Reporting on Cybersecurity Performance

Summary of Bachelor's thesis of

Diede Boerman
s1864750
IEM

October 13, 2020

Contents

1 Introduction **2**

1.1 Identification of problems . . . 2

1.2 Core problem . . . 2

1.3 Research methodology . . . 3

1.4 Research design . . . 4

1.4.1 Objectives and deliverables . . . 4

1.4.2 Research questions . . . 5

1.5 Current situation . . . 6

2 Theoretical framework **7**

2.1 Current situation . . . 7

2.2 KPI selection . . . 8

2.2.1 Theoretical perspective . . . 8

2.2.2 KPI selection from literature . . . 8

2.3 Data management . . . 11

2.4 Dashboard design . . . 12

2.4.1 User-friendly design . . . 12

2.4.2 Data visualisation . . . 13

3 Design and implementation **15**

3.1 KPI selection . . . 15

3.2 Data modelling . . . 15

3.3 Dashboard development . . . 16

4 Evaluation **17**

4.1 Validation . . . 17

4.2 Evaluation of objectives . . . 17

5 Conclusion **19**

5.1 Research Questions . . . 19

5.2 Company conclusion . . . 21

5.3 Recommendations . . . 22

A - Steps for selecting literature **25**

B - Selected literature **27**

C - Concept-Matrices **28**

1 Introduction

We have proposed and executed the thesis in cooperation with Company X. The research concerns the analyses of cybersecurity processes within the company and led to the creation of a dashboard. Because of confidentiality, we are not allowed to publish the actual thesis. Hence, we provide this summary in order to show the relevant steps taken during our research.

1.1 Identification of problems

Over the past years, internet based technologies have become an integral part of our lives. Along with this development, information security is becoming more important worldwide. Actors in society are capable of attacking IT infrastructure to damage or destroy computer networks or systems.

Cybersecurity has become increasingly common in recent years, and hence also in the operations of company X: the main activity of the company is identified to be part of a critical infrastructure that could result in severe social damage in the event of their failure or disruption. Cyberattacks can cause an interruption of operational services, which in turn can impose heavy costs and have a significant economic impact. For this reason, several programs and projects were introduced to guarantee continuity of the operations. The company aims to increase its resilience to protect the organisation against security threats.

The safety and security systems of the company are developed constantly. Projects are established to prevent and minimize cyber related problems. The company aims to increase awareness and knowledge regarding cybersecurity. Awareness is increased by accurate reporting of the cybersecurity processes.

The assignment proposed by the company is to create a dashboard to provide a clear overview of certain scores on Key Performance Indicators regarding cybersecurity. With clear insights management is aware and can provide a direction that is needed in order for the security programs to move ahead properly. With the overview, several departments will also be able to report the findings and tasks up to the higher organisational levels. In order to improve reporting, several indicators should be established. These indicators together must provide a proper overview of the cybersecurity processes.

1.2 Core problem

In this section, we map the identified problems and their relationships into a problem cluster (Figure 1). The cluster presents the problem context in a structured way and serves to identify the core problem [2].

We have decided the core problem to be that no accurate reporting regarding cybersecurity is provided for management. Measurements can be gathered on the performed analyses to identify dangers or other relevant findings regarding cybersecurity. Other indicators might

