Information Security

Developing an Information Security Strategy

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Armin Kraus, BSc

is161518

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Dr. Simon Tjoa

Mitwirkung:

St. Pölten, May 26, 2018

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

*

Fachhochschule St. Pölten GmbH, Matthias Corvinus-Straße 15, A-3100 St. Pölten,T: +43 (2742) 313 228, F: +43 (2742) 313 228-339, E:office@fhstp.ac.at, I:www.fhstp.ac.at

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Abstract

This master thesis addresses the topic of information security, more specific, how to develop an information security strategy. An information security strategy is the commitment of the management related to information security. This commitment is the official order to establish security within the company. One of the most frequently asked question after this commitment is; How to develop such a strategy? This research is exactly focused on this question and makes use of existing business models / corporate strategy development models / business development tools. Current existing methodologies such as SWOT analysis, Business Model Canvas, Ansoff matrix, Boston Consulting Group matrix, McKinsey 7S model and stakeholder analysis will be analyzed and adapted for information security strategy development. The modification of these models allows the identification of corporate information security objectives and their impact on the company. This identification will be enabled through different analysis methodologies which cover risk based, stakeholder based and vision based approaches. In addition, these models can also be used as technical base analysis, specific risk mitigation, risk mitigation in relation to business objectives or impact analysis. Further, a 'checklist' will be provided what should be at least in an information security strategy. This research also contains practical examples for these adapted models, an example information security strategy and a comparison of these developed models. These information's can be used by anyone to form an information security strategy related to their own corporation.

Contents

1. Introduction

Do you know who has information stored about you and how much? Today we live in a high technological constantly changing environment of information. Hundreds of years information transmission was restricted to spoken words and written books. It was relatively easy to keep information under coverage and control access. With the introduction of telegraph 1837 a third way of communication was established [1]. 80 years later, information can be transmitted over the internet, stored on every place around the world in multiple locations synchronously on systems where you don't have any idea about it. As the way information can appear changed, also threats to protect the information are different. There are various paths where information flows, be processed and stored. Information Technology (IT) offers organizations multiple ways to access corporate information everywhere. These features are really welcome and decision makers hopes to increase productivity and decrease costs. Regardless where information appears, it always requires an appropriate level of protection. Due to the continuous hazard of an information leakage, organizations have to define how to treat and handle information. Especially with the mixture of onsite services and public services, information security will be a challenge. To get rid of the whole technical possibilities and abstract paper is necessary where the organization can place his statement regarding to information security. This will be written down on a paper called, information security strategy (ISS). This research focus on the creation of an information security strategy. It describes which parts should be used in a strategy and what is their purpose. Existing business development methodologies would be analyzed and adopted to increase their support regarding usability to discover strategic objectives. Examples would be shown to use methodologies and their results. Pohlmann and Reimer [2, p. 1] identified two strategy types; (1) information security strategies that focuses on the CIA triad and (2) cyber security strategies which has a broader influence on objectives. This research are focused on the first type extended by Parkers parkesian hexad [3, pp. 12].

1.1. Research Problem

The history of strategic development has been evolved in the last 25 years [4, pp. 3]. Organizations had to learn how to analyze their current situation, identify their position, and create competitive advantages.

A lot of various approaches where tested to master the dynamic environment of competition. The experience from these tests resulted in recommendation how corporate strategies should be defined. The basis for a strategy is a business model. Business Models defines how a company should operate and how value can be achieved. A common definition of a business model is from Magretta, he defined it the following way: "stories that explain how enterprises work" [5]. As an essential part of developing strategies, business models support you by identifying key problems and gives you a baseline. Depending on the method, it supports organizations to determine their situation and allows conclusions about future events. Literature shows that most methodologies are designed for managing business strategies. Business models or methodologies for developing information security strategies are rare. The main objective of this research is to analyze current existing business models/business development methodologies and adopt their behavior to enable a development of an information security strategy. The research does not take care about any life-cycle approach or continuous development.
With the limited existence of methodologies about information security strategy development, this research is focused on two main questions:

- How can an information security strategy be developed using existing business models and development methodologies?
- Which components are required for an adequate information security strategy ?

1.2. Structure of Work

This research can be divided into six parts:

- **Information Security Strategy** – This chapter cover up the topics why an ISS is required and what is the purpose of a strategy. Further the needs will be demonstrated and what are common pitfalls during development process.
- **Building Blocks** – This chapter introduce which parts should be part of an ISS. It explains the most common elements of a strategy and how they should be defined.
- **Methodologies** – This chapter shows how existing business development methods can be used in an adapted way for developing of an information security strategy. Methods will be introduced and examined of their capabilities.
- **Sample Cases** – An example company has been defined and will be evaluated against adapted methodologies which are defined in prior chapters. This chapter demonstrates an exemplary application of the methods.

- **Example Information Security Strategy** – In this chapter an example ISS will be provided and analyzed. The strategy contain all identified building blocks. The strategy shows a possibility how an strategy can look like. The sample strategy is based on the YLM Ltd. described in chapter 5.1.
- **Conclusion** - The last chapter will give an short overview about developed methodologies, example use cases and opportunities. It summarizes the essential parts of these master thesis and merge it into an applicable picture.

2. Information Security Strategy

This chapter explains what is information security and why is it necessary. Further it shows which advantages can be genereated from these information. It will be described what an ISS is and why one is needed. In the last section an overview about common pitfalls will be provided.

2.1. What is Information Security

Information is a fundamental asset in organizations. Nowadays this is more important than ever, regarding to interconnected business activities that increase every year. Information occurs in many different forms. It can be spoken in a spoken conversation, shown on a film, stored electronically, transmitted by post or obviously printed or written on paper. It doesn't matter how information occurs, it has always to be appropriately protected [6, p. viii]. Employees, contractors and third-party users are creating and processing information within business processes. Information is created by users, used in business processes, flown through applications and tools which are reside on IT infrastructure (shown in figure 2.1) [2, p. 12].

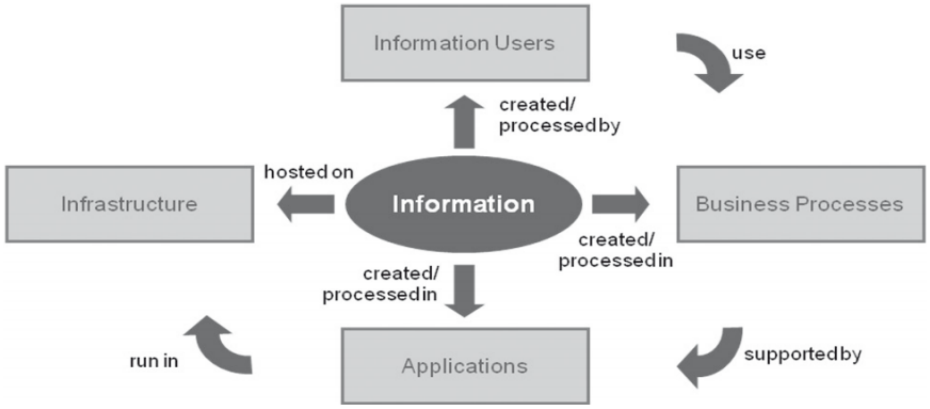

Figure 2.1.: Information Processing Life Cycle [2, p. 12]

Information security will work as a business enabler, bounded to the trust of the stakeholder. It addresses business risks or generates additional values for an enterprise. Competitive advantage or legal compliance

can be one of these values. Information is a significant increasing aspect of business and requires and adequate level of protection regarding to ever-changing threats [7, p. 28].

"Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities." [6, p. viii]

The key objectives of information security are the CIA triad. This triad will be extended by in the definition of Parkerian Hexad.

- **Confidentially** – "which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information" [8, p. 153]
- **Control/Possession** – "a state of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or Controlled" [3, p. 16]
- **Integrity** – "which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity" [8, p. 153]
- **Authenticity** - "Authenticity refers to the assurance that a message, transaction, or other exchange of information is from the source it claims to be from" [9, p. 15]
- **Availability** – "which means ensuring timely and reliable access to and use of information." [8, p. 153]
- **Utility** – "useful, fitness for some purpose". Information can be available but aren't usable (e.g. encrypted data). Information shall be useable [3, p. 17].

Further and more specific objectives of information security are:

- **Transparency**

  "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used." [10, p. 58]

  "The principles of ... transparent processing require that the data subject be informed of the existence of the processing operation and its purposes." [10, p. 60]

- **Non-Linkability**

  "... non-linkabiliy means that an observer cannot distinguish if two valid signatures for the same signing policy have been computer by the same user." [11, p. 230]

- **Privacy**

  "... privacy is control over when and by whom the various parts of us can be sensed by others." [12, p. 281]

2.2. Purpose of Information Security?

Information security protects the six key objectives of information and emphasize the protection of intellectual property and digital identity. Information security deal with a system of measures taken to protect information, information systems and data from unauthorized use or disruption. Information security is a continuous process that creates policies, procedures and strategies in organizations to resist any disruption [7, p. 28] [13, p. viii]. Information security supports important business assets, an improvement of information security can help to increase cash flow, profitability, legal compliance, and commercial image. Information systems of companies have to deal with a lot of security threats such as computer-assisted fraud, espionage, sabotage, vandalism, fire, or flood. There is an increasing number of computer hacking, malicious code and denial of service attacks. It is necessary to handle information security to protect critical infrastructures, regardless if public or private sector. The fusion of public and private networks makes it difficult enforce access controls. The 'access data everywhere'-trend requires a rethinking of what should and how should it be protected. Further the distributed computing has weakened the possibilities of control mechanism. It is often the case that information systems are not designed to be secure. Security has to be achieved via appropriate management support and technical limitations. As a minimum, information security requires a participation of all employees in the whole company. Information security further requires an aid of suppliers, shareholders, customers, third parties or other external parties [6, p. viii]. Information Security can be described like a relationship between the users with business requirements and the ability to access information. Information security is the 'gate' in this relationship which defines specific paths to this information. The information can only be accessed via this, hopefully secured, paths [14, p. 1089].

2.3. What is Information Worth?

Expenses related to IT has heavily increased over the last 20 years. A lot of these investment was to acquire additional hard and software that allows the gathering, processing and storage of data. This leads into a giant data leaks which have to be analyzed and frustrate user. The amount of data, regardless if structured of unstructured, grows continuously, therefore costs for storage and compute power increased. Simultaneously the requirements for compliance and data security also increased. IT in the past was

usually treated as utility with less importance for competitive advantage. There is a movement from IT as utility to information processing organizations, this requires tools such as business intelligence (BI) software. During the last 5 years, BI is on the top of the list of IT priorities (Gartner's CIO survey Oct. 2017 [15]). BI act as business relationship between IT and business. The requirement for an adequate analysis of information assets to provide knowledge to the decision-makers constantly increase. Deeper knowledge about all circumstances allow more precisely decisions and reduce wrong steps. Capgemeini (The Information Opportunity 2008 [16]) already discovered 2008 that in 80% of surveyed organizations raised information to the top-3 corporate priorities. For example; In cases where organizations only want to decrease costs, information about which amounts are invested or more generally; Where does the money flows? Decisions are based on the level of available information assets [17, p. 4].
Information is increasingly becoming the substance of our capitalist world that is affecting the paths of many companies [18, pp. 590]. The key word for set a worth to an information is: Infonomic. Deloitte define it as "The economics of information and principles of information asset management" [18, p. 591]. Companies in the world discover that information is a key asset. Focusing on information instead of technology helps organizations to extend the capabilities of IT and boost corporate performance. To unlock the full potential of information assets, account, rate and optimize it. This step requires knowledge about how information is created and affect corporate values. The finance department have the ideal position for accounting information, so it can act as keeper for corporate values and allows to move forward in an information era [17, p. 3].

2.3.1. Why do we take care about Information Assets?

Information Reduce Costs

Cost reduction is one of the main reason for information asset management. The following examples illustrate how expenditure can be reduced using information assets [19, pp. 5].

- The State New York saved approximately $9 million per year due to a new developed concrete mixture. The mixture was developed on the basis of a literature analysis.
- Texas Instruments determined a 515 percent return on investment after creating a library service.
- A US manufacturer figured out that the information created by literature researches which used corporate library was worth about $400,000 and the company invested only $17,000.

Table 2.1 shows the Benefit-Cost Ratio of internal information services:

Georgia Technical Institute	16 to 1
Exxon	11 to 1
Minnesota DOT	9-10 to 1
NASA	7.6 to 1
Paccar, Inc.	3 to 1

Table 2.1.: Benefit/Cost Ratio for Information Services [19, p. 6]

Information Save Time

Precise information can save time in different ways – stop unnecessary tasks, avoid pointless meeting, or adjusting inaccurate information.

- A survey conducted by Griffiths and Kind with 27.000 professionals in an time period of eleven years about the usage of information shows the result in table 2.2. This table indicates which type of information sources saved time in percentage value.

Information Source	**% Yielding Time Savings**
Journal articles	26 percent
Books	42 percent
Internal reports	50 percent

Table 2.2.: Information Sources and Time Savings [19, p. 6]

- Paccar, Inc. created a task force to reduce the amount of time for vehicle analysis that were on the test track. The results were published on corporate intranet within 6 days instead of multiple month. This leads into a significant boost during development phase.
- A reduction from 10 to 1 working days was accomplished by another corporate library. It was possible to develop a way which performs former external cost calculation functions internally.
- Parsons-Brinckerhoff was able to develop a corporate knowledge base to share data and information. This enabled a timely placement of specialized personal within organization.

Information Improves Decision Making

Organizations within a decentralized environment have to rely on their Information. It is essential that these information is of high quality, trustable and up-to-date when it comes to a management decision. The following examples convey an idea how important information is for decision-makers:

- A survey of Griffiths and King's examined the relationship between quality of work and information. Table 2.3 (1=low, 7=high) illustrates rated their work performance with and without specific information.

	Journals	**Books**	**Internal Reports**
With Information	5.82	5.68	5.78
Without Information	4.04	3.57	3.52

Table 2.3.: Information and Quality of Work [19, p. 7]

- A survey conducted by Marshall in 1993 of banking managers revealed that 84% of managers agree that provided information by their company's makes the decisions better. In cases of financial decisions, three-quarters of all surveyed mangers estimate the value of information more that $1 million.

2.4. What is an Information Security Strategy?

Information security strategy is a way to establish objectives of information security in a organization. It is an approach which uses defensive information security technologies and place measures in an coordinated way to defense organization's information infrastructure against internal and external threats. Further it offers paths to increase confidentiality, integrity and availability [20, p. 27]. Information security strategy should agree with general recognized principles withing organization. The design should be aligned to the organizational structure and business requirements, be complete and contains all necessary information to be actionable. Not everyone should have access to information security strategy, only to those people who require access [21, p. 186]. Costs are a not negligible part of each strategy, implementation and maintenance have to be cost effective. Further, ISS have to be fully integrated into organizational structure and processes to achieve compliance to your strategy [20, p. 29]. Before an developement of an information security strategy, it is important that you are familiar with your information security infrastructure. What are your critical assets? Which assets require more protection that others? Which threats and vulnerabilities exist? These questions can be answered through a well-established risk management. Risk management allows system owners to protect their information regarding their level of relevance. Due to the fact that risks can never be reduced to zero and your company have limited resources, it is rather important that your organization manage this scare resources regarding their risk level [22, p. 6]. Information security strategy and risk management are two heavily interwoven topics. Pironti [23, p. 1] is telling us that risk management and information security provides organizations a

path to reach business goals aligned on risk profiles. Information security and risk management (ISRM) are IT functions and are part of organizations IT strategic planning.

2.5. The need for a Strategy

Organizations and governments have become more dependent on computer-based information systems. Organizations heavy rely on IT. IT support different services and business critical application. This massively increase IT complexity and constantly changing information security threats. Information is nowadays easier to publish and to access around the world. The result: Information security become a mission-critical function [13, p. 15] [24, p. 2]. Information, as a business asset, requires an adequate strategy for protection. Wrong handling of information security can lead into dramatic press reports. Presses around the world publish reports of billions of Euro lost regarding to security weaknesses and information disclosure [25, p. 1]. (see Appendix A)

"If information security is permanent ignored by top managers, the result will be that organizations systems are not as secure as might necessary. Security breaches will occur more often and the damage will be having more impact." [26, p. 441-469]

To increase the level of protection for information, organizations have to be aware of their information and the importance for their selves [25, p. 1]. An ISS forces the importance level in the internal organization for information security and define a statement in what your company believes in and what are the goals to protect information. There is not always a clear defined way for every objective you have. May even the objective be more an estimation. Sometimes you may have an approximate idea where the journey will end. The objective will be more clearly as long you keep running. Finding the ideal information security strategy will be an equal experience. First drafts will be incomplete and not covering every aspect, but after some time it will reveal its inaccuracy. Defining the ideal target situation will not be possible for a lot of organizations. They may can only exhibit improvements for the current situation, but these improvements can be used to realize short term goals [27, p. 109].

"The information security strategy is the roadmap for the foreseeable future details how the organization intends to progress along the path of maturity ..." [27, p. 110]

The strategy provides an environment for improvements and ensure that the organization keep focused on the most important functions. This can only be achieved if the organization controls every aspect related to information security [27, p. 110]. Is a strategic plan still appropriate in a dynamic changing technical environment? Yes, only a strategic plan can determine where you are and where you want to

be in the next years. This is also true if it comes to information security strategy. A clear defined strategy enables management, executives and employees to see where they want to be. It also allows to check if the company is on the right way and if goals are already accomplished. A lot of organizations lack of information security strategic plans, or a plans are in place but outdated. A result would be that there is no focus on information security topics unless something very bad happens [28].

"You can't fight today's threats with yesterday's strategies" [29, p. 1]

Risk in relation to information security has evolved and changed, information security strategies could not keep up. The result will be that organizations rely on outdated strategies in a largely battle against well trained offenders [29, p. 1]. Security incidents reported from federal agencies (table 2.4) increased from 2013 to 2015 up to 10 percentage.

Reporting Source	**2013 Total Number of Incident Reports**	**2014 Total Number of Incident Reports**	**2015 Total Number of Incident Reports**
CFO Act Agencies	57,971	67,196	75,087
Non-CFO Act Agencies	2,782	2,655	2,096
Total Federal Incidents	**60,753**	**69,851**	**77,183**

Table 2.4.: Federal Agency Security Incidents [30, p. 14]

2.6. Common Pitfalls and Challenges during Development of a Information Security Strategy

History is littered with examples of bad strategies. After decades of development of business strategies, fails still remain. Some strategies plans that are based on greed and malfeasance are obvious wrong. Other failed strategies are not so easily determine why these are unsuccessful. Research has shown some main reasons for strategic failures [31, pp. 48]:

Overconfidence

Analysis shows that people inclined to make concrete prediction instead of defining wide open objectives. These predictions are often wrong. Further people who create statements tend to be overconfident of their own abilities.

