, process. Accessed April 3rd 2017: https://hub.globalccsinstitute.com/publications/strategic-analysis-global-status-carbon-capture-storage-report-5/72%C2%A0background.

Honkanen, M. & Mikluha, A. 1998. Successful management in Russia. Helsinki: International Assignments TT.

http://www.ey.com/GL/en/Services/Advisory/Risk-appetite--the-strategic-balancing-act.

Infosecurity Russia 2012. Blancco-s expansion into Russia coincides with European growth. Sep 20th 2012. http://eng.infosecurityrussia.ru/news/87260

Investopedia 2017a. *Specific Risk*. Accessed April 10th 2017: http://www.investopedia.com/terms/s/specificrisk.asp#ixzz4eLWUGtL8

Investopedia 2017b. *Systematic risk*. Accessed April 12th 2107: http://www.investopedia.com/terms/s/systematicrisk.asp

Irwin, R.D., 1969, Business Policy: Text and Cases. Homewood, IL.

ISO 2017. ISO Standards. Accessed April 3rd 2017: www.iso.org/standards.html

Jdsupra 2017. *IP, IT and mass communications. Major Russian legislation changes for 2016.* Jan 24th 2017. http://www.jdsupra.com/legalnews/ip-it-and-mass-communications-major-95146/

Kotler, A. 2016. *Why Do Most Cyber Security Startups Fail?* Jan 21st 2016. www.linkedin.com/pulse/why-do-most-cyber-security-startups-fail-amir-kotler

Litovkin, N. 2017. *Russia's Cyber Army Hacks a Spot in The Top 5*. RBTH. Jan 12th 2017. http://rbth.com/defence/2017/01/12/russias-cyber-army-hacks-a-spot-in-the-top-5_679221

Markowitz, H.M. 1952. Portfolio Selection, *Journal of finance*, 7 (1), 77-91.

Micromarketmonitor 2017. *Europe- Russia Cyber Security Market*. Accessed April 5th 2017: http://www.micromarketmonitor.com/market/europe-russia-cyber-security-6847423515.html

Moeller, R. 2011. COSO Enterprise Risk Management. 2nd Edition. New Jersey: John Wiley & Sons Inc.

OECD 2009. *Top Barriers and Drivers to SME Internationalisation*. Report by the OECD Working Party on SMEs and Entrepreneurship.

Pestelanalysis 2017. *What Is Pestle Analysis?* Accessed April 12th 2017: http://pestleanalysis.com/what-is-pestle-analysis/.

Rejda, G. E. 2008. Principles of Risk Management and Insurance.

Rouse, M., Moore, J. & Wigmore, I. 2017. *Distribution Agreement.* Searchitchannel. Accessed April 10th 2017: http://searchitchannel.techtarget.com/definition/distributor-agreement

saleshq.monster.com/training/articles/1696-risks-associated-with-long-sales-cycle-selling

Saunders, M. et al. 2009. Research Methods for Business Students, Pearson Education.

Saunders, M., Lewis, P. & Thornhill, A. 2012. Research Methods for Business Students. 6th edition. Pearson Education Limited.

Sciencedaily 2016. *Nations ranked on their vulnerability to cyber attacks. University of Maryland*. Mar 9th 2016: https://www.sciencedaily.com/releases/2016/03/160309125418.htm

Silvers, J. R. 2008. Risk Managment for Meetings and Events.

Soldatov, A. & Borogan, I. 2016. *Putin brings China's Great Firewall to Russia in cybersecurity pact.* Nov 29th 2016. https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact

SOTT 2017. *Trump adviser Scaramucci: Anti-Russian sanctions unsuccessful, united Russians around President Putin.* Jan 17th 2017. https://www.sott.net/article/339851-US-anti-Russia-sanctions-unsuccessful-united-Russians-around-President-Putin-Trumps-adviser-thinks-outside-the-box

Stoyan, T. 2012. Global from the Start: The Characteristics of Born-Global Firms in the Technology Sector. *Technology Innovation Management Review*.

SVKK 2017. *Information security Booming in Russia.* Dec 13th 2016. http://www.svkk.fi/uutishuone/liiketoimintamahdollisuudet_ja_myyntiliidit/information_security_booming_in_russia.28620.news

Van Teijlingen, E. 2014. Semi-structured interviews. Bournemouth University Graduate School. Dec 3rd 2014. https://intranetsp.bournemouth.ac.uk/documentsrep/PGR%20Workshop%20-%20Interviews%20Dec%202014.pdf

Walker R. 2013. Financial Engineering and Risk Management - Vol. 3: *Winning with Risk Management*. World Scientific: Singapore.