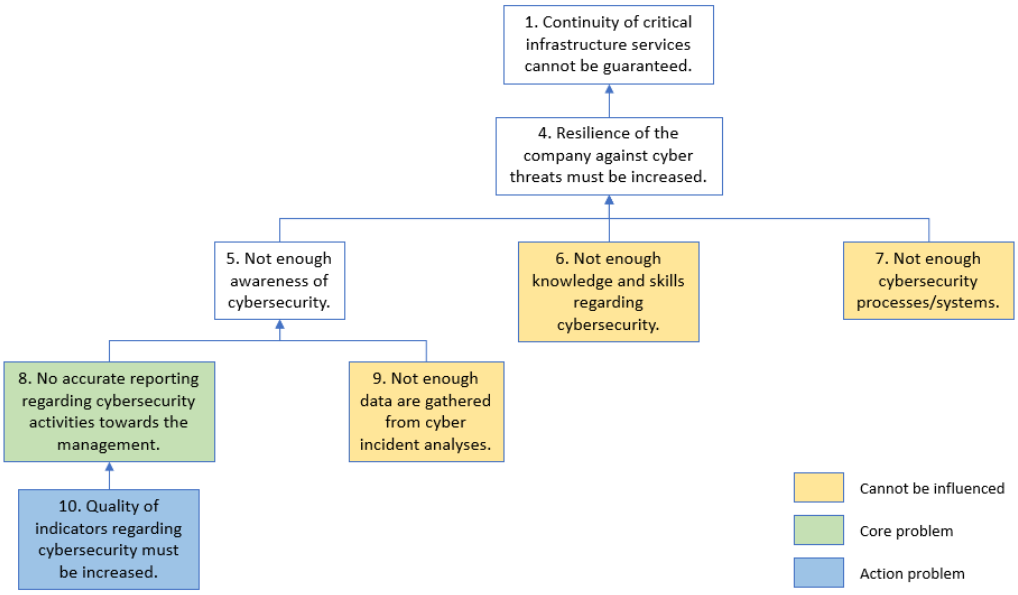

1. Continuity of critical infrastructure services cannot be guaranteed.
4. Resilience of the company against cyber threats must be increased.
5. Not enough awareness of cybersecurity.
6. Not enough knowledge and skills regarding cybersecurity.
7. Not enough cybersecurity processes/systems.
8. No accurate reporting regarding cybersecurity activities towards the management.
9. Not enough data are gathered from cyber incident analyses.
10. Quality of indicators regarding cybersecurity must be increased.
🟨 Cannot be influenced
🟩 Core problem
🟦 Action problem

Figure 1: Problem cluster.

be established about the activities related to cybersecurity. By defining indicators related to these measurements and processes, an overview of all important findings can be provided to the managers. The dashboard can serve as a tool to report on tasks and analyses towards the higher business levels. On the other hand the tool can be used to provide directions towards the security programs within the same business level. The assignment proposed by the company, to create a dashboard, will provide a clear overview of the insufficiencies, issues, risks and activities indicated within the systems.
Altogether, the indicators will improve reporting towards the higher business levels and directing towards lower or equal business levels. The action problem concerns the number of indicators regarding cybersecurity that must be increased. The main research goal is formulated as follows:

Determine key performance indicators based on the preferences of stakeholders and related to cybersecurity and portray the findings onto a dashboard in order to provide accurate reporting of the cybersecurity performance.

1.3 Research methodology

It is important to select the right research methodology, since it will be the foundation of the research. Within this bachelor thesis, we use the Design Science research methodology. Design Science is a research that applies knowledge to solve practical problems [14]. Design Science consists of two activities: designing an artefact that improves something for stake-