Optimism

In general, decision makers are tending to be optimistic regarding to their forecasts. Too optimistic estimations became unrealistic and can have impact on strategic based decisions.

Anchoring

Some presented key numbers will anchor on the listener. The listener tries every time to refer to these special numbers, regardless if they are correct/irrelevant or not. Anchored thoughts are barriers for developing new strategies.

The Status Quo Bias

There is a strong tendency for people to related decisions and approaches in the past. It doesn't matter if they were successful or not. 'As we always do'-Mentality and not mind opened. It is impossible to pursue new ways if you only deal with approaches that you've learned in the past.

Mental Accounting

Treat capital different regarding to their incomes/outgoings. So that means, investment is every time the same, regardless where it goes.

The Herding Instinct

People rely on confirmation and comparisons to others. It is necessary to walk its own way that meets to the requirement of the organization. This also has a drawback side. Because it is bad to make a mistake in a strategic plan, but it is catastrophic if you are the only one who made this in your industry.

False Consensus

Decision makers tend to overestimate the extent. During developing phase, wrong estimations and ignored threats can result in an impractical strategy.

C-Suite Support

It is necessary that every leadership is informed and support strategies. Strategies with less or none support of senior-level sponsorship will not or only partial executed on lower levels. C-suite executives should identify required steps to support strategic relevant key initiatives [32, pp. 3].

Resources

To reach strategic goals often additional specialists are required. A lack of skills or needed personnel can

peril strategic objectives. Top management have to identify additionally required resources and provide fully support [32, pp. 3].

Review of Strategic Objectives

Strategies are not sculpted into stone. Circumstances, markets and companies are changing. It is a requirement to review your goals and prove if they are still valid [32, pp. 3].

Start Initiatives/Projects to Achieve Strategic Goals

Strategic goals are decisions how the company will place themselves on the future markets. This usually cannot be achieved with one project. Reasonable steps have to be set on key competences of the business to move forward into the planned direction.

Communication

C-suite executive shall communicate to leadership the importance of the strategy and explain the drivers which fulfill the requirements to achieve the strategic goals. C-suite should delegate day-to-day aspects of projects or initiatives to leadership and only provide top-down support. Leadership are own more detailed understanding because they are closer to business [32, p. 9].

Say no

A strategy defines the way how the goals can be achieved. No organization is possible to do all, may useful, steps. The difference between a good and a bad strategy is to say yes to some specific actions and say no to everything else. It happened too often in the past that management are not able to define granular statements that leave no room for different interpretation [33].

No initiatives defined

It is often the case that objectives are defined that should improve the business and afterword's, nothing is happening. Management walk back to their desks and process with their current situation. Without strategic initiatives, strategy is senseless. Required steps that will push the business into the desired path shall be identified and defined [33].

Inaccurate strategic initiatives

- Promote a culture of accountability.
- Do not work harder, work smarter.
- Associates have to be appreciated.

Such steps are sometimes defined as strategic initiatives, but they will fail. A well described strategic initiative will enable each manager to know at each point to know what to do. Strategic objectives will never be accomplished if managers do not exactly know what to do [33].

Systematic Approach for an Information Security Strategy Development

Strategic planning is a relict of 1960s, where it was published as 'the one and only way' for managing corporations. Since 1960, strategic planning has changed due to the fact that it is not infallible. Mintzberg [34, p. 1] explained that "strategic planning is not strategic thinking", but this is often misunderstood. Managers should come back to the point where they capture data and learn it from various sources. Afterwards these data should be synthesized to form a path where the business moves forward.
Further Mitzberger define strategic planning as "formalized procedure to produce articulated result, in the form of an integrated system of decisions. In other words, planning is about formalization, which means the decomposition of a process into clearly articulated steps. Planning is thus associated with 'rational' analysis." [35, p. 13] Strategic planning is still a tool which can support business in a changing environment. These planning process can allow predictions about future interruptions and help organization to determine their vision and objectives [36, p. 953]. There are various papers of how strategic planning should be conducted. Organizations use planning tools as baseline for strategy development. Such tools or methodologies provide a step by step manuals which enable the most coverage of business values. These discovered values flow into new strategys. An information security strategy requires equal methodologies where decisions makers are able develop an appropriate strategy. The lack of such tools results into inaccurate and incorrect strategies.

3. Building Blocks of an Information Security Strategy

These chapter countains all relvant information about what should be included in a information security strategy. These parts are called buildings blocks. A building block is one element of a strategy. A strategy should contain at least at mission and vision statement, a part for governance, strategic objectives and initiatives, threats which can have impacts to objectives, measurement methods and values.

3.1. Mission

Mission statement should explain who is the company and what it does. It includes scope of the company and differ it from similar one. But there can is also more; Mission statement is referred as a 'credo', 'philosophy' or company's 'core values'. Mission statement can also be a justification of company's being. It can be defined as a precursor to realistic and clear business objectives. Business concerns mission statements should address interests of shareholder, employees, management and these parts of the world which are business relevant[37, p. 2]. Pearce and David [38, p. 1][39, p. 73] identified eight components that should be included in mission statement:

1. Definition of target customers
2. Identification of offers
3. Definition of geographic areas
4. Recognition of main technologies
5. Engagement to survival, growth and profitability
6. Definition of key elements in enterprises philosophy
7. Recognition of the enterprise self-concept
8. Recognition of the company's desired public image

John Hall [40] points out that in the last 20 years mission statements are turned into bad default messages. Mission statements are often filled with useless keywords and phrases. Sometimes mission statements meet the requirement of an 'about us' page. Len Sherman [41] asked manager the question how vision, missions and value statements affect their daily work. The answers were almost the same, 'little bit' or more worse 'which mission statement?'. On the other hand, Alawneh [39, p. 73] referred to actual studies that 84 percentage of managers rely on mission statements as an essential management tool. Mission and value statements where highly respected as top management tools which establish a corporation of employees in the same direction.

Example mission statements:

- "The world's leading provider of premium products and premium services for individual mobility." – BMW
- "To connect people with their world, everywhere they live and work, and do it better than anyone else." - AT&T
- "We strive to be the global leader in the sporting goods industry with brands built on a passion for sports and a sporting lifestyle!" - Adidas
- "We seek to be Earth's most customer-centric company for four primary customer sets: consumers, sellers, enterprises, and content creators." - Amazon
- "To refresh the world; to inspire moments of optimism and happiness; to create value and make a difference." - Coca-Cola

3.2. Vision

The vision statement delivers an impression how your organization should look like in the long-term future. It is a condition where your company should ideally be. Vision contains the hopes and dreams of the organization and is an inspiration for future decisions. It does not tell you how you can accomplish your vision, it set the direction for strategic planning [42, p. 2]. Writers of business strategies and leadership writers have suggested that a vision statement should contain some commonly shared properties:

1. "conciseness;
2. clarity;
3. future orientation;

4. stability;
5. challenge;
6. abstractness; and
7. desirability or ability to inspire." [43, p. 2]

A test of the University of Technology in Sidney discovered that 70 percentage of organizations employees does not know their vision statement [44]. The cause of this problem is that vision developers work in ambiguous organization, with ambiguous people which deal with complex problems – therefore they design an sophisticated vision statement. One golden rule for developing a vision statement is: Developing a statement is complex, understanding a statement shouldn't.
A vision statement should be able to answer the following questions [45][43, p. 2]:

1. Does your vision statement describe what you actually do?

   If yes, then you have to redesign your statement. The vision statement is not a possibility to describe your organization operations and activities in an particular language. It is focused to describe the business outcome. Organizations often explain to detailed who they are and what they are doing instead of what is the result if the work is finished.

2. Is it simple?

   Or is it sophisticated and complex? Are all simple descriptions are gone? If that is true, cancel it. There is a relationship between your keywords and the clearness of your vision. Less words being more powerful in that case.

3. Is it explainable?

   Is it possible to explain this vision to someone who are not part of your company? It should be. It is an obvious advantage that employees who understand the vision can make it real. Further important is the impression that the vision statement tells everybody who read it.

4. Wait one day

   If you are confident that your vision statement fulfills all aspects, wait one day, and evaluate it tomorrow. If you still think next day that it is great, you are on the right way.

Example vision statements

- "To be the most successful premium manufacturer in the industry" - BMW

- “Our vision is to create a better every-day life for many people.” – IKEA
- “Bring inspiration and innovation to every athlete* in the world. (*If you have a body, you are an athlete.)” – Nike
- “To be the best quick service restaurant experience. Being the best means providing outstanding quality, service, cleanliness, and value, so that we make every customer in every restaurant smile.” – McDonald’s
- “To be Earth’s most customer-centric company, where customers can find and discover anything they might want to buy online.” - Amazon

3.3. Governance

"Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly." [46, p. 12]

In other words, information security governance is the responsibility of the decision makers regarding to information security. Governance must be an essential and visible part for management. Management must have a clear expectation about what Information Security will deliver to their organization and how security collaborate with strategy and objectives. The outcome of information security governance should be an alignment of information security strategy with business strategy which include the support of business objectives [46, p. 12]. The board of directors and executive management have the responsibility for information security governance. Information security governance should be a relevant part of enterprise governance. Information security governance is significant growing, cause their dependence on information importance. Most organizations strongly depend on their information assets and business continuation without is not possible. The handling of such information has a direct effect on business output. This dependency of businesses regarding to their information, and systems that handle this information, have pushed information security governance as a critical aspect of global governance. Governance can provide fundamental benefits:

- Comply with policies
- Critical decisions are based on adequate information
- Enhanced customer relationships

- Protection of enterprise reputation
- Improve electronic communication

Due to the fact that new technologies can provide essential improvements on business performance, optimal information security can contribute important values to the enterprise [31, p. 31].

3.4. Strategic Objective

Strategic objectives represent the goals that should be achieved. These objectives will be discovered and determined through strategic methodologies. Definition should be as simple as possible to ensure that it is easy to understand. Further ambiguous and unspecific phrases should be avoided. Definition of strategic objective shall be SMART Specific targets should be defined for improvementsc(Specific). Objectives have to be measurable or require an additional definition of possible ways to measure the status. Immeasurable strategic objectives cannot be assessed and consequently not be controlled (Measurable). Top management have to provide adequate human resources for managing, fulfillment and tracking strategic objectives (Assignable). Surreal objectives that never can be reached will not be supported by c-suite or staff (see section 2.6). Goals have to be reachable in an appropriate period of time (Realistic, Time-related) [47, p. 36].

3.5. Strategic Initiatives

"A Strategic Initiative is an investment of resources dedicated to accomplish an organizational objective" [48]

Strategic initiatives are investments which contain budget, scope and start/end date to support strategic objectives. These initiatives close the gap between current situation and defined strategic objectives. It should provide a way forward from the current situation [48].

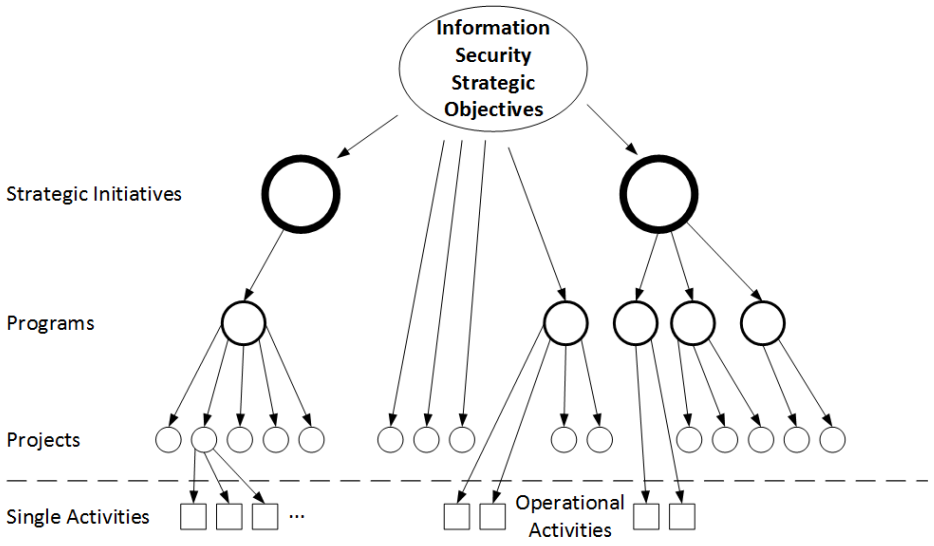

Figure 3.1.: Strategic Initiatives [49]

Strategic initiatives (3.1) trigger programs and/or projects which will result in tasks. The greater the initiative, the more increase the size of programs and projects. Programs have to be managed and monitored against defined performance measures. Managers have to be familiar with initiatives which allow them to recognize how their projects support strategic objectives.

3.6. Threats and Vulnerabilities

Information security strategic objectives are almost not a small project that can be accomplished in one year. It consists of a lot of projects that mesh together in a complex environment. Threats and Vulnerabilities regarding to objectives should be identified during strategy development to be able to track them. Threats can have different emphasis; Loss of knowledge, resource bottlenecks, unavailable partners, change of business strategy, compliance regulation or changed threat situation [50]. Threat catalogues can be used to identify threats and vulnerability on the way to strategic objectives. A threat catalogue is a summary of threats which enables creation of controls to detect them. The most common catalogues are:

- **BSI – Elementary Threats**

  Handles various threats from natural disasters, information manipulation to absence of personnel. [1]

- **NISTIR 8144 - Assessing Threats to Mobile Devices & Infrastructure (draft)**

[1] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats

Deals with risks especially in the field of mobile devices. It covers wireless technologies such Bluetooth, WiFi, Near Field Communication (NFC), Application Stores, Enterprise Mobility Management (EMM) solutions and mobile services. [2]

- **NIST 800-30 - Guide for Conducting Risk Assessments**
  Offer a list of approximately 100 threat event over various areas. [3]

- **ENISA - Threat Taxonomy**
  Provide a list of threats which is able to cover abuse, loss/damage of IT assets, eavesdropping, legal aspects, outages, malfunctions, physical attacks and unintentional damages. [4]

- **ISO 27005 - Information security risk management**
  Deliver a list of approximately 50 most common threats. [5]

Usually threats are bounded on a condition in the environment. Threats are substantial changes of external environment that can have significant negative effect on strategic objectives.

3.7. Performance Measures

Measurement of progress of a strategy is a requirement for setting actions and to know to be on plan. Defining adequate attributes that allows to evaluate the current status of a strategy would lead into a better controllable strategy process. Performance measurement can take many forms, but one feature is to present managers financial and non financial measures that covers different perspectives which provide a translation of strategy into performance measures. Performance attributes should be set to allow financial measures regarding to short-term consequences of managers decisions. Enable to supplement financial measures with non financial measures and attributes should be designed to fulfill multiple purposes. From cost determination to enable value creation [51, p. 2]. Strategic Performance Measurement (SPM) can help organizations to achieve their strategic objectives. Studies has shown that appropriate measurement have benefits in reviewing and formulation strategies [52, p. 1].

[2] https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[4] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

[5] https://www.iso.org/standard/56742.html

3.8. Values

Values are qualities of the organization that are considered as important. These values represent the key priorities and drivers for what they do. These values define how the behavior looks like within the organization. This statement should tell how value will added to stakeholders, vendors, customers, and employees. The values act as a description of the corporate culture [42, p. 2].

4. Methodologies for Strategy Developement

In this chapter methodologies will be introduced which are designed for creating an ISS. These methods are based on existing business developemnt models like swot analysis, business model canvas, ansoff matrix, boston consulting group matrix, McKinsey 7S model and stakeholder anlysis. New models, focused on information security, have been developed using these methods. Furthermore, instructions for the ussage of these models will be provided.

4.1. SWOT Analysis for Information Security

SWOT stands for Strengths, Weaknesses, Opportunities and Threats (table 4.1) [53, pp. 3]. SWOT analysis is a straight forward approach for generation strategic decisions from situation analysis. It allows to discover strengths, weaknesses, opportunities and threats for your company and business [54, p. 2]. After identifying these factors strategies can be developed that are based on strengths, able to eliminate the weaknesses, use opportunities or mitigate threats [55, p. 2]. Strengths and weaknesses are covered up by internal analysis, opportunities and threats by external analysis of an organization [53, pp. 3]. Internal analysis examines every aspect which are controllable, for example: Employees, production plants, sites, products, resources, capabilities, services and core competences. External analysis deal with aspects which are uncontrollable, for example: Competitors, politics, social, economic, ecologic, demographic, ethical, technologic and regulatory implications [55, p. 2] [56, p. 1] [57, p. 390]. SWOT analysis is its attempt to combine internal and external aspects to simulate strategies [58, p. 93].

	Helpful	**Harmful**
Internal	Strengths	Weaknesses
External	Opportunities	Threats

Table 4.1.: SWOT Analysis [58, p. 93]

There are the following categorizations within the matrix of SWOT analysis:

- Aspects related to organization itself are *Internal* (Strengths and Weaknesses)
- Aspects related to organizational environment and their relationships are *External* (Opportunities and Threats)
- Aspects which support organizations are *Helpful* (Strengths and Opportunities)
- Aspects which can have a negative impact on organization are *Harmful* (Weaknesses and Threats)

The four buildings blocks are:

- **Strengths** – Thompson [59, p. 57] define strength as “those elements of success such as a strong competitive position". Kormaris [53, p. 4] tell us strengths are “The strengths of an organization are the core competencies of the company, the key factors which enable it to excel in certain aspects . . . ”. Further Gretzky [58, p. 93] tells us that see “. . . strengths as current factors that have prompted outstanding organizational performance”.

  As a sum of these statements; Strengths are values of an organization which achieve a unique selling proposition (USP) that emphasize a product or service from competition.

- **Weaknesses** – Kormaris [53, pp. 4] said “As weaknesses we define the flaws that an organization has, something which means that these weaknesses might lead to serious problems . . . ”. Gretzky [58, p. 93] defined it that “Weaknesses are organizational factors that will increase ... costs or reduce ... quality”. Thompson [59, p. 57] tells us that weaknesses are “those elements which prevent the organization from achieving that competitive advantage“.

  Summarizing; Weaknesses are properties of an organization that prevent it to achieve an USP compared to competitors, this may can into serious problems.