WIPO 2016. *Global Innovation Index 2016 – Winning with Global Innovation.* Johnson Cornell University. http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2016.pdf

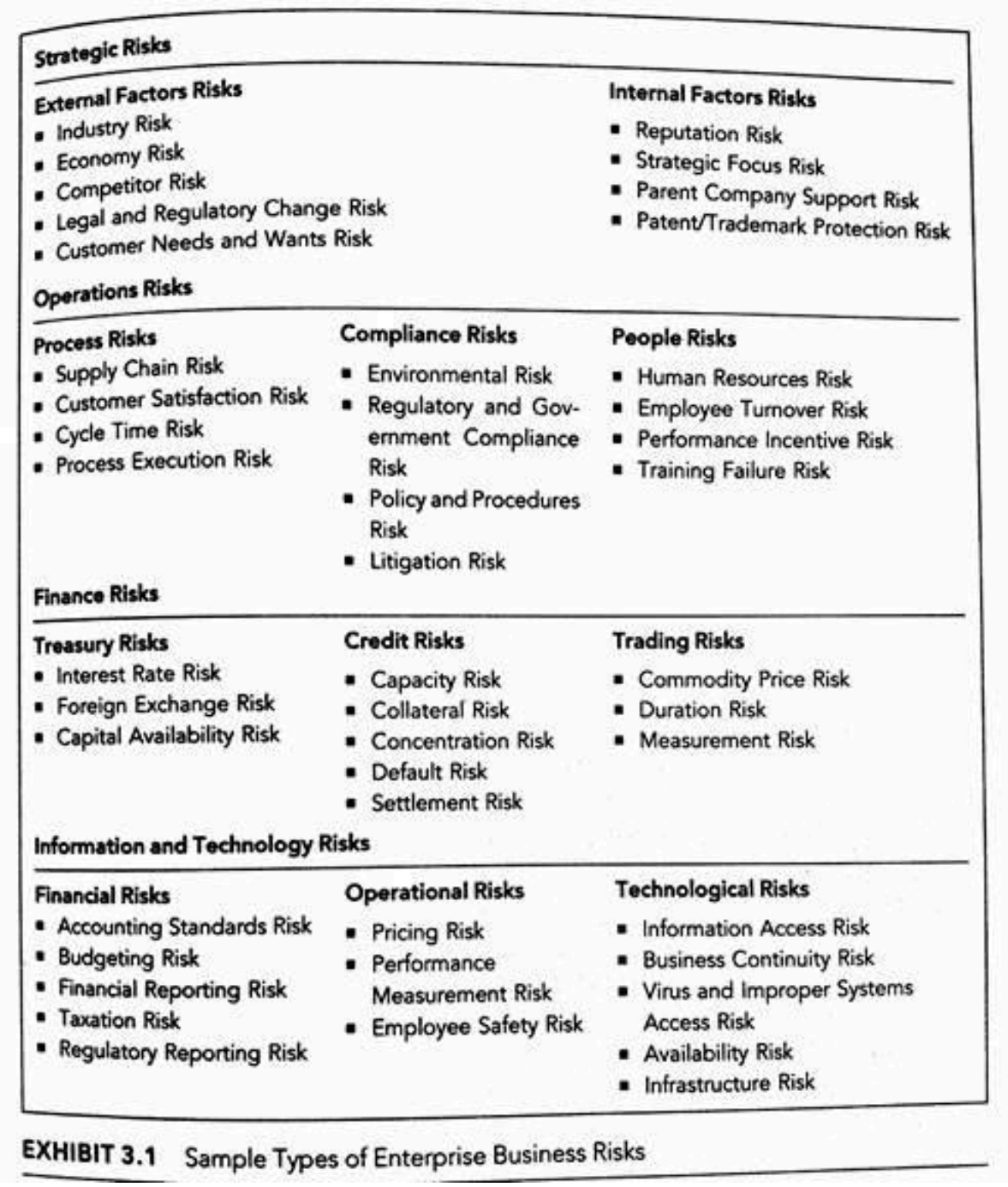
World Economic Forum 2016. *Things to Know about Russia's Economy*. Dec 2016. https://www.weforum.org/agenda/2016/12/things-to-know-about-russia-s-economy/.

Zerohedge 2017. *Russia Launches Biggest Arctic Military Expansion Since Fall Of USSR.* Jan 30th 2017. http://www.zerohedge.com/news/2017-01-30/russia-launches-biggest-arctic-military-expansion-fall-ussr.

8 Appendicies

Survey Questions

Risk types and Elements



Strategic Risks

External Factors Risks
- Industry Risk
- Economy Risk
- Competitor Risk
- Legal and Regulatory Change Risk
- Customer Needs and Wants Risk

Internal Factors Risks
- Reputation Risk
- Strategic Focus Risk
- Parent Company Support Risk
- Patent/Trademark Protection Risk

Operations Risks

Process Risks
- Supply Chain Risk
- Customer Satisfaction Risk
- Cycle Time Risk
- Process Execution Risk

Compliance Risks
- Environmental Risk
- Regulatory and Government Compliance Risk
- Policy and Procedures Risk
- Litigation Risk

People Risks
- Human Resources Risk
- Employee Turnover Risk
- Performance Incentive Risk
- Training Failure Risk