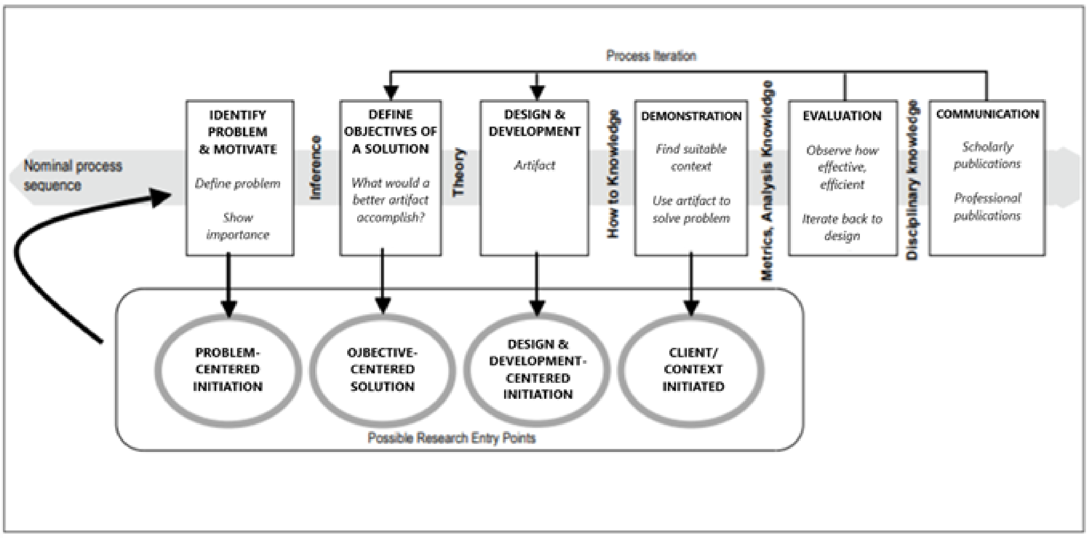

Process Iteration
Nominal process sequence
IDENTIFY PROBLEM & MOTIVATE
Define problem
Show importance
Inference
DEFINE OBJECTIVES OF A SOLUTION
What would a better artifact accomplish?
Theory
DESIGN & DEVELOPMENT
Artifact
How to Knowledge
DEMONSTRATION
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
EVALUATION
Observe how effective, efficient
Iterate back to design
Disciplinary knowledge
COMMUNICATION
Scholarly publications
Professional publications
PROBLEM-CENTERED INITIATION
OJBECTIVE-CENTERED SOLUTION
DESIGN & DEVELOPMENT-CENTERED INITIATION
CLIENT/ CONTEXT INITIATED
Possible Research Entry Points

Figure 2: Design Science Research Methodology framework [14].

holders and empirically investigating the performance of an artefact in a context [6]. Those activities are related closely to the assignment proposed by the company, because the object of study is an artefact in context. Focusing on the assignment, the dashboard is an artefact and the context consists of the stakeholders who want to have an insight in the cybersecurity performance. Figure 2 shows the Design Science Research Methodology (DSRM) framework.

The model consists of six activities and research applying the framework may start at almost any step of the process. We have used the objective-centred solution approach within this research, since the research need was triggered by the development of the dashboard.

1.4 Research design

During this research, we explore the critical cybersecurity processes of the company. These are of importance to determine KPIs. Furthermore, we will identify the relevant stakeholders related to the cybersecurity activities. At different levels of the organisation, stakeholders have to provide directions to achieve certain goals. Oversight increases accountability. The dashboard may be used at different business levels providing insight in various processes and tasks. Therefore, the indicators of the dashboard will be based on different stakeholder levels. The final dashboard is created in Qlik Sense.

1.4.1 Objectives and deliverables

The central solution of my research is the dashboard with the defined Key Performance Indicators. In order to define the measurements of succes in the end, some objectes are formulated:

- The dashboard should provide insight in cybersecurity performance based on existing security processes and information.
- The dashboard should be easy to use by the stakeholders related to cybersecurity processes.
- The dashboard should be built within the platform Qlik Sense.

We have listed the most important outputs, or key deliverables, below. These deliverables are the results of the research when all stages of the Design Science framework are performed.

- A dashboard in Qlik Sense providing Key Performance Indicators giving insight in cybersecurity processes and information.
- Information on the design process of the dashboard and its features.
- A document containing information about the functionalities and feautres of the dashboard intended for the identified stakeholder groups.

1.4.2 Research questions

Design Science describes two kinds of research problems, namely design problems and knowledge questions [6]. The design problem is to design a dashboard so that cybersecurity reporting can be improved towards higher business levels. The knowledge questions aim to describe and explain phenomena relating to the dashboard. We have combined the design problems and knowledge questions and turned them into research questions. The research questions are divided into sub-questions. Altogether, the questions will help to solve the research problem.

1. What is the current situation at the company regarding the security processes?
Insight in the current situation is necessary to understand the process flow and the existing cybersecurity processes. The following sub questions are determined:

1.1 Which processes and systems are involved in the security domain?

1.2 In what way is cybersecurity maintained within the company?

Answers to these two research questions will not be discussed in this summary. Therefore, we briefly discuss how we received insight in the current situation at the end of this chapter.