- **Opportunities** – “maximized to fit the organization’s values and resources” [59, p. 58]. Kormaris [53, p. 5] defined it the following way “These are certain steps which will help a company to perform better”. Gretzky [58, p. 94] said, “SWOT analysis views opportunities as significant new business initiatives available to a ... organization”.

  Summarized: Opportunities are paths which allow to adapt values to gain new significant business improvement.

- **Threats** – “factors that the organization is not well equipped to deal with” [59, p. 58]. Grezky [58, p. 94] said that “Threats are factors that could negatively affect organizational performance”. Kormaris [53, p. 5] identified it as “. . . the potential reasons which might harm a company”.

Summarized: Threats are elements that have the capability to harm organization.

4.1.1. SWOT Analysis

SWOT analysis should provide a situation analysis. What is our current situation regarding to information security? Because this is a complex question, a direct analysis with SWOT of information security will not cover the full topic in deep. Sub questions have to be formulated. This questions refer to parkerian hexad (see 2.1). To cover information security in an adequate intensity the six topics of parkerian hexad have to be examined to identify strength, weaknesses, opportunities and threats. The result of this analysis will be six SWOT analysis about the following segments: Confidentiality, possession or control, integrity, authenticity, availability and utility. The following information should support you to identify all aspects of one segment [9, pp. 8] [3, pp. 16]:

1. **Confidentiality**

   Are all information of organization protected against unauthorized access?

2. **Possession or Control**

   Are all information of organization protected even if they can be access physically by a third party?

3. **Integrity**

   Are all information protected that it cannot be changed in an unauthorized and undesirable manner?

4. **Authenticity**

   Can every information be determined to a specific person or group?

5. **Availability**

   Are all resources available when they are needed?

6. **Utility**

   Are all information exist in a useful type?

4.1.2. TOWS Matrix

TOWS matrix (table 4.2) is a variation of SWOT, where multiple factors are identified and merged together into one big picture. It merges the external opportunities and threats against internal strengths and weaknesses. TOWS provide a systematic approach to identify relationships between strengths, weaknesses, opportunities and threats. These relationships will be used to identify business information security objectives [57, p. 387][60, p. 2][61, p. 771].

	External Opportunities (O)	**External Threats (T)**
Internal Strengths (S)	SO Strategies that use strengths to maximize opportunities	ST Strategies that use strengths to minimize threats
Internal Weaknesses (W)	WO Strategies that minimize weaknesses by taking advantage of opportunities	WT Strategies that minimize weaknesses and avoid threats

Table 4.2.: TOWS Matrix [61, p. 771]

4.1.3. Process

The process for the TOWS analysis is carried out as follows:

1. Object definition of SWOT analysis
2. Introduce participants about SWOT analysis procedures
3. Everyone should consider about the parkerian hexad topics regarding to strength, weaknesses, opportunities and threats against the organization
4. Summary all ideas of every member to a big TOWS summary
5. Discuss the TOWS summary and the classification of each topic
6. Derive strategic objectives from TOWS analysis [57, p. 388]

A graphical overview about the process can be found on picture 4.1.

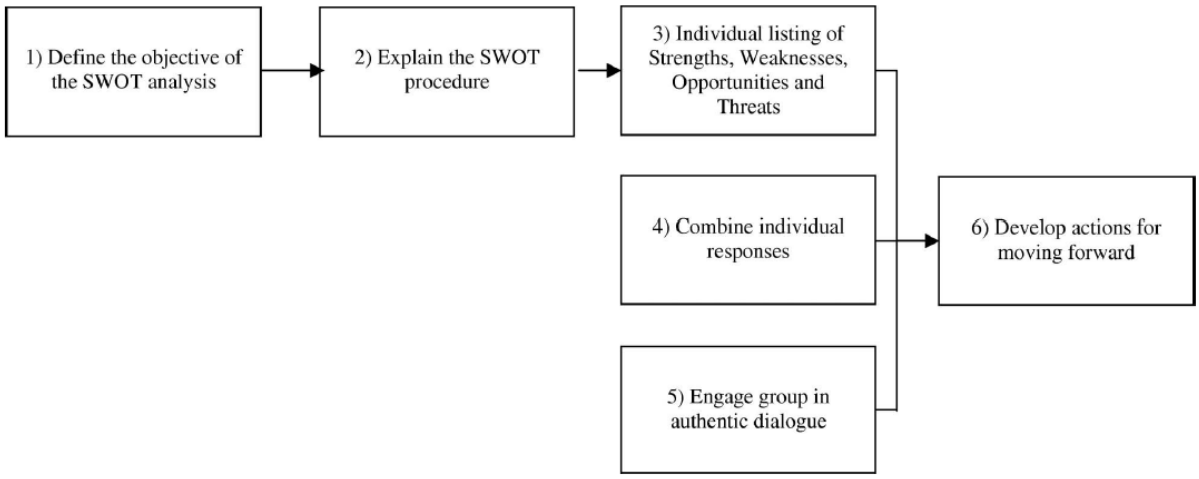

Figure 4.1.: SWOT Analysis Life Cycle [57, p. 389]

Step One: Objective Definition

Defining the desired end state and the main subject should be the first steps in SWOT analysi. This have to be approved by all participants. Definition of main subject and end state have to be placed carefully, failure during explanation can lead into waisted resources such as time consuming and unnecessary discussion.

Step Two: Explain the SWOT Process

After objectives are approved and defined, the second step will be to explain all participants the procedure how an SWOT analysis will performed. This step is essential to align the same level of experience to each participant. Future meetings should be scheduled with the same participants, fluctuating members will increase the risk of unsolved situations.

Step Three: Individual Situation Assessment

The third, and most well-known step, is to ask all participants to assess the objectives against strengths, weaknesses, opportunities, and threatss that can have influence on organization. Results of each participant will be written down of their own on a worksheet.

1. Strengths – Where we are good in
2. Weaknesses – Where we are inefficient

3. Opportunities – Who could we be
4. Threats – What could happen

Step Four: Summarize All Considerations

After all consideration are collected the next step is to summarize these responses into one larger picture, a TOWS matrix. This picture contains all collected aspects of organizational strengths, weaknesses, opportunities, and threats.

Step Five: Global Discussion

Review every SWOT part with all participants and analyze it. The results can have some mind changeing effects. Strengths should be reviewed as weaknesses. Hidden threats are can be included in opportunities. Therefore, it is important to ask the following questions:

- Can specific threats also be an opportunity?
- Are threads part of opportunities that should be considered?
- Can strengths also be weaknesses?

The answers to these questions can change thinking and enable managers to draw a complete picture, which allows to develop appropriate strategies and promote innovative paths. Keep in mind that the way how issues are analyzed and classified are heavily depends on involved people during analysis. For example, if new technologies occur, some treat it as opportunity, others as threat [57].

Step Six: Strategic Evaluation

The last step in this process is to fulfill TOWS matrix. Strengths, weaknesses, opportunities and threats are already in place and have to be merged together. The essential outcome of this strategic evaluation is to identify information security strategic objectives.

4.1.4. Analysis of SWOT for ISS Development

SWOT analysis can be used as it is known in public. The only difference to traditional SWOT analysis is that this analysis is directly targeted to information security, or more specific, to 6 topics of information security. Analysis cannot be satisfied without experienced technicians and people who are familiar with

organizational structures. To fill out every of these 6 topics, a deep knowledge about security is mandatory. Risks are not part of SWOT analysis. This means that it could happen, that a strategy against a threat will be developed that statistically happens every 10.000 years or impact will be low. For example; If technicians are involved in strategy development, they tend to think in products, not in solutions. Product decisions shall not be part of strategic development process. Product evaluation, if additional products are required, should be accomplished after a confirmed information security strategy. SWOT analysis can deliver strategic objectives which are evaluated against a specific parts of information security. The objective can stabilize strength, eradicate weaknesses, use opportunities, or mitigate threats. It allows to identify issues for certain areas which shows present and future performance of information security.

4.2. Business Model Canvas for Information Security

Business Model Canvas (BMC) is a tool to visualize a business plan. Traditional BMC is divided into 9 parts: customer segments, customer relationships, channels, value propositions, revenue streams, key activities, key resources, key partners, cost structure [62, p. 1]. BMC offers three main advantages [63]:

1. **Focus** – It allows you to focus on your business drivers (customer needs). It shows which activities are slower you and hamper your business. That allows you to evaluate your business model to cover up customers' needs.

2. **Flexibility** – It is an easy brainstorming tool to make thoughts about the business model. That makes it easier to test new possibilities instead of writing inflexible business plans. BMC can be varied.

3. **Transparency and Comprehensible** – It is easier to talk to other about your business model with this simple approach.

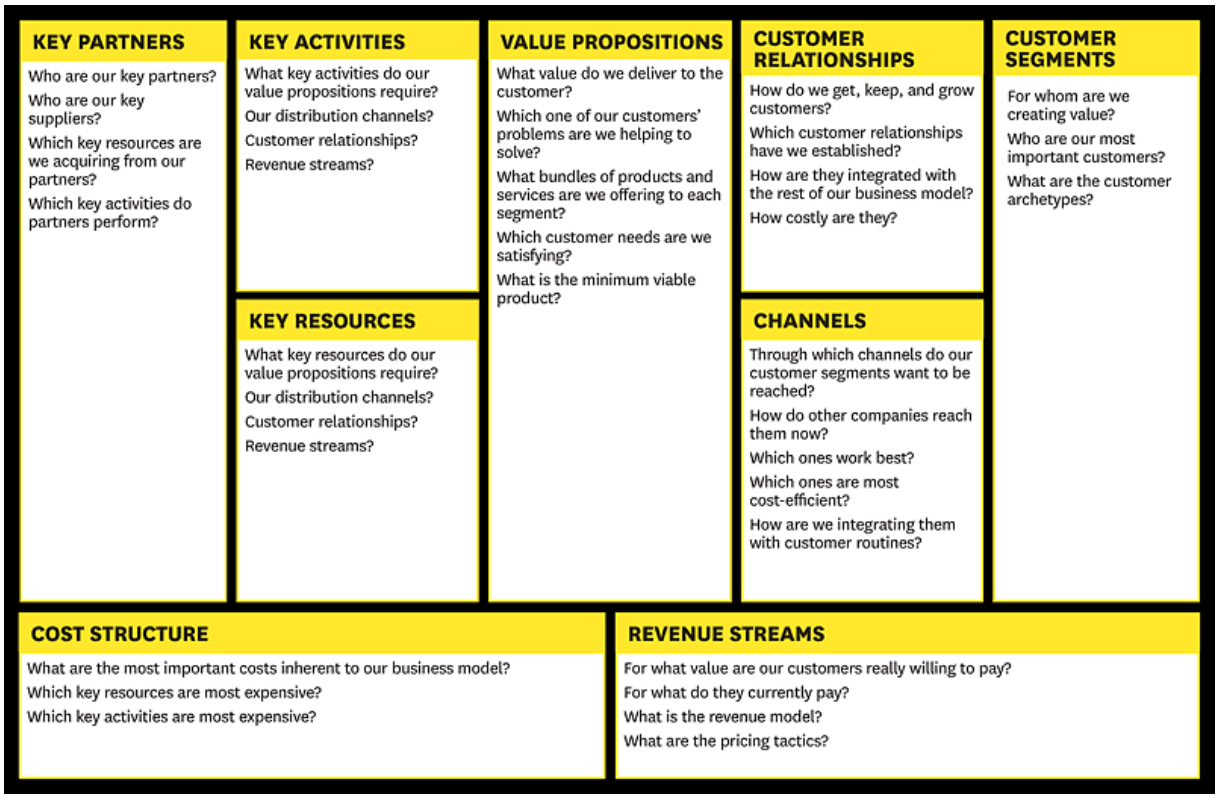

Figure 4.2.: Original Business Model Canvas [64]

4.2.1. Adapted BMC for IS

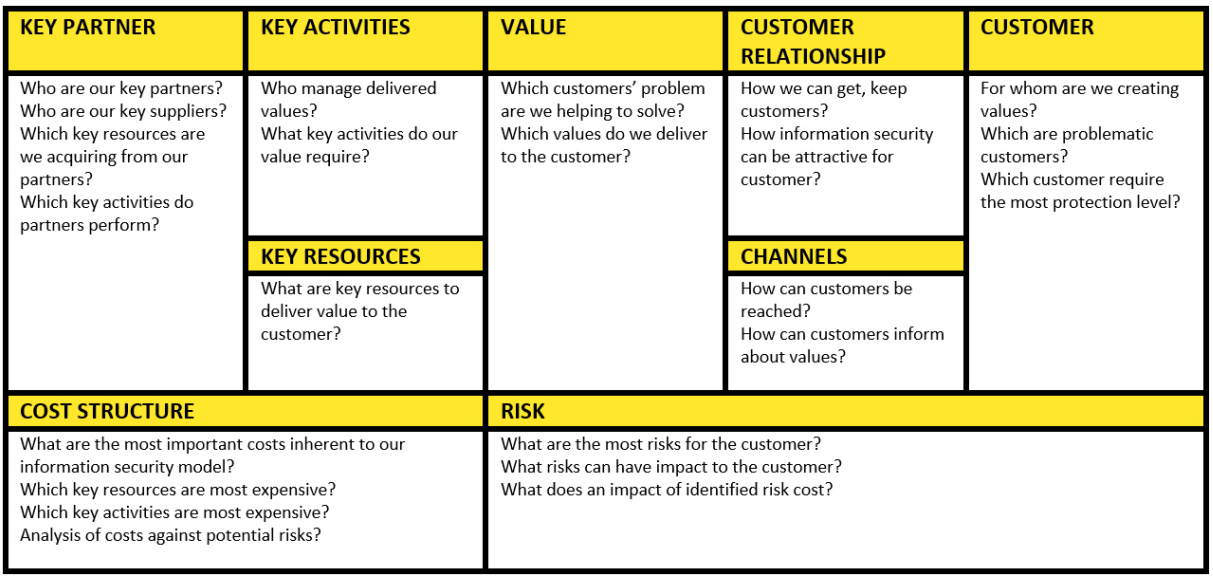

Figure 4.3.: Adapted Business Model Canvas

CUSTOMER SEGMENTS renamed to CUSTOMER because this BMC is focused on information security, so the segment is already fixed. It is still focused on the question 'who is the customer?' It should be determined for whom are values created. Different customers have been treated in a different ways. Information security is not only based on products it is rather based on people. In every organization, there are people which created resistance against changes. To get a full picture of your considered topic, it is helpful to think about such people especially if such persons are in leading positions. For specific considerations, it can be useful to know if there are customers which require a higher level of protection. For example, a payroll accountant operates with more sensitive data as a trainee.

CHANNELS are focused on how the communication between customer and value provider can happen. Due to the fact that people are part of information security, there have to be a channel to communicate with them. One or more communication ways can be defined how the customer can be informed or can inform themselves. The customer should have the ability to look up the amount and details of values that the provider offers.

CUSTOMER RELATIONSHIP is dealing with realationships to our customers. How can win we the minds of the customers for the common cause and how keep them? How can it done together as a big team who everybody knows what to do? Every way to place information security in an attractive way are welcome.

VALUE is telling us about the benefit for the customer. Which value do the customer receive? Customer have problems as well and requires support, how can we help them? In which positions can values transferred to the customer? Values is based on resources and activities.

KEY ACTIVITIES are activities that have to be done to bring value to the customer. Key activities rely on persons, who will do these activities? May additional activities requires additional resources. Key resources are required to deliver value to the customer. Resources are consumed by key activities. This can be personal resources, external partners, or simply operational costs. Key resources should be controlled appropriately, missing key resources can lead into incomplete values for the customer.

KEY PARTNER are partners or suppliers which support you to deliver value to the customer. They do not simple support you, they are a fixed part of value generation and have a powerful position. key partner also requires key resources. It should be defined which activities are performed by key partners.

COST STRUCTURE is showing the costs of this model. What are the cost in sum the established costs to implement all values for the customer. Costs occur from key activities, key resources, and key partner. Cost structure is a common criterion of managing decision.

REVENUE STREAMS was replaced by RISK. The idea behind that, there is no real revenue. Information security are always dealing with risks, so the revenue can only be risk mitigation. In addition, the risk now serves as the basis for BCM for IS. The main question is; Against which risk should be evaluated? It should be defined what are the most risks on the chosen topic and how can these risks have impact on the customer. A powerful indicator for calculation can be potential costs if the risk occur. This value can be compared with the costs of mitigate this risk in section "cost structure".

4.2.2. Process

The sequence for BMC for IS divided into ten parts. It begins with the (1) selection of the risk. Afterwards (2) customer identification and (3) value definition. The further six steps have no specific order. The last step will be (10) evaluation.

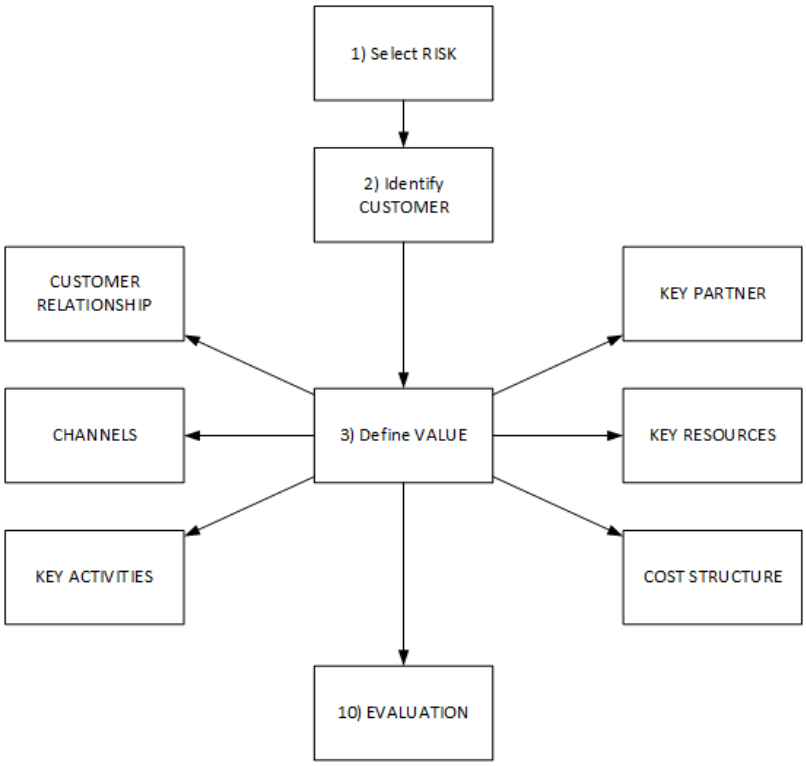

Figure 4.4.: BMC for Information Security

Step One: Know your Risks

Risks are the most essential part in BMC for IS. Every BMC in this context is based on risks and how to handle them. Risk is affecting all other eight parts. If you are starting to use BMC for IS you have a risk and want to identify mitigations and how much does it cost. Risks are usually retrieved from risk management department or can be determined at you own. In the first step, a risk should be analyzed in detail to know what can be a potential impact to our customers. The goal is to define an calculatable number of money that tells you, if that risk happen to our customer, my estimated costs are XYZ.