Finance Risks

Treasury Risks
- Interest Rate Risk
- Foreign Exchange Risk
- Capital Availability Risk

Credit Risks
- Capacity Risk
- Collateral Risk
- Concentration Risk
- Default Risk
- Settlement Risk

Trading Risks
- Commodity Price Risk
- Duration Risk
- Measurement Risk

Information and Technology Risks

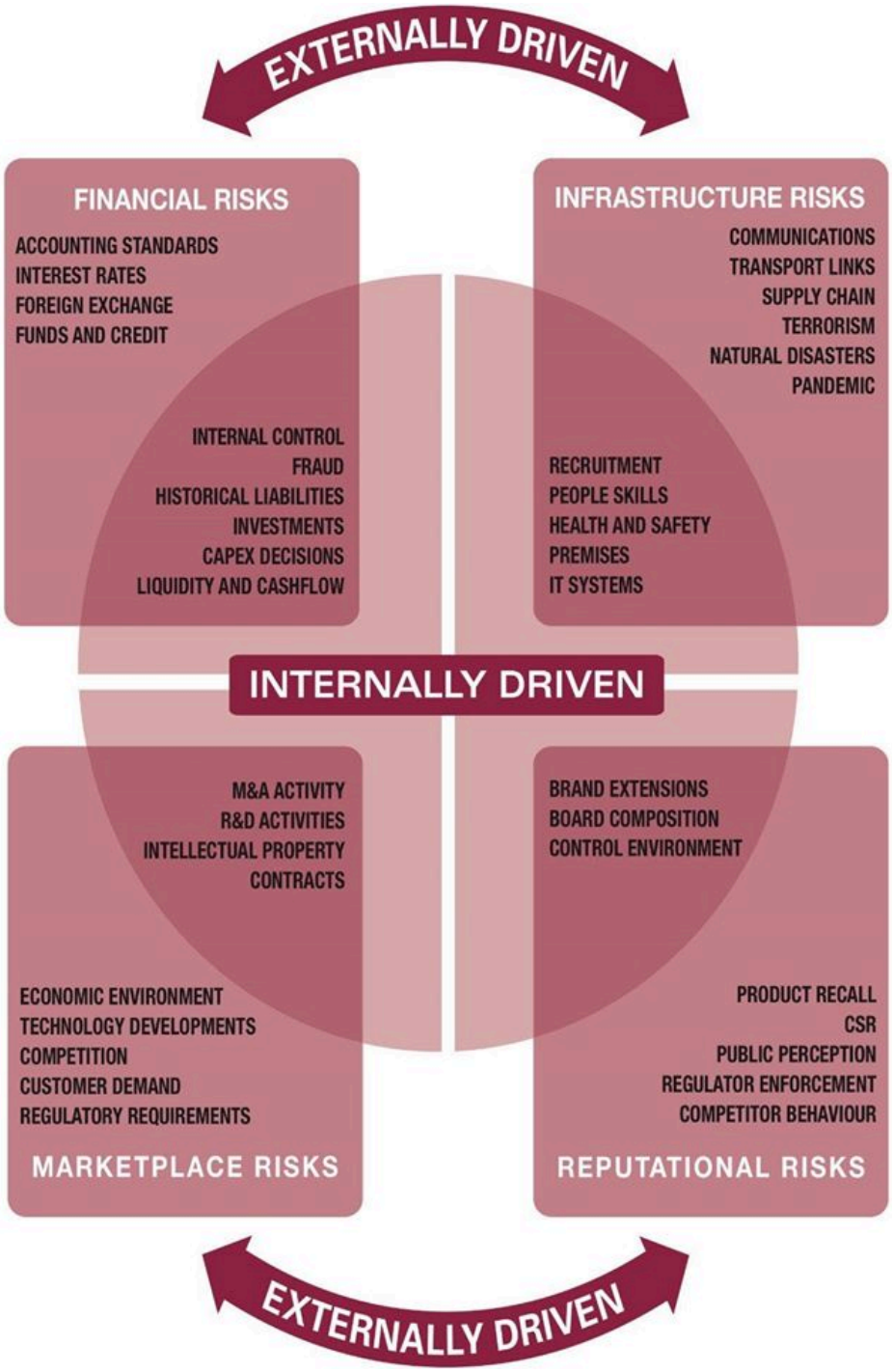
Financial Risks
- Accounting Standards Risk
- Budgeting Risk
- Financial Reporting Risk
- Taxation Risk
- Regulatory Reporting Risk

Operational Risks
- Pricing Risk
- Performance Measurement Risk
- Employee Safety Risk

Technological Risks
- Information Access Risk
- Business Continuity Risk
- Virus and Improper Systems Access Risk
- Availability Risk
- Infrastructure Risk

EXHIBIT 3.1 Sample Types of Enterprise Business Risks

(Moeller 2011, 35)



Drivers of Risk Management - AIRMIC, 2010, A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO, P.14