2. Which KPIs can be used for reporting on cybersecurity?
The dashboard must provide an overview of relevant security indicators at different business levels. In order to determine the right KPIs, research has to be done. To systematically conduct this research, we have defined some sub questions:

2.1 Which KPIs can be determined to express cybersecurity performance?

2.2 Who are the relevant stakeholders and which KPIs should be selected based on stakeholder preferences?

3. How can we use data to report on KPIs on the dashboard?
After determination of the KPIs, the right data should be collected. We have to visualise data by the dashboard. In order for this to work an efficient data model architecture is required. Also KPIs should be visualised in the right way to prevent misinterpretations or misunderstandings.

3.1 How to prepare and structure the data in an efficient data model?

3.2 How to visualise the KPIs and metrics on the dashboard?

4. How can we use the dashboard to provide accurate reporting?
This last question serves to explain the information on the dashboard. With the dashboard, the stakeholders at different business levels should be able to report easily and accurately on cybersecurity processes and analyses. We will provide a description of the dashboard and the database for the identified stakeholders, in order for them to be able to report on the cybersecurity related events.

1.5 Current situation

The research questions with related sub-questions have been described in the previous section. The first research question concerns the current situation. Using insights from Chapter 2, we provided an answer to the first research question. We briefly discuss the answering process in this section.

First, we mapped and explained the functionalities of one of the domains within the company. We have used the concept of business process modelling. Related concepts to business process modelling will be discussed in the next chapter. Unfortunately, we are not able to show the final process diagram in this report. However, we hope the purpose of the model becomes clear while reading Chapter 2: provide an understanding of the functionalities of a domain and information elements exchanged with other domains.

Second, we described the cybersecurity processes within the company. To be able to provide reporting about the cybersecurity performance, it is important to gain insight in the cybersecurity processes of the company. Knowledge about these processes will also help increase understanding of cyber terminology. We have used the NIST framework to describe the Information security processes of the company. Again, we will not share the details of the processes in this report.

2 Theoretical framework

Phases 1 and 2 of the Design Science Research Methodology have been described in the previous chapter. Before moving on to the third phase, the design and development of the dashboard, we have to answer some research questions. The DSRM framework describes this by the *Theory* component between Phase 2 and Phase 3.

2.1 Current situation

The first research question is about the current situation at the company regarding the security processes.
The focus of the current situation is on one of the specified domains within the company. In order to increase the understanding about the operations within the domain, we will create a business process model. The current processes and systems can be visualised by using conceptual models. Identifying the activities and relationships within the domain will help to communicate about the processes in an effective manner [9].

Weske [9] describes a business process model as a set of activity models and execution constraints between them. Before the actual creation of the conceptual model, the concepts used to establish such a model have to be explained first. An official notation has been released by the Object Management Group, Inc. in order to cover different modelling types. This notation is known as the Business Process Model and Notation (BPMN) and aims to guide business process modelling on different levels of abstraction [4]. The BPMN makes use of several simple elements to express complex business processes. The elements are shown in Figure 3.

BPMN models can be classified into three categories: processes (orchestrations), choreographies and collaborations [11]. To model the activities and processes involved in the domain of the company, we will use the orchestration sub-model. Orchestrations provide an overview of the internal behaviour of a business process and details about the execution constraints of activities within a process [4].

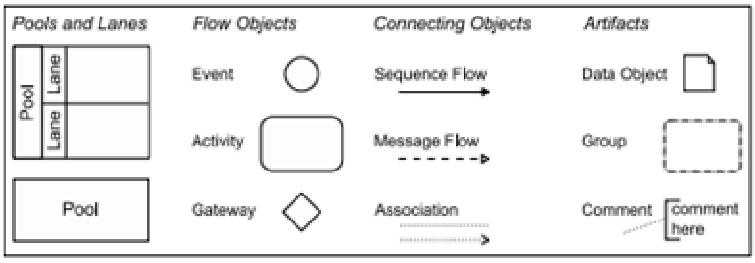


Figure 3: BPMN elemnets [4].