Step Two: Identify Customer

The second step is dealing with the customers. It identifies for which customer will values be served. An organization contains different customers with different needs. A customer can be an organization, department, group of persons, group of companies or a single person. It is an important part to know, who should have a benefit of delivered values. Customer definition can change after the definition of values and risks. For example, values affecting more customers as initial predicted or risks are larger than expected. If your value are awareness trainings, it is essential to know which customers and how many are involved. Payment should be considered during customer selection, at the end of the day someone have to pay for the value. A department leader with fixed budged are able to manage his costs, employees in production rather not. Customer selection highly depends on risks. Which customer will be affected if a specific risk occurs or which action on which customer have to be taken to mitigate a risk.

Step Three: Determine the Value

This step should identify and define the value that should be deliverd to the customer. The value is a service or product to mitigate or eliminate a specific risk. A research should be done to evaluate how the risk can be handled. This can lead into a specific product, organizational change, or new policies. One main point is to enable a cost estimation. A statement like “secure all data against threats” will make a cost estimation rather impossible. As more specific values can be identified, the costs can be ordered more accurately.

Select Channels

This step should define the communication channels between you and your customer. Information secu-

rity is a continuously process, there is no fire and forget. This have to be communicated with customers in defined channels. Channels can be email, sms, personal contact, phone, web page or files which customers have committed to read periodically. Different channels have different advantages and disadvantages. Channel selection should be considered regarding to delivered values. Updates and smaller changes can be posts on intranet where every customer have access. Projects mostly require personal contact or at least phone conversations.

Manage Customer Relationship

This step should determine how customers being supervised by you. Contact to the customer is an important factor to keep customers informed about values and changes. An individual person should be defined to 'sell' information security to the customer. That's not a job you can do on the side. Information security is not very popular at every level in each organization, a custom relationship manager should educate customers why they bought values and why they are still needed. Take considerations of the following topics during customer relationship establishment:

1. Communication to the customer is as almost important as delivered values
2. Values depends on customer requirements which have to be known

Decision makers are regularly not familiar with information security topics and their requirements/impacts. Only informed top management will invest in information security.

Identify Key Resources

This step should identify all key resources that are required to deliver values. Key resources are resources that will lead in waiting periods or failure of implementation is case of absence. To identify key resources, a specific definition of value is helpful. Key resources can be personal, capital, external partners, or knowledge. It should be considered that key resources are always limited and be used up.

Identify Key Activities

This step identifies the key activities that are necessary to fulfill value delivery to the customer. Key activities can be accomplished by internal or external resources. Activities are versatile, from calculating power in a public cloud till persons who solves service requests. Activities rely on values that should be

delivered, an adequate value definition is required. One key activity that should always considered is that who will bring value to the customer. Key Activities should be considered by the following criteria:

1. Time consuming activities
2. Activities that require a lot of key resources
3. Activities that have an very high impact on value creation

If partnerships are in place, a key activity is to manage these relationships [65, p. 10].

Identify Key Partner

This step identifies your key partners to succeed value delivery to the customer. Partnerships have the purpose to support you to deliver values. Partners offers key resources and fulfill key activities which are required by values. Considerations during partnership selection should be:

1. Availability of partner resources
2. Knowledge of partner

Key partners can be internal and external. Security department can be an internal partner. External partners could be consultants or contract workers. Key Partners support you in a not negligible part of value delivery and should be considered carefully. Partners have effects on required resources which lead into increased costs [65, p. 10].

Define Costs

This step is focused on the overall costs of your information security model. All costs have to be collected from key partners, key activities and key resources. The sum of all these costs give you the estimated number what an implementation of this model will cost. Consider the following costs:

1. CAPital EXpenditure (CAPEX) – licenses, hardware and implementation
2. OPerational EXpenditure (OPEX) – salary, maintenance and consulting

Step Ten: Evaluate Business Model

The last step is to evaluate the information security business model. After completion of the model it delivers an overview which allow to create a decision. Delivers this model a strategic objective for an information security strategy? The main focus should be on an economic decision. One important question to ask is:
Are the costs of a potential impact higher than the mitigation? If costs are too expensive or other limiting factors occur, there is always the possibility to adapt the business model to fit perfect to organization needs.

4.2.3. Order of Elements

BMC for IS allow a restructuring of containing parts which allows to set a graphical focus on RISK. An adapted model could look like figure 4.5.

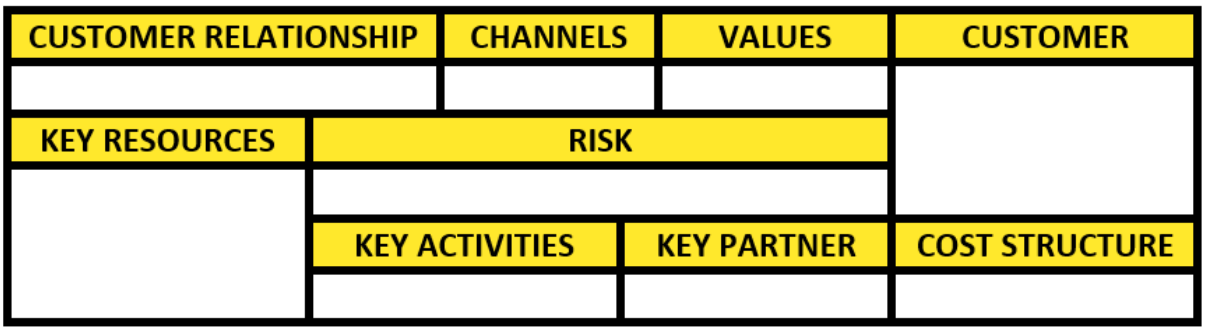

Figure 4.5.: BMC Reordered

4.2.4. Analysis of BMC for ISS Development

This model is mainly focused on risks. It deals with identified risks from organization and do not discover risks. Risk management is not part of this model. As result of this model, a possible solution with all influence factors should be identified related to a specific risk. Influencing factors can be limited resources, the value itself or customers. This model offers a possibility of an overview of a solution. The model relies mostly on traditional BMC, this increase the possibility of acceptance for management. Top management is usually familiar with BMC and a limited adapted BMC for information security will be easier accepted instead of a complete new model. To fulfill this model, a deep knowledge about security and how business works is essential. Especially cost estimation would be more specific if detailed knowledge about key partner, key activities and value are available. This model allows to play with possible

values for customer to mitigate risk and detect the best fitting solution for business. It enables to specify customers for the intended purpose and see direct impacts. Further is delivers key resources which, most of the times, have a direct impact on cost structure. BMC for IS is an interwoven model where every part can affect each other, relationships can be directly demonstrated.

4.3. Ansoff Matrix / BCG Matrix

4.3.1. Ansoff Matrix

The Ansoff Matrix is a 2x2 matrix, which presents various strategies that a company can follow in its entirety or for individual business units. The dimensions of the product and the market are considered in each case in the characteristic 'present' and 'new'. With the help of the Ansoff matrix, the general direction of the company can be defined (strategic planning) at an abstract generic level [66, pp. 30].

	Existing Products	**New Products**
Existing Markets	Market Penetration	Product Developement
New Markets	Market Developement	Diversification

Table 4.3.: Ansoff matrix [67, p. 5]

Usage

- Simplify strategy definition by reducing options to four generic strategies
- Support for the derivation of concrete measures within a quadrant

Market Penetration

(Existing products in existing markets)

- The company is trying to increase the market share of current products in the current market, e.g. by
  - Purchase of competitors' customers
  - Attracting customers who have not purchased the product so far
  - Intensify the purchasing behavior of existing customers

Product Development

(New products in existing markets)

- The company is trying to increase demand in the current market by changing the current products or by developing completely new products
- An attempt can be made to align the products with specific customer requirements, e.g. to offer a product in different quality levels and at different prices

Market Development

(Existing products in new markets)

- The company is also trying to offer existing products in new markets
- This can happen over:
  - The identification of new customer groups in the current sales territory (e.g. instead of only private customer expansion of sales to business customers)
  - The geographic expansion of the sales activities

Diversification

(New products in new markets)

- The diversification strategy may be very attractive from the potential but very difficult to implement because the company is not really familiar with the products or the markets (typically acquiring know-how)
- The success of this strategy is the identification of specific core competences of the company, which can be a strategic competitive advantage for products in other markets (keyword: USP)

4.3.2. BCG Matrix

The Boston Consulting Group Matrix model is an approach for portfolio analysis. It will be used to analyze strategic business units (SBU) of an organization. The model is focused on market share and growth of SBUs. The BCG matrix looks like figure (4.6).

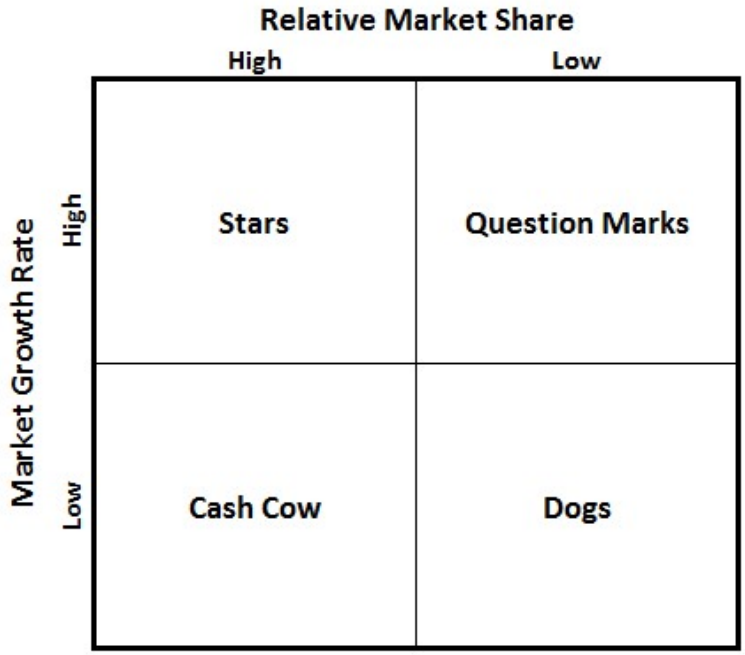

Figure 4.6.: Boston Consulting Group Matrix [68, p. 105]

Stars

Stars are markets which are high-growing. Organization are a market leader and this business unit generates a considerable income. This business unit requires a large investment to support growth. Investments in this part are needed to meet working capital and expand production environments. Stars offer opportunities for growth and long-term profits. If the markets annual growth rate decreased under 10 percentage, Star becomes a Cash Cow.

Question Mark

Question marks are markets with high growth but relatively low market share. Usually they require an substantial amount of cash to keep up with market development with the wish to change into a cash cow. One major problem with question mark is that the sum of required cash for marked development may never returns and will be a loss.

Cash Cow

Cash cows are markets which are slow growing, but organization have a strong position and a high market share. These business units are organizations core business. These units produce an substantial profit. Organizations try to keep their market share.

Dog

Dogs are markets which organization have low market share and markets a growing slowly. Organization will generate low profits or have a loss, further they have low long-term potentials [68, p. 107].

4.3.3. Adapted Ansoff/BCG Matrix

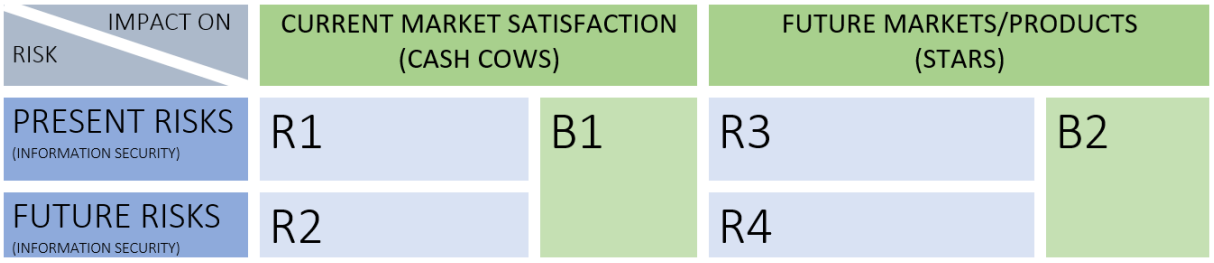

Figure 4.7.: Adapted BCG/Ansoff

This model is an approach to involve top management and security department in one strategy for information security. The idea behind this model is that top management provides information about business current situation & future alignment and security department place risk regarding this business assets. This allows an ideal alignment of information security related to business objectives. Further, an adjustment of strategic business objectives has a direct impact on information security strategy. These information security model is a mixture of two business model; Ansoff matrix and BCG matrix. Ansoff matrix analyzes existing/new products in existing/new markets [66, p. 22-23]. This part of Ansoff model was adapted to existing/new risks in existing/new SBUs. The SBUs are initially defined in BCG matrix. In this model (4.7) Cash Cows and Stars are used. Dog and Question Mark are not part of this model.

Description

Box B1 represent the current SBU (Cash Cow) which the company hold a relative high amount on market share and this produce a substantive amount of income. The content of this box will be derived from top management that visible their current business situation. Box B2 represent SBUs which are known as Stars. Organization determined B2 as future business markets. This value has also been filled out by top management. R1 are known risks related to current business situation (B1). This box should represent risk that can have direct impact on business. The same risks can also have negative impact on future market situation (B2). This have to be considered in box R3. R2 and R4 are obvious risk that are able to have a major affect future business success in current and future markets. These risks shall be identified via risk management.

Process

1. Determine business Cash Cows and Stars
2. Place existing risks against business strategy
3. Identify future risks which interfere business objectives

Step One: Determine Business

The first step is to identify business objectives (B1, B2). This have to be done in coordination with management. Only the management can show up business strategies and objectives. These objectives have to be divided into Stars and Cash Cows. Management support is mandatory. This step guarantees that risks will be directly evaluated against business objectives.

Step Two: Place current risks

The second step is to fill out known risks (R1, R3) against business objectives. These risks have to be provided by risks management. The key question to fill out these risks is:

- Which risk can have substantial negative impact on business objectives?

Risks will be evaluated for current markets (Cash Cow) and future markets (Stars). Only risks with major impact should be written down.

Step Tree: Identify future risks

The Last step is to estimate risk which can have essential impact on business objectives. These risks have to be placed in R2 and R4. The question for this is:

- What risk, related to information security, can have an significant negative impact on future business goals?

The way of risk identification is not defined and can be choose by participants during strategy development.

4.3.4. Analysis of Adapted Ansoff/BCG Matrix

The mixed version of Ansoff and BCG matrix offers one main advantage: The information security strategy is directly aligned to business goals. Further, top management, is involved in information security

strategy development. Cash Cows and Stars must be defined by board and cannot be estimated by CISO or security department. Moreover, it enables that board members can participate in strategy development. This integration of top management during strategy development raises the knowledge about why information security is needed in an organization. This model forces the corporation between top management and security department. The drawback of this model is risk assessment. Participants must be able place current risks in relation to business goals. A risk catalogue with known and assessed risks will be helpful. Further, future risk have to evaluated against strategic objectives. This is the most complex part of this model. On the one hand risk have to be identified, which is part of risk management. On the other hand, these risks should be set in relation to strategic objectives. Identifying future risks is an extensive work. A well-established it risk management is indispensable.

4.4. McKinsey 7S Model

Tom Peters, Robert Waterman and Julien Philips developed in 1980 McKinsey 7S model. It is based on human resources (Soft Ss) and hard facts (Hard Ss). The objective of this model is to show seven elements of the company together to achieve organization success. Each element is connected to each other element and interact together. The model can be found below (figure 4.8), divided into Hard S (Grey) and Soft S (Blue) [69, pp. 2].

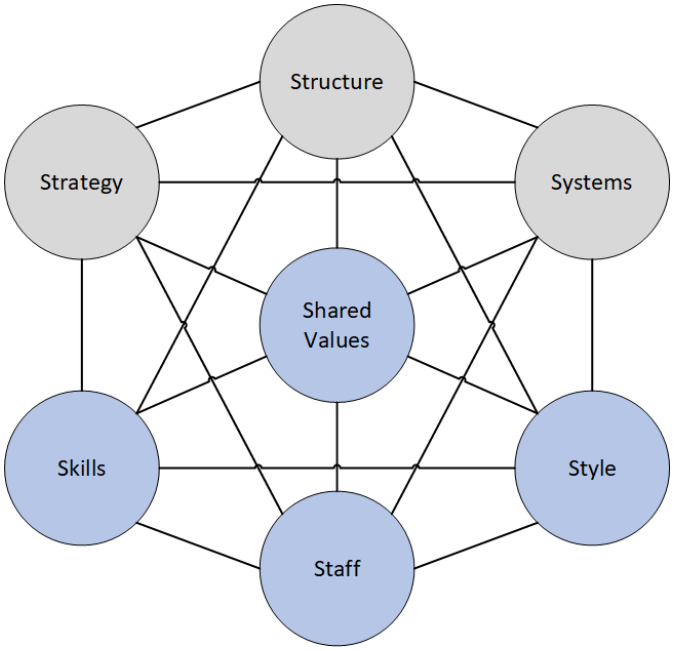

Figure 4.8.: McKinsey 7S Model [69, p. 8]

The model is valuable and can be used in different situation. The most common situations are:

- Change of organization
- Develop/Implement new strategy
- Future changes of elements
- Merging organizations

The model is divided into seven elements which are subdived into hard and soft areas. Hard elements are Strategy, Structure and Systems. These elements are easier to handle and identify rather than soft facts. Soft areas (Skills, Staff, Style, Shared Values) are the basis for competitive advantage.