The tool used to model the orchestration is Bizagi Modeler. This application was taught and practiced during one of the bachelor modules of IEM and can be downloaded free of charge. The tool supports the Business Process Model and Notation. To be able to model the processes into Bizagi Modeler, we have to identify the functions and activities related to the domain. Information about functionalities of domains is saved in company documents.

2.2 KPI selection

One of the knowledge questions formulated in Section 1.4.2 has to be answered by conducting a systematic literature review. We will determine several Key Performance Indicators based on literature and on stakeholder preferences and use them as inputs for the final dashboard. The research question to be answered by a systematic literature review is the following:

2.1 Which KPIs can be determined to express cybersecurity performance?

We have selected nine studies from the systematic literature review. The steps taken to select the final articles are documented in Appendix A and the list of these articles is added to Appendix B.

2.2.1 Theoretical perspective

From the literature, many KPIs can be selected to express cybersecurity performance. However, not all are of relevance for the company. In order to select the right KPIs, we have to determine a theoretical perspective. The perspective helps to classify the KPIs. The

National Institute of Standards and Technology (NIST) has developed a framework for managing and reducing cybersecurity risks. An organisation can use the framework within its systematic processes to identify, assess and manage cybersecurity risk [10]. The core of the framework provides key cybersecurity outcomes that are helpful in managing cybersecurity risk: identify, protect, detect, respond and recover. The KPIs described in the literature can be categorized amongst these five areas. A concept-matrix of the five perspectives per study is shown in Appendix C.

2.2.2 KPI selection from literature

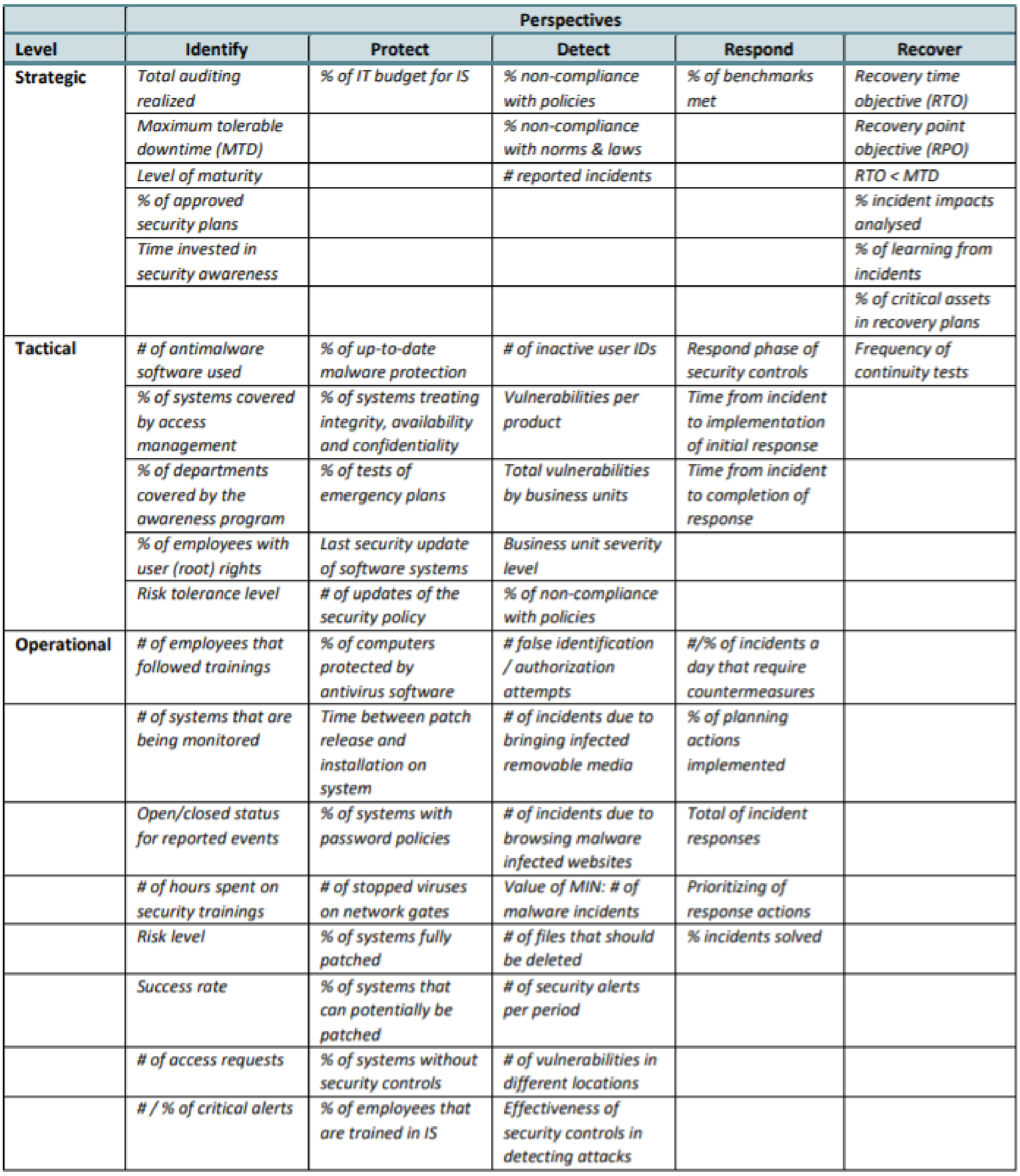
Some KPIs were not directly extracted from the literature, but could be determined by careful reading of studies.