Hard S	**Soft S**
Strategy	Style
Structure	Staff
System	Skills
	Shared Values

Table 4.4.: Hard/Soft-S [69, p. 8]

Strategy is the concept how to be successful on the market and achieve substantial competitive advantage. A strategy should provide objectives with mission, vision and values. The interaction between strategy and other elements can be analyzed if they fit together. Structure is the way how organization is structured and organized. Structure is the hierarchical chart of an organization. This is one of the easiest adoptable elements of the framework. Systems represent organizations processes and procedures and how decisions are performed. This area introduces how the organizations works. In cases of organizational changes, Systems are the most important area. Skills are areas, which attendees provide high capabilities. Often specific competences and capabilities are required in cases of organizational changes to enforce a new strategy. Staff are dealing with employees of the organization. This element is focuses on training, motivation, hiring and rewards. Style is the kind of how managers control the organization. This includes interaction with other managers and how decisions are made. Style refers to the management style. Shared Values are the centre of 7S model. This contains norms and standards which direct attendees. Therefore it provides the basis of organization [69, pp. 2].

4.4.1. Adapted Version of 7S Model

The adapted version of 7S model is focused on information security. The central element, which can be named as subordinate goal, is the vision. The IS vision represents the ideal situation where the company

want to be with 7S for IS. Every area has a relation to the information security vision element. This, as already expected, requires a previous definition of vision statement. The IS Strategy, if already exist, should show the current direction of the organization related to information security. IS Structure representing how information security is aligned within organization. Who is responsible for which part of information security? Which roles exist and what is their purpose? IS Systems are containing processes and procedures regarding to information security. This show how information security will be lived in organization. Skills still represent the capabilities of employees. The visibility of competences allows and overview how information security roles and responsibilities can be distributed and which projects requires specific skills. Staff concerns about the number of employees which are dealing with information security and how keep them up to date. Further, it is involved in the whole human resources lifecycle which takes care about reward, assessment, motivation, and training. Style is concerned about information security managers. This means, how manager establish processes and take actions to increase information security. In other words, how IS managers coordinate IS related topics. The adapted version of McKinesys 7S model can be found below (figure 4.9):

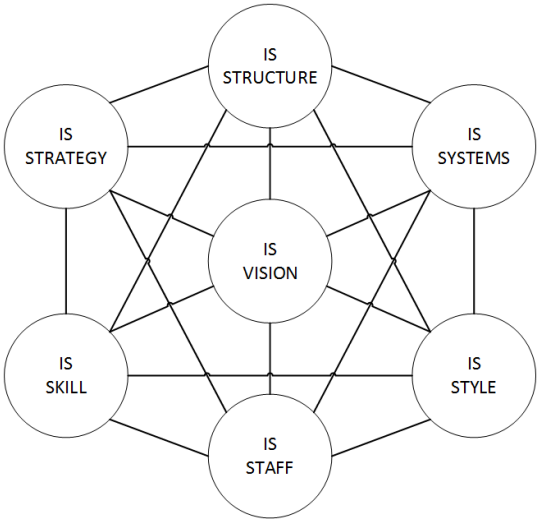

Figure 4.9.: Adapted 7S Model

4.4.2. Process

Step One: Fulfill Model

7S model provides an organizational overview, it is irrelevant on which element will be started and in which order elements will be filled out. After fulfillment of every area, an abstracted picture of information security will occur. Misaligned strategies or uncommon systems can be detected. It is also

be able to discover elements which are not support IS vision. For Example: You define a strategy for fast security incident response, but you don't have the staff neither processes that support this strategy.

Step Two: Specify the Ideal Organization Design

Form a team which are familiar with security design and evaluate what is the most effective information security design for your organization. With the knowledge of connections and alignments, you will be able to identify information security strategic objectives which support all elements of 7S model. The starting situation will provide you a basis where your information security considerations can start.

Step Three: Identify Initiatives

After you've defined your current situation and the ideal situation, information security strategic goals will be identified. To achieve these goals, action steps have to be taken. These steps are called information security initiatives. The initiatives should provide help during the movement of your organization to the predefined ideal information security situation [69, pp. 2].

4.4.3. Analysis of Adapted 7S Model

This adapted 7S model provide a big picture of information security within organization. Global decision can be visualized in a big context and it provide visibility of interactions between all those elements. This allows to foreseen necessary actions in cases of organizational changes. The model allows to identify false used elements and a straight approach towards IS vision. The drawback of a top-level overview is the level of details, specific details cannot be shown in this model.

4.5. Stakeholder Analysis for Information Security

The process of identification of various parties that can be affected by an information security strategy is called stakeholder analysis. Stakeholder analysis depends on utilized techniques which are used to identify relevant stakeholder and information about how these groups can be affected. These informations will be provided to the developer of the information security strategy to design it in an efficiently and effectively way [70, p. 10]. Stakeholder referenced to information security can be a single person, a group of persons or organizations which take advantages or disadvantages of investments in information security. Stakeholders can have positive or negative impacts of successful implemented information

security initiatives, or can influence their success. Every stakeholder has different requirements and attitudes. It is an essential to identify the different stakeholders. An stakeholder analysis can accomplish identification. Stakeholder analysis is defined as [71, pp.130]:

"Stakeholder Analysis is an analysis that aims to identify the stakeholders that are affected by the result of a project simultaneously with the result's success depending on the coorporation between the stakeholder and the project." [71, p.130]

Impacts can occur in a short or a long-time period. Stakeholders can be affected by direct action (first-order impact), or as a result of the action (second-order impact). For example, an organization want to establish a data classification. Every department leader has to classify his files with his team, the affect will be a direct first-order impact. If new files where created, classification have to be accomplished too. This addition work is an second-order impact [70, p. 10]. The purpose of stakeholder analysis are:

- Determine the positive or negative impacts of an strategic direction
- Identification of every stakeholder where there is a possibility to be affected from the intended actions
- Evaluate how the stakeholder be affected from proposed actions
- Find and assess possible changes in strategy that could mitigate negative impact on stakeholders

4.5.1. Importance of Stakeholder Analysis to Efficient Information Security Strategy Development

Traditional developing methodologies uses a risk based approach. These approaches evaluate the risk to specific services, processes or people to identify countermeasures. Risk is defined as "... security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information." [72, p. 4] Risk based approaches are focused on identification, assessment and prioritization of risks. The goal of risk management it to keep decision makers informed about information security risks [73, p. 10]. Relevant information about critical risk will be provided to decision makers to allow them to set the appropriate steps. Stakeholder analysis goes a different way. Management creates a draft of information security strategy and stakeholder analysis will estimate the potential impacts. The knowledge about the impacts will allow a statement if the strategy will fulfill its intended purpose. Further, unconsidered outcomes can be identified and adjustments can be provided.

4.5.2. Why do we need Analysts, Experts and Managers?

Each of this role is important in the stakeholder analysis process. Analysts managing the whole stakeholder analysis process and are responsible for them. Further they know how to use the required methodologies. Experts are knowledge carriers with large experience. These persons can estimate which impacts possible objectives, determined by the managers, will have. Moreover, experts guide managers related to information security. Managers are the executive instance, they set the direction of the information security strategy. This direction will lead into strategic objectives [70, p. 11].

4.5.3. Process

Before stakeholder analysis can start, decision makers have to provide a draft of information security strategy. The business process looks like (graphical view in figure 4.10):

1. Executive Board set direction
2. Perform stakeholder analysis
3. Check if direction fits to the intended consequences and initiatives
4. Fix strategic objectives

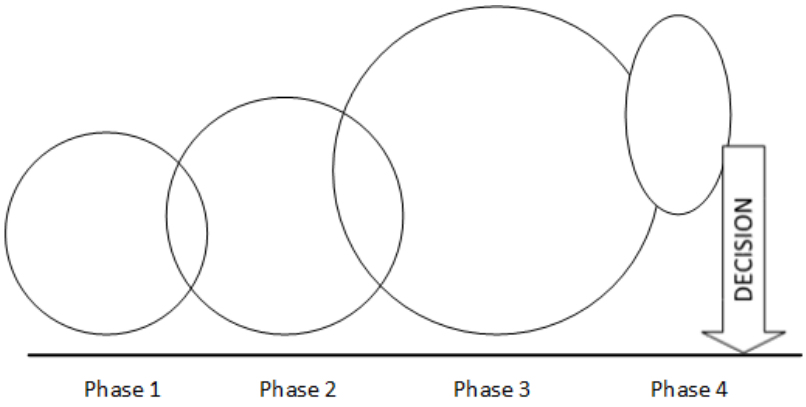

Figure 4.10.: Stakeholder Analysis Phases

After executive board committed to a potential direction, stakeholder analysis process will be started. Stakeholder analysis detect possible advantages and disadvantages to various stakeholders. Figure 4.10 shows the identification process. After a direction was set by board members, analysts and experts check if it fits to the intended purpose. If the stakeholder analysis detects an important negative aspect, a rethinking of direction should appear.
Required steps of stakeholder analysis:

1. Literature review
2. Assessment of the impact of information security strategy
3. Systematic approach for stakeholder identification
4. Extend the impact assessment
5. Get stakeholder input about future strategy
6. Evaluation of influence and the significance of stakeholders
7. Report results to management board

4.5.4. Step 1. Literature Review

The first step in the analysis will be to review appropriate data and gather information on what the intended strategy will have affect. Review resources can be books, articles, dark web information's, forum entries or newspapers. The reviewer will get familiar with strategy, intended actions, possible stakeholder, and related topics. The literature review decreases the possibility of misunderstandings during stakeholder analysis. It is not possible to do a complete research to all information security related topics. The research enables a state of the art know how about the strategy and their related topics [70, pp. 23].

4.5.5. Step 2. Assessment of the impact of information security strategy

The second step deal with the impacts of the information security strategy. These impacts should be identified systematically. Cases of false assessed or overlooked impacts will result in an inaccurate analysis [70, p. 32]. Information about the impact of the information security strategy will be delivered by experts and literature review. Brainstorming can act as first attempt for impact identification. A broad team consists of Analysts, Experts and internal information security members can deliver important input for impact identification. These information's will be used later for a systematically determination of impacts. First-,Seconds-, and Third-order impacts should be identified.

1. **First-order impacts**

   These impacts can be directly referenced to the proposed actions in the information security strategy.

2. **Second-order impacts**

   This kind of impacts are caused by first-order impacts.

3. **Third-order impacts**

   These impacts are indirect caused by second-order impacts. For example; Strategy define that every information has to be classified. The first-order impact will be a project to classify all existing data. The second-order impact is that every newly generated data has to be classified. The third-order impact is that it required more time for creating new documents because user have to choose the appropriate security level.

An example for a graphical impact analysis can be found on figure 4.11. This graphic shows the example impacts of an ISO 27000 implementation. A diagram which shows the relations between the impacts of the new strategy is useful. This diagram simplifies the identification of affected stakeholder. Analyst will have the possibility to identify stakeholders related to the proposed actions in the ISS.

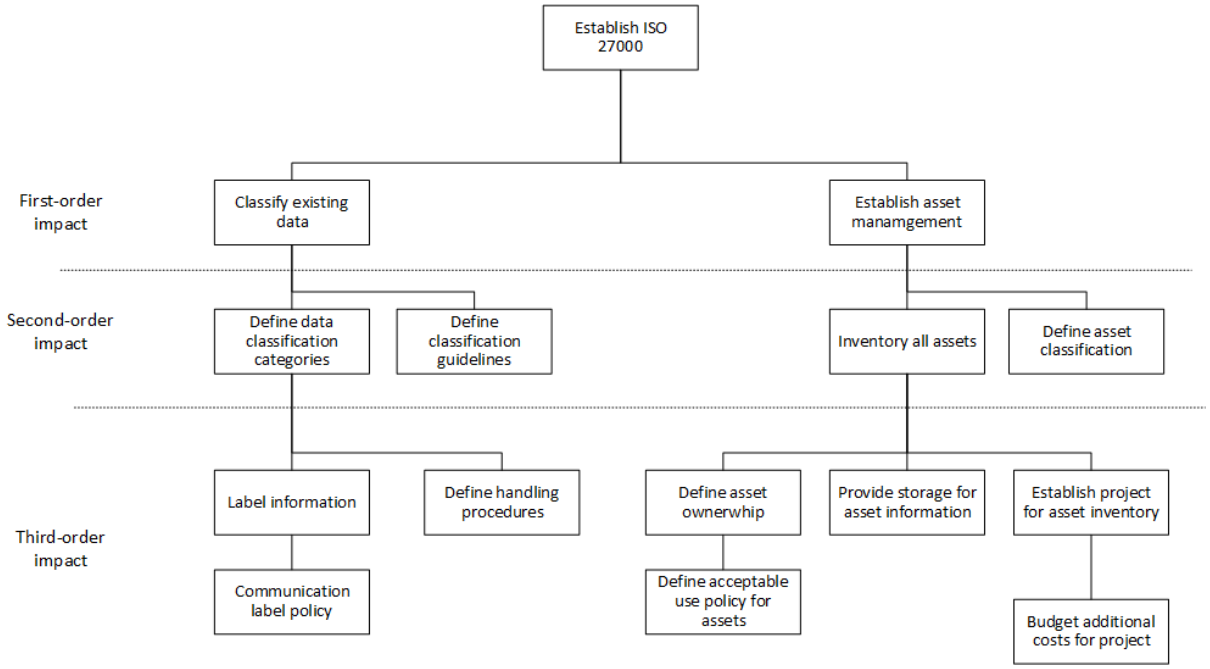

Figure 4.11.: Example Impact Analysis

First-order impacts

- Existing data have to be classified
- Asset management have to be established

Second-order impacts

- Data classification categories have to be defined
- Classification guidelines have to be defined

- All assets have to be inventoried
- Asset classification have to be defined

Third-order impacts

- Information have to be labeled
- Procedures for information handling have to be defined
- Label policy have to be communicated
- Asset ownership have to be defined
- Appropriate storage location for assets have to be identified
- Project for asset inventory have to be initiated
- Acceptable use policy for assets have to be defined
- Costs for asset inventory project have to be announced

Other areas of the iso 27000 may also have an impact on the company. This example shown a very detailed overview of how structuring impacts can occur. For real world situation, a top level approach will be more effective, otherwise you will get lost in details.

4.5.6. Step 3. Systematic Approach for Stakeholder Identification

To provide a complete stakeholder identification, there is a requirement for a systematically approach. The analysis of likely impacts must be happened in a coordinated way. A review of the influenced domains by information security strategy can support identification of stakeholder. Which departments are affected by which intended actions? Which parties are involved if strategy got fixed? Such questions can be handled in a systematic approach [70, pp. 24].
Analyst have to understand the units of stakeholder analysis. Stakeholder analysis striving to determine the impact, including social aspects and interests of participants. The diversity of these stakeholders can be shown to decision makers to estimate the consequences of the ISS. Stakeholder are identified with their interests in the areas where intended actions should appear.

Areas of Interest

Usually a new strategy affects multiple areas. An identification of the areas of interests provide a starting point which stakeholder need to be included. Areas can be determined by defining affected functions. Functions are activities which behavior will change by proposed action or which unintentional suffer from intended actions. The proposed actions should be reviewed by analyst related to functions. Think of the ISO 27000 implementation, depending on how the implementation occur, different functions will be affected in a different intensity. A smooth integration with trainings and courses will lower the entry level. A strict defined policy set without any possible user response can interrupt functions in their efficiency. An approach for an systematic identification of affected functions are non-existent. Two approaches can support you in definition phase of functions. (1) first/second/third- order analysis and (2) interview experts and stakeholders to support you during function definition. As a different example, comply with General Data Protection Regulation (GDPR), can have affect to the following functions:

- Legal department
- Executive board
- Governance
- Sales
- Finance
- IT innovation
- Education
- Information management
- Change management
- Data analytic
- Privacy
- Reputation

Techniques for Stakeholder identification

The following techniques can support you during stakeholder identification process, to enable a complete identification of affected stakeholders by ISS. The usage of more than one technique increases the likelihood of identifying all affected stakeholders. Techniques should be selected regarding the current

situation of the analysts. Limited resource can force analysts to shorten or cancel multiple techniques. Analysis should take care to use the best fitting technique for their purposes.

Self Identification

This technique offers the possibility to people, groups, departments to inform analysts that they assume that they are affected from ISS and their intended actions. Self-identification can occur in different forms:

- **Presentation**

  Analysts prepare media, presentations, newsletter, or intranet entries for a general audience. People can enter their names and topics of concern in an appropriate list. Analysts will review that list to identify stakeholders.

- **Public meeting**

  Analysts and experts will prepare public meetings where interested groups can participate. In these meetings will the ISS explained and what are the intended actions to succeed. Participants can, in case of concerns, enter their names in a list which can later be reviewed by analysts.

Staff Identification

This technique primary relies on already existing information about affected stakeholders by ISS. Together with self-identification, the following methods are the fastest ways for stakeholder identification:

- **Information Analysis from Employees**

  Information security department provide names of may affected individuals or groups. These stakeholders will be reviewed by analysts.

- **Association Analysis**

  Analysts gather lists and other material of groups in organization to figure out which can be affected by ISS. After analyzing these materials, analysts will examine appropriate stakeholder.

- **History Analysis**

  Analysts collect information about related or similar intended purposes in related activities. This information may support stakeholder identification.

4.5.7. Step 4. Extend the Impact Assessment

In the step 2 and 3, information about likely affected stakeholder are gathered related to intended action of ISS. Follow the pointed steps to identify how stakeholders likely be affected. To extend the impact assessment following techniques can be used. These techniques rely on expert knowledge:

Delphi Technique

"Delphi . . . be characterized as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem." [74, p. 3]

Delphi technique goes back to the US Air Force which started a study in early 1950 with the goal to obtain the opinion of a group of experts. Actually, the Delphi method exist in two forms [74, p. 5]:

- Delphi Exercise
- Delphi Conference

The 'Delphi Exercise' form is formerly known as paper and pencil. In this particular form, a small team creates a questionnaire for a large group of participants. It is not known if all of these group are stakeholders. The assumption is the following; Stakeholder will reply to this questionnaire. The questionnaire in the first step is rather simple and should distinguish if the participant is a stakeholder or not. After the first response, analysis will review the answers, summarize it and prepare a further, more specific, questionnaire. Usually the responders have at least one possibility to reevaluate their answers. The 'Delphi Conference' make usage of computer which replaced the reviewer team. This computer will summarize the answers and will carry out the results. The advantage of this method is that the delay between the questionnaires will increase to zero. The computer is possible to change the Delphi method to a real-time system. An appropriate definition of communication by analysts is a prerequisite of this method.

Brainstorming

Brainstorming is a technique which allows an individual to share their ideas with a group of people. The key for a successful brainstorming session is to provide an room free of criticism and create an area where ideas can be shown unrestricted.