All KPIs are related to measuring cybersecurity performance of companies. According to NIST organisations can use measures and metrics to set goals, also called benchmarks. ”Success or failure can be determined against these benchmarks” [10]. The dashboard should provide both abstract and concrete overviews of the KPIs, because it will be used at different business levels. Several stakeholders may be interested in data generated by the dashboard in order to provide directions towards the domains or business areas they are responsible for. For a manager it is fundamental to have control of the current situation of their department [3]. In order to be able to provide clear and reasonable directions, KPIs have to be collected and presented for making meaningful decisions [1].

Some KPIs mentioned in the studies were not included in the concept-matrix, because they are irrelevant for this situation. Examples of irrelevant KPIs are indicators describing personal data or forecasting indicators. We have included KPIs from all business levels in the concept-matrix. The dashboard created for the company should be useable at different levels of the company. In some of the studies a distinction of relevant KPIs for different levels has already been made, for example per business function, or on abstract and concrete levels of reporting. We decided to roughly divide the KPIs from the chosen literature into strategic, tactical and operational business levels.

Appendix C includes a concept-matrix classifying the KPIs along the NIST perspectives. In Figure 4 on the next page we sorted the KPIs in the final concept-matrix, including the different business levels. We have removed duplicate performance indicators from different articles. Some KPIs are considered to be of relevance for more than one level.

We will discuss the KPIs described in Figure 4 with relevant stakeholders. Interviews with the stakeholders will be conducted in order to determine more relevant KPIs. After the interviews, some KPIs might turn out to have a lower priority than others. We might leave KPIs out of consideration if it turns out it is not feasible to measure them within the given time.