Brainstorming is "A tool used by teams for creative exploration of options in an environment free of criticism." [75, p. 3]

This technique allows to break out of the usual doing and find new possibilities. It should generate new, may unconventional and half grown, ideas which can solve existing problems or create new opportunities. The benefits of brainstorming are [75, pp. 2]:

1. **Promote creativity**

   The way of thinking should be extended to cover up the whole problem or solution. A bunch of new ways can be identified.

2. **Create a large amount of ideas**

   All people should be encouraged to offer any idea which they can imagine. This enables to generate a lot of ideas in a short amount of time.

3. **Involve all participants**

   Every participant should take part of the brainstorming session and provide ideas. This can be accomplished by a nonjudgmental environment. Every idea of each participant is noted down.

4. **Promote ownership for the topic**

   If every participant is fully involved in the idea-development process, they are more interested to find an appropriate solution for that. The sense of responsibility increases and therefore participants will likely support the solution or action.

Brainstorming can be used to develop a large amount of ideas about problems, possible solution, opportunities, drawback of actions or future approaches.

Brainstorming Rules

To establish a pleasant ambience where the development of creativity is possible, some rules must be followed. These rules have to be known by each participant to allow a successful brainstorming session. The rules are:

1. Participation by each member. Every member should develop ideas, regardless if they are unconventional or stressful.
2. No conflicts – discussions, criticism, or complaints.
3. Create ideas based on other ideas of participants.
4. Write down all ideas so that everyone can see it.
5. Limit the brainstorming session.

6. Explain ideas. Every participant should understand what is meant by this idea. There shall no judgment about the idea only clarifying.

7. Connect ideas. Examine if ideas are presented multiple times and connect them.

4.5.8. Step 5. Get Stakeholder Input about Future Strategy

The fifth step takes care about the identified influenced stakeholder groups. Group representative will be invited for an assessment how does they think they will be influenced by the new ISS. Stakeholder input phase make usage of common reactive data collection techniques to gather input about future policy sets. Analysis can start after a selection of group representatives. If it is not possible to invite all representatives, a sample of people have to be chosen. The results, gathered from representative people, have to be generalized to all affected parts of organization. If the sample selection wasn't diverse, generalized data will only deliver information about a part of affected groups in organization [70, p. 48].

Sampling

Sampling is a technique which allow to make inferences about unknown aspects using statistical values. For example, an organization want to know which impact on productivity an ISO 27000 certification will have. Instead of a survey of every production plant which ever has implemented such standard, only a subset will be evaluated. The important fact is to group the production plants to stakeholder groups and identify how much samples are required. Sampling methods have the objective to define which sample will be included into analysis. Analysts want to prevent biased results by using appropriate sampling techniques. A randomization of samples increases the confidence in the result.

Sampling Methods

Sampling can be split in two main areas: (1) probability and (2) non-probability sampling techniques [76, pp. 127].

- **Probability**

  Every part has the same probability to be inserted in the sample, random sampling methods build a base. Techniques are random samples, systematic samples, stratified samples and cluster samples.

- **Non-Probability**

  Are not based on random selection. Techniques are convenience samples, purposive samples and quota samples.

Only samples with the same probability of usage are representative. The result will be that only probability sampling techniques allow valid designs. Non-Probability design does not allow to determine the probability of inclusion. A generalization of non-probability samples are not possible.

Sampling Stakeholder Groups

The scientifically justifiable sampling of stakeholder groups poses particular problems, as it is difficult and expensive to obtain a sampling framework for each group that allows probability sampling. In our ISO27000 example, it will not be possible to evaluate which affects have this certification on production environments. But how should be proceed? In these circumstances, analysts typically use targeted spot checks to select informants to take specific positions on specific topics. This technique allows analysts to collect data representing the spectrum, divergence and specificity of positions on a proposed measure.

Data Collection

The data collection process can begin after identification of sample informants. The data will be used to assess impacts of the future information security strategy on stakeholder groups. Only accurate used techniques can guarantee reliable data. In case of questionnaires; Questions should be asked in an structured way and requires and initial test. Observations and structured interviews can be accomplished with minimal training effort. One of the most effective techniques are focused interviews but require expertise and significant training. Data collection can occur with 3 different techniques: (1) reactive techniques, (2) observational techniques, and (3) unobtrusive techniques.

1. Reactive techniques require an interaction with informants to get information.

2. In the observation techniques, the actual behaviour patterns are observed and then evaluated. However, a key challenge for the researcher is to decide what to look for and how to decide what constitutes a certain behaviour.

3. Unobtrusive measures are measures in which the researcher does not have to intervene in the research context. Direct and participatory observations require the physical presence of the researcher. This can cause respondents to change their behavior to look good in the eyes of the researcher. A questionnaire is an interruption of the natural behaviour flow. Respondents may be tired of completing a survey or getting angry with the questions asked.

4.5.9. Step 6. Evaluation of influence and the significance of stakeholders

Influence signifies the strength of a stakeholder in the information security strategy. Stakeholders with a lot of power control key points in the strategy. Key points are budget, compliance or employee sat-

isfaction. These stakeholders can facilitate or complicate the development of the information security strategy. Key variables measure the power of stakeholders to influence the strategy and the position that these stakeholders have. Significant signifies the level of participation that these stakeholder wish. This is often based on the requirement of stakeholder to achieve strategic objectives. The level of significant indicates which priority is assigned to stakeholder requirements and concerns to the strategy. The relationships can be shown in a diagram which is based on potential risks and groups of stakeholders who needs to be addressed [71, pp. 130]. An example infcluence are shown on figure 4.12.

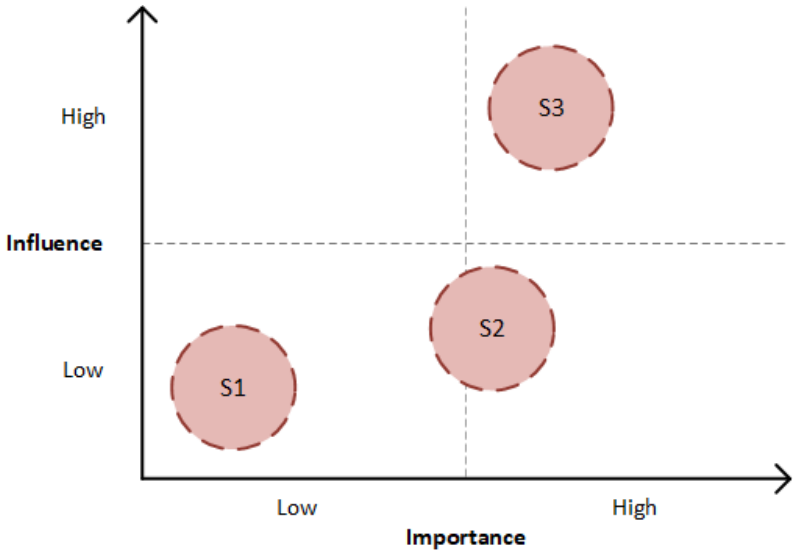

Figure 4.12.: Example Importance/Influence Analysis (Si=Stakeholder) [71, p. 131]

Evaluation how to best involve/access stakeholder

The last step is how to interact with stakeholders. Stakeholder where treated in different ways during strategic implementation. The picture below (4.13) shows how stakeholders can be sorted in a matrix to get a graphical overview.

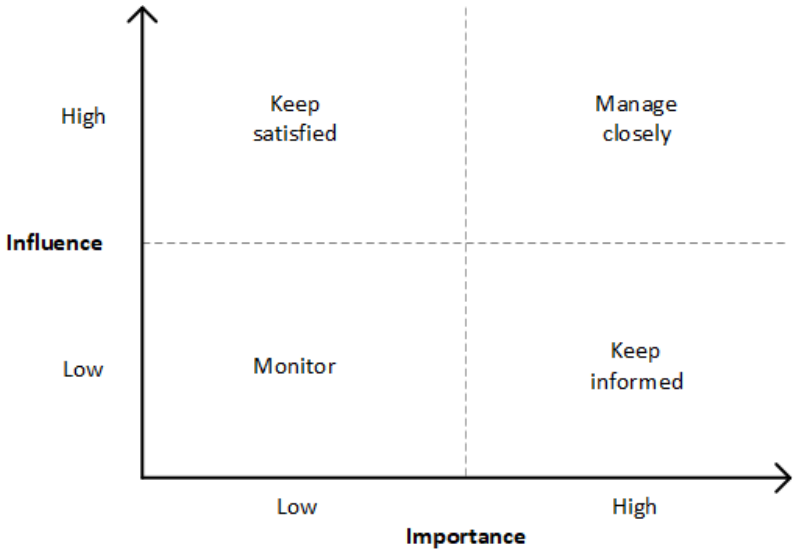

Figure 4.13.: Importance/Influence Matrix [71, pp. 132]

Importance

The importance relates to how likely it is that the stakeholder would like to be informed about the project and the process. It can also be perceived as a likelihood of conflict if the stakeholder is not involved [77, p. 9]. Stakeholder can be divided into 3 main categories:

1. Stakeholder have a direct impact or belief that there is an impact
2. Stakeholder have an indirect impact
3. It is not important for the stakeholder

Importance relies from a direct impact or believe that they are affected. This is the most important form of impact and set the level of interest to the highest values. Indirect impacted stakeholders have a smaller interest level as direct impacted stakeholder. They are may be affected by another stakeholder. Not interested or less to not impacted stakeholder have only to be notified about the project, depending on their level of power. Direct and indirect impacted stakeholders can set to a level of importance depending on their main objectives and how these affect ISS. All relevant interests of stakeholders should be monitored. They may change their opinion and this changes the level of importance.

Influence

Influence cover the possibility of stakeholder which can affect the future strategy. The following are generic categories of influence [77, p. 10]:

1. Power to cancel or start strategy

2. Possibility to slow down or push strategy
3. Can break or merge key relationships
4. No impact

The highest level of influence is the power to start of cancel the strategy, these essential stakeholders possess key positions. May these key influencers be less interested in this strategy but have the ability to change everything. Further, these key influencers can be biased by other stakeholder groups. Some stakeholder groups which have no direct impact on the project are able to slow down processes or push other groups to support the strategy. The last influencer group have the possibility to influence key relationships in a positive or negative way. These influencing categories can then be weighted according to their probability of use, whereby the potential for such use must always be monitored.

Higher Importance/Higher Influence

Stakeholders in the top right of figure 4.13 require the most attention, because they are interested in the strategy and have a major impact on its progress. A permanent communication is important to handle problems and keep them informed. Involving them in the decision-making process is likely to be necessary due to their influence and prioritization of the strategy. All required efforts should be fulfilled to make these actors feel that their voices are important and to show how their contribution is being used.

Higher Importance/Lower Influence

Stakeholder in the bottom right of figure 4.13 have to be observed regarding major problems and shall be informed about the status. They key action is to inform and give advice to these stakeholders.

Lower Importance/Higher Influence

First and foremost, this group (stakeholder in the top left of figure 4.13) must be kept informed so that it is not surprised by any part of the strategy. When these stakeholders are approached by less influential people, they are already on the same page with all stakeholders. However, care should be taken not to overburden these stakeholders, as this can easily lead to anger and avoidance of details. Regular updates and references to potential major conflicts are the primary forms of public relations that are needed. These stakeholders should be monitored if their interest grows.

Lower Importance/Lower Influence

Stakeholders with less or no points of contact reside in the bottom left of figure 4.13. These groups of these stakeholders should be monitored if their interests change. Information can be obtained from

this group if it can provide useful advice or opinions. Stakeholders should be informed about major progresses but not exposed with details.

4.5.10. Step 7. Report Results to Management Board

In the final stage of stakeholder analysis, analysts present their assessment of measures that could mitigate negative effects of proposed strategy. Recommendations are based on the information collected in preceding steps. The recommendations should be useful to decision-makers in clarifying the extent of changes needed to mitigate the negative impact of the proposed measures. Information on the impact that a measurement can have on stakeholders, combined with information on the extent of the changes needed to reduce the negative impact of the proposed measures, is important to decision-makers. It offers the possibility to adapt strategy, so that it can be integrated with minimal disadvantages [70, p. 38].

4.6. Applicability of Methodologies

This section provides an overview about the developed methodologies and their fields of application. The evaluation handles the following methods:

- SWOT Analysis for Information Security (SWOT-IS)
- Business Model Canvas for Information Security (BMC-IS)
- Ansoff Matrix / BCG Matrix for Information Security (A/BCG-IS)
- McKinsey 7S Model for Information Security (7S-IS)
- Stakeholder Analysis for Information Security (SA-IS)

The provided methods can be divided into two main groups; (1) Information security strategy developed by executive level or (2) employees with non/low-leadership position can participate during strategy development. This is formyl known as Bottom-Up or Top-Down approach. SWOT-IS and BMC-IS are mainly driven by employees because these methods require technical expertise. SWOT-IS delivers a baseline to which a ISS can be built, BMC-IS on the other hand analyze a specific risk and allow strategic decisions based on this particular risk. An essential benefit of BMC-IS is that it provides a cost estimation. A/BCG-IS, 7S-IS and SA-IS are classical Top-Down approaches which allows different perspectives. A/BCG-IS delivers the possibility to map business values against a set of risks. This allows information security decisions based on corporate strategy objectives. 7S-IS goes one step further with an analysis of organizational values. These model is oriented to an information security vision which

represent the ideal state where corporation want to be. If the management have already a ISS in place or already defined a draft, SA-IS enables the possibility to verify if this strategy has the intended affects. SA-IS analyze the stakeholder and shows unintended effects. The results are summarized in table 4.5.

	SWOT for IS	**BMC for IS**	**A/BCG Matrix for IS**	**McKinsey 7S Model for IS**	**Stakeholder Analysis for IS**
Analysis Target	Situation Analysis	Analyze specific risk	Analyse risk to business success	Analyze IS business env.	Evaluate IS strategies related to their impact
Analysis Approach	Technical Summary	Risk Based	Risk Based	Vision Based	Stakeholder Based
Analysis accompl. by	Technical Analysis	Org. Analysis	Mangement Analysis	Management Analysis	Stakeholder Analysis
Bottom-Up / Top-Down	Bottom-Up	Bottom-Up	Top-Down	Top-Down	Top-Down
Possible Initiator	Teamleader	Risk Management	Management	Management	Management

Table 4.5.: Comparision between Methodolodgies

5. Case Study

This case study of a yogurt lid manufacturer serves as an illustration of information security methodology applicability. It examines how developed methodologies can be applied to a fictive company. The company is based on my personal experience in working of production environments for several years. The different models should provide a solution that meet these specific requirements and should introduce how these methods can be used in an environment.

5.1. The Yoghurt Lid Manufacturer

YLM Ltd. is, as already estimated in the name, a manufacturer of yogurt lids. It sells lids globally around the world and have production plants around the world with about 10.000 employees (70% production worker). YLM will be supported by a centralized IT which deliver services to their plants. YLM use fully automated internal methods to produce lids and heavy rely on their privacy. Competitors, such as chinese manufacturer, are in strong competition to YLM, but have a lack of knowledge in lid manufacturing. Currently every knowledge carrier has to sign an NDA (Non Disclosure Agreement) that he/she will not disclosure internal methods. IT controls access to documents. There are no further information security controls in place. Risk department detected that YLM heavily relies on information and identified information disclosure as main risk. There is a plan for an information security strategy to mitigate these risks. Different methodologies should be considered to define information security strategic objectives.

5.2. SWOT Analysis

5.2.1. Part Analysis

Confidentiality

S: Permission grant/revoke centralized	W: External user permission delegation undefined
O: Information classification	T: Information Disclosure

Table 5.1.: SWOT Confidentiality

YLM discovered that it is a strength that their permissions will be centralized granted and revoked. A weakness is an undefined handling of external user permissions. They see information classification as an opportunity for the organization to separate sensitive data from public. Information disclosure was identified as threat for the organization.

Possession or Control

S: Physical servers stored in two locations	W: Unencrypted hard drives
O: Biometric scanners for access control	T: Access control isn't in place

Table 5.2.: SWOT Possession or Control

YLM recognized that their servers are located in two locations and not distributed around the globe. Possession or Control affect only two sites. If someone can access these locations, hard drives can be stolen and the containing data is not encrypted. Organization identified that access control via biometric scanner can be an opportunity instead of a key. Further there is no data center access management in place, that means: Nobody knows who have access to corporate data center.

Integrity

S: People who can modify documents are known	W: —
O: Enable change tracking on documents	T: Changes to documents cannot be tracked

Table 5.3.: SWOT Integrity

It is possible to figure out which employees have access to which data, but there is room for improvement. For example: Currently there is no document change tracking in place. YLM identified that

undocumented changed to documents opening room for fraud and disguise.

Authenticity

S: Source of document are stored as attribute	W: Digital Signatures are not in place
O: Define document requirements for author	T: Authors of documents can be adapted without any change tracking

Table 5.4.: SWOT Authenticity

The initial author will be stored as attribute of each file, but signatures are not in place. It cannot be determined if a document may be edited by another person. An opportunity can be a policy that request a set of an author for each document. A threat of authenticity is that authors of documents can be adapted without authors knowledge. Knowledge can be stolen from others and masqueraded as own idea.

Availability

S: Synchronously storage system in two datacenters are in place	W: No knowledge about storage system available inhouse, highly dependent on external partner
O: Reduce complexity, have a look at software defined storage	T: Only one virtual server provides data access

Table 5.5.: SWOT Availability

The strength of YLM is the synchronous storage of data in two datacenters. Data are still available if one datacenter is broken down. The drawback of this solution is their complexity and limited knowledge inhouse. YLM relies in cases of storage issues on partner and cannot deal with issues. Corporation identified new software defined solutions as opportunity to reduce complexity. Data is available on storage but will be provided with a single virtual instance. If this instance is not available, data is not accessible.

Utility

S: Most data can be shown with common office tools	W: Backup only occurs on weekly basis
O: Enable shadow copies to keep data utility in case of deletion	T: Data can be encrypted and will be useless

Table 5.6.: SWOT Utility

Most of the data at YLM are stored in common office formats. Data can nearly be viewed everywhere. In cases of a data loss, only a weekly backup is available. An opportunity that ensures utility will be shadow copies of data (formal known as snapshots). The main threat is ransomware, if data gets encrypted, it will be useless for corporation.

5.2.2. TOWS Summary

The TOWS summary shows a merge of all swot analysis in one big picture.

YLM Summary Analysis	STRENGTHS of YLM	WEAKNESSES of YLM
	1. Permission grant/revoke centralized 2. Physical servers stored in a central location 3. People who can modify documents are known 4. Source of document are stored as attribute 5. Synchronously storage system in 2 datacenters are in place 6. Most data can be shown common office tools	1. External user permission delegation undefined 2. Unencrypted hard drives 3. Digital Signatures are not in place 4. No knowledge about storage system available inhouse, highly dependent on external partner 5. Backup only occurs on weekly basis
OPPORTUNITIES FOR THE YLM 1. Information classification 2. Biometric scanners for access control 3. Enable change tracking on documents 4. Define document requirements for author 5. Reduce complexity, have a look at software defined storage 6. Enable shadow copies to keep data utility in case of deletion	• Information shall be trackable, classified and only accessible by users with authorized permission • Establish process for access management of data center	• External users shall only have access to classified and approved documents • Enable document versioning. History shall be available unlimited.
THREATS FACING THE YLM 1. Information Disclosure 2. Access control isn't in place 3. Changes to documents cannot be tracked 4. Authors of documents can be adapted without any change tracking 5. Only 1 virtual server provides data access 6. Data can be encrypted and will be useless	• Every permission delegation have to be recorded and approved • Data access shall be available 99,99% during production hours[24x5] • Establish solution for prohibiting data manipulation	• Establish full backup on daily basis • Establish SLA Agreement with partner for supporting storage system • Official documents have to be explicit assigned to corporation (digital signatures)

Figure 5.1.: TOWS Analysis

5.3. Business Canvas Model

Example: Risk - Information Disclosure

5.3.1. Model

<table>
<tr><th>KEY PARTNER</th><th>KEY ACTIVITIES</th><th>VALUE</th><th>CUSTOMER RELATIONSHIP</th><th>CUSTOMER</th></tr>
<tr><td rowspan="2">Key Partners ABC have experience is information security management systems

Partners deliver knowledge how to build a secure information lifecycle regarding to ISO 27000</td><td>Evaluate current system

Set up plan for an Information Security Management System(ISMS)

Evaluate partner</td><td rowspan="2">ISO 27000

Reduction possible ways that sensitive data leave company

A defined process which protect information</td><td>Project marketing through intranet
Security trainings</td><td rowspan="2">YLM Ltd are customer

User who can access corporate production methodologies require most protection</td></tr>
<tr><td>KEY RESOURCES
External partner
Internal security manager
IT Operations</td><td>CHANNELS
Intranet
Direct contact to leadership</td></tr>
<tr><td colspan="2">COST STRUCTURE
Estimated tool costs X €
External support Y €
Implementation costs Z €
Maintenance costs W €</td><td colspan="3">RISK
Important data that are identified as business critical assets are discovered by competitor or gained public
If important data get public, continued existence of organization are precarious.
Potential impact cost X €</td></tr>
</table>

Figure 5.2.: BMC-IS Analysis

RISK

Company YLM have a risk regarding to information disclosure received from its risk department and try to evaluate a business model to mitigate this risk. The risk is critical and can have effect of the existence of organization. These risks can be divided into two categories:

- Human Error

  A human was the reason for information disclosure. For Example; Accidental release of sensitive data or improper software protection of sensitive data (data is not marked as sensitive).

- Software Error

  Attacker gained access to systems through software bugs. For Example: Privilege escalation, exploits or trojans.

This model is focused on Human Errors.

CUSTOMER

Referring to the value (ISO 27k), YLM Ltd. is defined as scope for certification. That means, YLM is the customer. Not every employee is directly affected from certification. Most of the production worker have no access to sensitive information about production methods and have no corporate user to access files. For Example, a forklift driver is not affected. Relating to risk and value, model is focusing on employees as weakest point. Organization identified all employees which can theoretically access sensitive data as

customers. Employees who have access to sensitive data are identified as people who require special protection. These people possess the most risk regarding to their privileges.

VALUE

Organization want to mitigate risk (information disclosure) with an implementation of ISO 27000 to identify and control sensitive data. Organization want to have a process to protect sensitive data. The main goal is to know which employees have access to which files and how sensitive is the content. Further there should be a process how permission delegation is managed. Only specific persons should be able to allow access to sensitive data.

CUSTOMER RELATIONSHIP

YLM recognized that such implementation project has to be sold to their employees to increase probability of success. Because there are a lot of different employees identified as customer, a stable relationship has to be established. Organization decided to do that via a project marketing site on its intranet. This site should sensitize employees about information security and inform what is planned. Further, YLM offers security trainings to raise employees' security attitude.

CHANNELS

Intranet is focused to be the main communication channel to customers. Due to the fact that it isn't possible to communication direct to each employee an broader communication channel is required. Additional leaderships will be informed separately to ensure that manager have the ability to support their employees regarding security considerations.

KEY ATIVITIES

Currently there is no Information Security Management System (ISMS) in place, so there is no status quo which provided a basis. One key activity is to evaluate the current system regarding to ISO 27000 requirements and check how certification can be accomplished. A further important step is partner evaluation. At the moment, there is no or less security experience available in organizations IT department and an partner for how ISO 27000 works is mandatory. With this partner, it should be possible to set up a plan how an ISMS for organization can be integrated.

KEY RESOURCES

Organization identified external partner, internal security manager and IT operations as key resources. External partner provides the knowledge how to do it. Internal security manager serves as communication channel between organization and external partner. IT operations will maintain the ISMS continuously.

KEY PARTNER

A partner with deep knowledge about ISO 27000 was chosen and identified as key partner which supports key activities such as set up a plan for implementation.

COST STRUCTURE

Organization estimated principal costs in four categories:

- Tool – Which is required to handle ISMS
- Support – External partner costs for consulting
- Implementation – Costs related to implementation in organization
- Maintenance – Costs for keep system running

Possible outcomes can be:

- Costs highly depend on external partner; Further investigations have to be accomplished before a qualitative answer about costs can be taken.
- Mitigation model is adequate. Strategic objective: Implementation of an information security management system as defined in ISO 27000 series.
- Costs are too high, model should be adapted.
- Customers are not able to handle this value, awareness trainings regarding to information security are required before.
- Not enough internal key resources. IT employees are not familiar with information security management systems and employees are overloaded. Additional staff required.

5.4. Adapted BCG/Ansoff Matrix

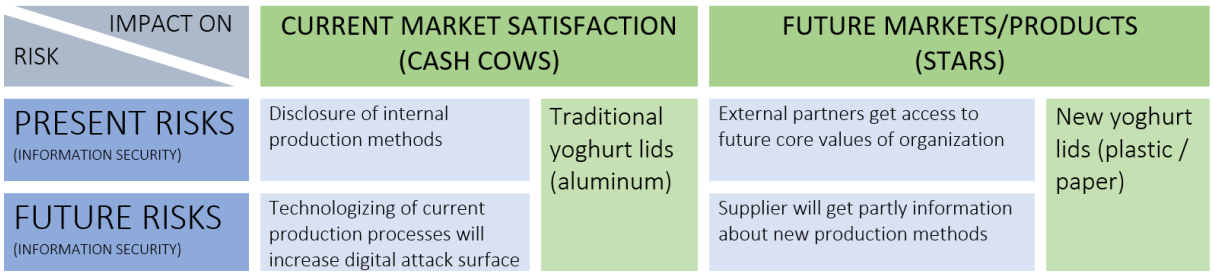

Figure 5.3.: Adapted BCG/Ansoff Matrix

As well-known Yoghurt Lid manufacturer, YLM core competences are producing traditional yoghurt lids, which contain aluminum. Top management identified this as cash cow of YLM Ltd. Further management recognized that lids, consisting of plastic or paper will guarantee future success. Research and development in this area is a strategic business objective. This objective will be placed under stars. After identifying stars and cash cow, current existing risks (identified by risk management), will be placed as present risks. Only risks which can have an substantial negative impact on stars or cash cows will be chosen. These risks should carry out on which current information security parts business success relies. YLM identified that disclosure of production methods can interfere current business objectives. During development of future technologies and methodologies for plastic/paper production, YLM heavy relies on external partners. These partners will have access to core values of YLM, therefore internal knowledge will leave the organization. In the last step, YLM defined that one important future risk against current cash cows is industry 4.0. This digitalization of production can lead into increased attack surface of production environment. The border between office and production will be softened. Devices from production have to communicate with multiple servers, remote offices, cloud services and so on. Smart devices will control production and heavy rely on their information which are used to make decisions. A risk regarding to stars will be that supplier, which support production, have knowledge of how future methodologies work. Further, required materials, machines and special construction are provided by external. This allows external to get a deep look how production systems work at YLM. External partners can use this knowledge to support competitors.

5.5. Adapted Version of 7S Model

5.5.1. Model Completion

YLM, as international packaging company, use 7S model as basis of their information security strategy. As first step, an information security vision is defined:
YLM as a continuously growing company, a leader in flexible packaging business, with international presence, information security is part of our organizational culture. Information security support top-quality services, offers our employees opportunities to increase their knowledge, thus guarantees a secure handling of data.

IS STRATEGY

Currently there is no information security strategy in place, therefore IS strategy remain empty.

IS STRUCTURE

Structure of information security department is defined as following picture:

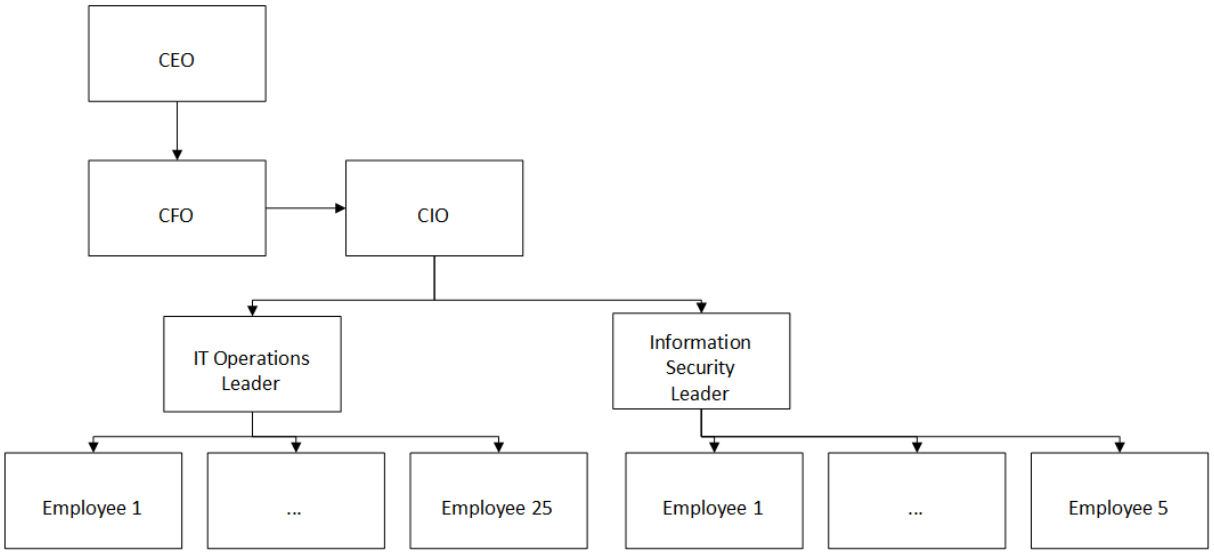

Figure 5.4.: Adapted 7S Model

Information security department is no field office, in this structure it is placed under CIO. This means in effect, CIO have to deal with information security topics and typical IT operations activities. If IT budget is defined globally, information security department have always to show up information security risks to prove their right to exist. CIO decide how important information security will be treated, less experience CIOs underestimate the importance of information security.

IS SYSTEMS

Main processes:

- Permission delegation will be done in a structured order and always require an approval. Every delegation will be recorded.
- Education of IT employees to detect possible data leaks.
- Integrated evaluation of each case in ITSM system, which can violate internal security policies.

IS SKILLS

Information security department uses global recognized certifications as skill-levels. Therefore, they use a matrix with accomplished certifications and educate their stuff.

Employee	Capabilities
Information Security Leader	CISA, CISM, CRISC, ACS, CSSGB, SSBB, PSCU-FS
Employee 1	CGEIT, CISA
Employee 2	CISA
Employee 3	CISSP, CISA
Employee 4	GIAC, CAP
Employee 5	CISA

Table 5.7.: 7S Model Skills

IS STYLE

Information security knowledge is concentrated in IS department. Executive Board receive information security trainings annually. This guarantees a minimum level of information security awareness. IS leader have to extract knowledge from his employees to know which threats are present and set the appropriate steps. As direct contact to the board, IS leader have to inform CIO about IS relevant topics to ensure that information security is placed at executive management.

IS STAFF

Information security lead must ensure that IS employees have the ability to visit trainings. A training program is established in cooperation with human resources department. It is the function of IS leader to keep motivation high to enable a positive culture. Benefits will be offered to motivate staff.

5.5.2. Designing Ideal Information Security Organization

In an ideal organization, every information assets are classified and will be protected with the appropriate level. Information flows are controlled and recorded. Sensitive data locations are identified and complain with regulatory requirements. IT infrastructure provide solutions which prohibit undesired access of information and protect them in cases of disaster. Periodically reviews of it infrastructure and used software guarantee an appropriate level of protection. All employees are aware of information security and can report potential issues to IS department. Executive board provide all necessary resources to increase the level of protection of assets within organization. Executive board force information security to prevent an inappropriate treatment level of information due to lack of resources. Future projects will

be evaluated regarding information security and information security department have a seat in project team.

5.6. Example Information Security Strategy

5.6.1. Mission

Provide unique and high-quality lids to our customers.

5.6.2. Vision

Be the best lid manufacturer with delivering an economic product.

5.6.3. Governance

The increasing requirement for a secure workplace and further to protect corporate information has resulted in an information security department. A Chief Information Security Officer (CISO) was hired to create an information security program with the goal to protect all corporate data on all sites. The CISO will be responsible to reach objectives defined in this strategy. To successful achieve strategic objectives, an alignment with business goals is required. The following positions are participated in the decision-making process:

- Chief Information Officer (CIO) – The CIO is responsible for the holistic management of global IT, which includes information security.
- Chief Information Security Officer (CISO) – The CISO is responsible for all topics related to information security, this includes IT security and organizational security.
- Chief Finance Officer (CFO) – The CFO is responsible for all major finance decisions and the IT is subordinated to this position. In this role strategic decisions have to be approved by this position.

The information security department is instructed to schedule reports on a monthly basis. These reports include all security initiatives and their progress. Further CISO is encouraged to brief CIO/CFO on a regular basis about the overall security status of the company.

5.6.4. Strategic Objectives

YLM encountered information security inadequacies and therefore defined objectives to counteract these evolutions. In assumption of adequate resource usage, the objectives can be implemented in the following 1 to 3 years. These objectives will be accompanied by one or multiple strategic initiatives. The

strategic objectives related to information security department are:

General Data Protection Regulation (GDPR) – To comply with legal requirements, a program to establish a GDPR compliant organization shall be initiated. In this program a link between all relevant departments and information security will be established to gain support for implementation.
Protection of corporate information assets - Our information's are bundled and concentrated in IT systems. These data form the basis of our success. A data classification and protection system must enforce corporate protection of internal knowledge.
IT Risk Management – Extend corporate IT risk management and integrate it into enterprise risk management. Focus on risk identification, management and implementation of controls to mitigate such risks.
Improve IT security – A corporate it security program shall be established which evaluate current IT security status and enable the possibility to detect inadequacies. IT security have to be threaten as continuous process which protect us against cybersecurity threats. Countermeasures should be recognized and implemented.
Industrial Security – Establish security measurements which protect industrial IT systems and enable continuous production. Create communication channels between IT and industrial developers to increase production security.

5.6.5. Strategic Initiatives

Initiative 1 – Data Classification, Protection of Assets, Policy

Enables Objective – Enables that corporate information, which can have negative impacts, are protected.
Description – Develop an classification model and identify assets which contains sensitive data. This classification model shall be based on ISO/IEC 27001. Corporate policies shall establish a ruleset how to handle such sensitive data. Further establish a technical protection and monitoring of sensitive corporate assets.
Key Benefits

- Clear baseline how to handle with information assets
- Technical restriction which enables additional protection
- Developed according to an international standard

Initiative 2 – Integration of Risk to Global Risk Management

Enables Objective – Allows board members to get an overview of IT risks and set appropriate counter-

measures

Description – Integrate corporate risk management key performance indicators (KPI) into IT risk management and adapt risk measurement to comply with corporate standards. Establish a group processes related to risk management to ensure appropriate reporting.

Key Benefits

- Appropriate reporting structures
- Global risk map
- Share knowledge between risk management departments

Initiative 3 – Disaster Recovery and Continuous Operation

Enables Objective – Allow adequate protection of IT assets and regulatory compliance with GDPR.

Description – Develop, monitor and maintain a plan in case of a disaster scenario. Operation of IT systems shall be possible even in disaster cases. The expected results are a disaster recovery plan and disaster recovery policy.

Key Benefits

- Preparation in case of disaster which allows to continue provide core services
- Allows to recover all systems in an appropriate time frame

Initiative 4 – Extend IT Risk Management

Enables Objective – Expand the coverage of IT security risk management in the field of information security.

Description – Develop, verify and launch information security risk identification methods which allows to extend the degree of coverage related to information security. Assess these risks and ensure adequate reporting structure.

Key Benefits

- Enables a proactive management of risks
- Ensure that information security risks are known by management
- Provide a standardized method of risk identification and assessment

Initiative 5 – Vulnerability Management

Enables Objective – Ensure a continuous health check of all IT systems.

Description – Establish a department which monitors all IT systems referring to patching, malware

and security leaks. This allows an overview of the health state of all corporate it systems. Further communication channels will be created between security and functional department to enforce corporate patch management policy.

Key Benefits

- Ensure that all IT systems are up to date
- Mitigate the possibility of 'forgotten' IT systems which are not patched
- Reduce the shadow IT systems

Initiative 6 – Information Security Awareness Training

Enables Objective – Ensure an adequate awareness level of corporate employees which handle with information. This enables to lower IT security risk related to human errors.

Description – Establish and Security Awareness Training related to ENISA Guide[1] (How to raise information security awareness). A global corporate level of information security awareness shall be developed. This contains continuous adapted training for specified target groups.

Key Benefits

- Higher corporate information security awareness
- Less security incidents

Initiative 7 – Protect Industrial Production

Enables Objective – Ensure protection of industrial environment.

Description – Define, manage and control intersection points between IT and industrial environment. Establish a security concept which controls the communication between these both worlds. Implement security concept with the focus of less production interruption.

Key Benefits

- Fixed defined intersection points between IT and industrial environment
- Only allow known communication between these both worlds

5.6.6. Threats and Vulnerabilities

Threat 1 – Loss of Knowledge

YLM as global industrial company consists of a serious amount of people which never got in contact

[1] https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport

with information security related topics. These group of people hold considerable amount of sensitive information which are required on their daily work. A loss of these knowledge can have serious impact on productivity and quality of our products.

Threat 2 – Shadow IT

Industrial departments are built before IT was established. It cannot be precluded that production environment is free of non-managed IT equipment. Unmanaged devices can create backdoors for potential attackers.

Threat 3 – Security vs Usability

IT Security, regardless if organizational or technical, are always in conflict with usability. Additional security measures increase the potential rejection of using IT systems in a security way. End-User should be able to handle products to fullfil their daily work.

Threat 4 – Sabotage of Industry

As main source of income, production environment is business critical. Digitalization melt IT and industrial together, this increase the attack surface of industrial systems. An attack against our productive systems can lead into production downtime or in worst case, employees could be injured.

5.6.7. Performance Measures

General Data Protection Regulation (GDPR)

Key Performance Indicators:

- % of companies which have a defined data officer
- % of companies which have a complete procedural directory
- % of companies which have privacy by design implemented
- % of companies which have privacy by default implemented
- % of companies which have processes regarding duty of disclosure

Protection of corporate information assets

Key Performance Indicators:

- % of companies which have fully implemented data classification policy
- % of companies which have fully implemented technical software for asset protection
- % of companies which have implemented a disaster recovery plan

IT Risk Management

Key Performance Indicators:

- % of critical business services which are not covered by risk analysis
- % of critical information security incidents which are not reported to board
- % of critical information security risks which are not reported to board

Improve IT security

Key Performance Indicators:

- % of systems which are not covered by vulnerability management
- % of users which are not trained by security awareness program
- % of business-critical IT security equipment which are not reviewed annually

Industrial Security

Key Performance Indicators:

- % of intersection points which are secured and reviewed annually
- Hours of meetings between industrial and information security department
- % of intersection points which are not covered by industrial security concept

5.6.8. Values

We are YLM, an industrial company which manufactures high-quality products for our customers. As result of the global development of industrial digitalization, information security becomes business-critical. The importance of storage knowledge digital and share it enables a wide range attack surface which have to be covered. Our knowledge, which allows us competitive advantage, shall be protected and maintained.

6. Conclusion

The core idea for an ISS is to protect information, but not only information, it concerned with the protection of intellectual property which are built on information. This master thesis shows that it is entirely possible to set up a strategy, even if data located in a virtual environment and there are more possibilities to share it as with a telegraph. First of all, information security has to be sold. Chapter 2 provides you information about the hard facts. What is information security and why is it used for? You have to recognize that knowledge is power and the protection of these knowledge has to be priority number one. Information is an asset with a euro sign and also the handling should be accordingly. The administration of information should be equal to physical assets and enable a finance aspect. With these knowledge, explanation of why you require a strategy shouldn't be a problem anymore. Further, to answer the research question if existing models can be used for ISS development; Yes. This can be accomplished with an adaption of the objective of a model (like SWOT-IS analysis) or through a redesign of a model (like BMC-IS). It is also possible to create something new, as for example with the merge of Ansoff and BCG matrix. Another example is McKinsey 7S model which was adapted to support information security but the initial core idea to follow a vision is still the same. In opposite to the previously mentioned models provide a stakeholder analysis a complete different view. This analysis enables an impact analysis which is only partially covered by other models. Each model has different advantages and field of application. Section 4.5 show which model should be used in which situation. Another important cognition is that these models can be combined. For example, if you have a vision which your IT follows but you want to take care of specific risk. In this case you can combine McKinsey 7S-IS model with BMC-IS or A/BCG-IS matrix. The application of these models is always a crucial point, how can that be accomplished in my corporation? The example company YLM 5.1 should serve as a reference example. The building blocks give an advice how an ISS can look like. The core statement of this chapter is well known; Plan(mission, vision, strategic objectives), Do(strategic initiatives), Check(threats and vulnerabilities, performance measures), Act(governance, values). As the most important point I would like to mention again that the goals must be made measurable. If you cannot measure it, you cannot reach it. Equipped with this knowledge, it is possible to create your own ISS. Last but not least, an example strategy is designed and provide an overview how such things can look like.

A. Cyber Crime Breaches

List of cyber crime breaches:

- http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html
- http://www.reuters.com/article/us-usa-crime-cybercrime-idUSBRE9AH0YZ20131118
- https://www.bloomberg.com/news/articles/2017-03-16/here-s-how-russian-agents-hacked-500-million-yahoo-users
- http://www.computerweekly.com/news/450403530/US-Navy-breach-highlights-third-party-cyber-risk
- https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record
- http://www.wired.co.uk/article/85-million-accounts-dailymotion-hacked
- https://www.theregister.co.uk/2016/11/10/tesco_bank_breach_analysis/

B. Glossary

7S-IS	McKinsey 7S Model for Information Security. 60, 79
A/BCG-IS	Ansoff Matrix / BCG Matrix for Information Security. 60, 79
BCG	Boston Consulting Group. 38, 40, 41
BMC	Business Model Canvas. 29
BMC-IS	Business Model Canvas for Information Security. 60, 67, 79, 83
CAPEX	Capital Expenditure. 35
CFO	Chief Finance Officer. 73
CIO	Chief Information Officer. 73
CISO	Chief Information Security Officer. 42, 73
EMM	Enterpise Mobility Management. 21
GDPR	General Data Protection Regulation. 51, 74, 75, 77
IS	Information Security. 43–45, 70, 72
ISMS	Information Security Management System. 68
ISRM	Information Security and Risk Management. 10
ISS	Information Security Strategy. v, 1–4, 9, 10, 23, 28, 36, 49–53, 55, 58, 60, 61, 79
IT	Information Technology. 1, 4, 6, 7, 10, 21, 51, 62, 68, 69, 71–79

ITSM	Information Technology System Management. 71
KPI	Key Performance Indicator. 75
NDA	Non Disclosure Agreement. 62
NFC	Near Field Communication. 21
OPEX	Operational Expenditure. 35
SA-IS	Stakeholder Analysis for Information Security. 60, 61
SBU	Strategic Business Units. 38, 40
SMART	Specific, Measurable, Achievable, Relevant, Time bound. 19
SPM	Strategic Performance Measurement. 21
SWOT-IS	SWOT Analysis for Information Securit. 60, 79
USP	Unique Selling Proposition. 24, 38
YLM	Yoghurt Lid Manufacturer Ltd. - Sample Company. 62–65, 67, 68, 70, 73, 76, 78, 79

List of Figures

List of Tables

Bibliography

[1] J. J. Fahie, A History of Electric Telegraphy, to the year 1837. London: E. & FN Spon, 1884.

[2] R. M. Lenka Fibikova, "Threats, Risks and the Derived Information Security Strategy," 2012.

[3] D. Parker, "Our excessively simplistic information security model and how to fix it," ISSA Journal, pp. 12–21, 2010.

[4] R. Casadesus-Masanell and J. E. Ricart, "From strategy to business models and onto tactics," Long range planning, vol. 43, no. 2, pp. 195–215, 2010.

[5] J. Magretta, "Why business models matter," 2002.

[6] ISO, "Information technology — security techniques — code of practice for information security management," International Organization for Standardization, Standard ISO/IEC 27002:2005, Jun. 2005.

[7] ISACA, "Basic Foundational Concepts Student Book: Using COBIT® 5," Feb. 2014.

[8] U. G. P. Office, "Public Printing and Documents / Coordination of Federal Information Policy / Information Security / Definitions," 2014. [Online]. Available: https://www.gpo.gov/fdsys/pkg/USCODE-2014-title44/pdf/USCODE-2014title44-chap35-subchapII-sec3552.pdf

[9] G. Pender-Bey, "The parkerian hexad."

[10] G. D. P. Regulation, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46," Official Journal of the European Union (OJ), vol. 59, pp. 1–88, 2016.

[11] A. Nitaj and D. Pointcheval, "Progress in cryptology–africacrypt 2011," in AFRICACRYPT 2011-4th International Conference on Cryptology in Africa, vol. 6737. Springer, 2011, p. 387.

[12] R. B. Parker, "A definition of privacy," 1974.

[13] R. L. B. DETMAR W. STRAUB, SEYMOUR GOODMAN, "INFORMATION SECURITY POLICY, PROCESSES, AND PRACTICES," 2008.

[14] M. K. Harold F. Tipton, "Information Security Management Handbook, Fith Edition," 2004.

[15] Gartner, "Gartner survey of more than 3,000 cios confirms the changing role of the chief information officer," 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3810968

[16] CapGemini, "The information opportunity report," 2008. [Online]. Available: http://www.eurim.org.uk/activities/ig/voi/The_Information_Opportunity.pdf

[17] C. Higson and D. Waltho, "Valuing information as an asset," White paper, SAS, London, UK. Google Scholar, 2009.

[18] D. Laney, "Infonomics: the economics of information and principles of information asset management," in The Fifth MIT Information Quality Industry Symposium. Cambridge, vol. 9, 2011, p. 2.

[19] S. C. Dresley and A. Lacombe, "Value of information and information services," Tech. Rep., 1998.

[20] S. Park and T. Ruighaver, "Strategic Approach to Information Security in Organizations," 2008.

[21] ISACA, "COBIT® 5 for Information Security," 2012.

[22] S. Elky, "An introduction to information systems risk management," 2006.

[23] J. P. Pironti, "Developing an information security and risk management strategy," ISACA Journal, vol. 2, p. 28, 2010.

[24] P. Bowen, J. Hash, and M. Wilson, "Information security handbook: a guide for managers," in NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Citeseer, 2007.

[25] M. E. Whitman, "Enemy at the gate: threats to information security," Communications of the ACM, vol. 46, no. 8, pp. 91–95, 2003.

[26] D. W. Straub and R. J. Welke, "Coping with systems risk: security planning models for management decision making," MIS quarterly, pp. 441–469, 1998.

[27] S. Purser, "A practical guide to Managing Information Security," 2004.

[28] B. Evans, "The importance of building an information security strategic plan," 2015. [Online]. Available: https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/

[29] PWC, "Defending yesterday - key findings from the global state of information security survey 2014," 2014. [Online]. Available: http://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf

[30] O. O. MANAGEMENT and BUDGET, "Annual report to congress: Federal information security modernization act," 2016. [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf

[31] ISACA, "Cism review manual," 2012.

[32] E. I. Unit, "Why good strategies fail: Lessons for the c-suite," London: Economist Intelligence Unit Limited, 2013.

[33] B. Conerly, "3 strategic planning pitfalls," 2013. [Online]. Available: https://www.forbes.com/sites/billconerly/2013/08/15/3-strategic-planning-pitfalls/#5d969947136e

[34] H. Mintzberg et al., "The fall and rise of strategic planning," Harvard business review, vol. 72, no. 1, pp. 107–114, 1994.

[35] H. Mintzberg, "Rethinking strategic planning part i: Pitfalls and fallacies," Long range planning, vol. 27, no. 3, pp. 12–21, 1994.

[36] M. Pirtea, C. Nicolescu, and C. Botoc, "The role of strategic planning in modern organizations," Annales Universitatis Apulensis: Series Oeconomica, vol. 11, no. 2, p. 953, 2009.

[37] V. Dermol, "Relationship between mission statement and company performance," Annals of the Alexandru Ioan Cuza University-Economics, vol. 59, no. 1, pp. 321–336, 2012.

[38] J. A. Pearce and F. David, "Corporate mission statements: The bottom line," The Academy of Management Executive, vol. 1, no. 2, pp. 109–115, 1987.

[39] A. A. Alawneh, "The impact of mission statement on performance: An exploratory study in the jordanian banking industry," Journal of Management Policy and Practice, vol. 16, no. 4, p. 73, 2015.

[40] J. Hall, “How to create a content marketing mission statement,” 2013. [Online]. Available: https://www.forbes.com/sites/johnhall/2013/12/15/how-to-create-a-content-marketing-mission-statement/#2225d51a4aa0

[41] L. Sherman, “Corporate mission statements don’t really matter, unless you want to be a great leader,” 2017. [Online]. Available: https://www.forbes.com/sites/lensherman/2017/04/03/corporate-mission-statements-dont-really-matter-unless-you-want-to-be-a-great-leader/#27b950d32246

[42] AchieveIt, “The link between mission, vision, and strategy.” [Online]. Available: http://www.achieveit.com/wp-content/uploads/2014/02/The-Link-Between-Mission-Vision-and-Strategy.pdf

[43] S. Kantabutra and G. C. Avery, “The power of vision: statements that resonate,” Journal of Business Strategy, vol. 31, no. 1, pp. 37–45, 2010.

[44] H. B. Review, “When ceos talk strategy, is anyone listening?” 2013. [Online]. Available: https://hbr.org/2013/06/when-ceos-talk-strategy-is-anyone-listening

[45] K. International, “Your company vision: If it’s complicated, it shouldn’t be,” 2013. [Online]. Available: https://www.forbes.com/sites/johnkotter/2013/10/14/the-reason-most-company-vision-statements-arent-effective/#189bbbeb2dc7

[46] W. K. Brotby, Information security governance: guidance for boards of directors and executive management. Information Systems Audit and Control Association, 2006.

[47] G. T. Doran, “There’s a smart way to write management’s goals and objectives." and miller,” Arthur F. & Cunningham, James A" How to avoid costly job mismatches" Management Review, vol. 70, no. 11, 1981.

[48] D. Solow, “What is a strategic initiative?” 2016. [Online]. Available: https://www.esmgrp.com/blog/what-is-a-strategic-initiative

[49] M. F. Wanner, “Implement strategy by strategic initiatives with effective program and change management,” 2014. [Online]. Available: https://www.pmi.org/learning/library/strategic-initiatives-program-change-management-1466

[50] J. Evans, “Most companies don’t see strategic threats coming until it is too late – part 3,” 2013. [Online]. Available: https://www.vistage.com/research-center/growth-strategy/most-companies-dont-see-strategic-threats-coming-until-it-is-too-late-part-3/

[51] A. B. White and F. Lourdes, "Strategic performance measurement system charac teristics, outcomes, and performance," 6th Global Conferenceon Business & Economics, 2006.

[52] P. Micheli and J.-F. Manzoni, "Strategic performance measurement: Benefits, limitations and paradoxes," Long Range Planning, vol. 43, no. 4, pp. 465–476, 2010.

[53] G. Kormaris, "Swot analysis," 2009.

[54] C.-Y. Lai and W.-C. Liou, "A study on the swot analysis from knowledge point of view the case of the sijhih community university," Asian J. Inform. Tech, vol. 6, no. 5, pp. 538–543, 2007.

[55] R. G. Dyson, "Strategic development and swot analysis at the university of warwick," European journal of operational research, vol. 152, no. 3, pp. 631–640, 2004.

[56] N. R. R. LALITHA CHAVALI, DEVI PRIYA CHITTIPROLU, "Swot analysis," 2017.

[57] T. J. Chermack and B. K. Kasshanna, "The use and misuse of swot analysis and implications for hrd professionals," Human Resource Development International, vol. 10, no. 4, pp. 383–399, 2007.

[58] W. Gretzky, "Strategic planning and swot analysis," 2010.

[59] J. L. Thompson and F. Martin, Strategic management: Awareness & change. Cengage Learning EMEA, 2010.

[60] X. Wang, J. Zhang, and T. Yang, "Hybrid swot approach for strategic planning and formulation in china worldwide express mail service," Journal of applied research and technology, vol. 12, no. 2, pp. 230–238, 2014.

[61] I. Aslan and R. Bozkurt, "Strategic sustainable development and creating strategies from tows matrix at kipaġ group," 2010.

[62] P. Pitayachaval, K. Chittrakool, and W. Arjharn, "Integration of business model canvas (bmc) and quality function deployment (qfd) to design product," in Industrial Engineering and Applications (ICIEA), 2017 4th International Conference on. IEEE, 2017, pp. 76–80.

[63] W. Sammer, "Der business model canvas: Dein geschäftsmodell kompakt." [Online]. Available: https://ut11.net/blog/dein-geschaftsmodell-kompakt-der-business-model-canvas/]

[64] A. Osterwalder, "A better way to think about your business model," Harvard Business Review, vol. 6, 2013.

[65] MaRS, "Business model design," 2012. [Online]. Available: https://www.marsdd.com/wp-content/uploads/2012/12/Business-Model-Design-WorkbookGuide.pdf

[66] C. Schawel and F. Billing, "Die top 100 management tools," in Top 100 Management Tools. Springer, 2012.

[67] F. Haq, H. Y. Wong, J. Jackson et al., "Applying ansoff's growth strategy matrix to consumer segments and typologies in spiritual tourism,'," in refereed paper presented at 8th International Business Research Conference, 2008.

[68] P. T. Udo-Imeh, W. E. Edet, and R. B. Anani, "Portfolio analysis models: a review," European Journal of Business and Management, vol. 4, no. 18, pp. 101–117, 2012.

[69] M. M. Ravanfar, "Analyzing organizational structure based on 7s model of mckinsey," Global Journal of Management and Research: A Administration and Management, vol. 15, no. 10, pp. 6–12, 2015.

[70] W. M. Babiuch and B. C. Farhar, "Stakeholder analysis methodologies resource book," National Renewable Energy Lab., Golden, CO (United States), Tech. Rep., 1994.

[71] S. O. Saèd El Aoufi, Information security economics. The Stationery Office, 2011.

[72] E. Steve, "An introduction to information system risk management," SANS Institute InfoSec Reading Room. Available on-line at http://www. sans. org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204. Accessed March, vol. 16, p. 2011, 2006.

[73] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002.

[74] H. Linstone and M. Turoff, "The delphi method: Techniques and applications.[adobe digital editions version]," ISBN 0-201-04294-0. Retrieved from http://is. njit. edu/pubs/delphibook, Tech. Rep., 2002.

[75] U. Navy, "Handbook for basic process improvement, module brainstorming," 1996.

[76] D. T. Perumal, "Cmrm6103 research methodology/gmrm5103 research methods in competitive intelligence," 2009. [Online]. Available: http://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0021_22_research_methodology/CMRM6103_Research_methodology_10.pdf

[77] J. Prozzi, "Stakeholder analysis for value extraction projects," Tech. Rep., 2012.