	Perspectives				
Level	Identify	Protect	Detect	Respond	Recover
Strategic	Total auditing realized	% of IT budget for IS	% non-compliance with policies	% of benchmarks met	Recovery time objective (RTO)
	Maximum tolerable downtime (MTD)		% non-compliance with norms & laws		Recovery point objective (RPO)
	Level of maturity		# reported incidents		RTO < MTD
	% of approved security plans				% incident impacts analysed
	Time invested in security awareness				% of learning from incidents
					% of critical assets in recovery plans
Tactical	# of antimalware software used	% of up-to-date malware protection	# of inactive user IDs	Respond phase of security controls	Frequency of continuity tests
	% of systems covered by access management	% of systems treating integrity, availability and confidentiality	Vulnerabilities per product	Time from incident to implementation of initial response	
	% of departments covered by the awareness program	% of tests of emergency plans	Total vulnerabilities by business units	Time from incident to completion of response	
	% of employees with user (root) rights	Last security update of software systems	Business unit severity level		
	Risk tolerance level	# of updates of the security policy	% of non-compliance with policies		
Operational	# of employees that followed trainings	% of computers protected by antivirus software	# false identification / authorization attempts	#/% of incidents a day that require countermeasures	
	# of systems that are being monitored	Time between patch release and installation on system	# of incidents due to bringing infected removable media	% of planning actions implemented	
	Open/closed status for reported events	% of systems with password policies	# of incidents due to browsing malware infected websites	Total of incident responses	
	# of hours spent on security trainings	# of stopped viruses on network gates	Value of MIN: # of malware incidents	Prioritizing of response actions	
	Risk level	% of systems fully patched	# of files that should be deleted	% incidents solved	
	Success rate	% of systems that can potentially be patched	# of security alerts per period		
	# of access requests	% of systems without security controls	# of vulnerabilities in different locations		
	# / % of critical alerts	% of employees that are trained in IS	Effectiveness of security controls in detecting attacks		

Figure 4: Sorted Concept Matrix.

2.3 Data management

After determination of the KPIs to use in the dashboard, we must collect the right data. The Key Performance Indicators or metrics will be displayed to managers or other users through several dashboards. In order for this to work, we have to manage the data first. This section provides an answer to research question 3.1:

3.1 How to prepare and structure the data in an efficient data model?

The data over which Business Intelligence tasks are performed often comes from different sources - typically from multiple operational databases across departments within the organisation [16]. Different databases make use of varying data types, formulas, codes and formats. The security processes within the company concern several systems and departments and probably use multiple databases to store information. Therefore, an efficient data model architecture is required.

The model-driven dashboard design framework covers the many facets of the dashboard design process including useful model artifacts [5]. Figure 5 shows the end to end dashboard component flow.

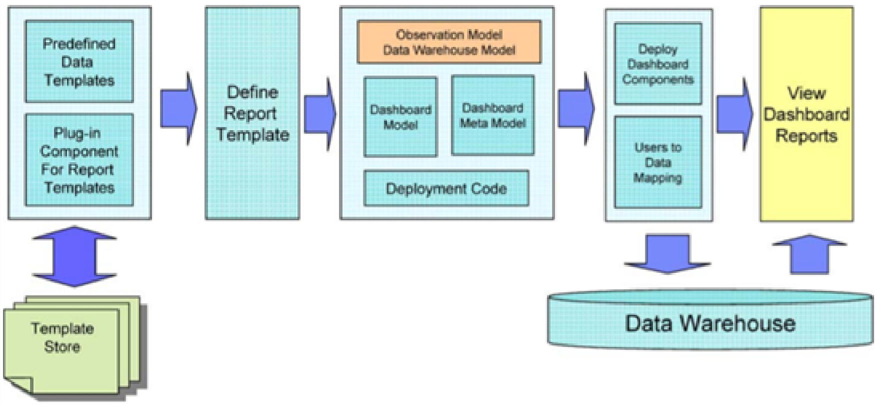


Figure 5: Model-driven dashboard design [5].

The model can be classified roughly into three main categories:

1. Pre-modelling activity
2. Modelling activity
3. Post-modelling activity

Pre-modelling activity
The first activity relates to the understanding of the components that will be included in the eventual dashboards. Predefining the components helps to efficiently design the solution. During this modelling phase, we have to get acquainted with the data templates and data structures used within the company. Eventually, we will use these reports to retrieve appropriate data to present on the dashboard interface.

Modelling activity
The second category describes the actual modelling of the reporting requirements. During this phase, we will have to define metrics, create the report templates for the different data types and identify different user roles that need access to the dashboard portal [5].

Post-modelling activity
Lastly, we discuss the post-modelling phase. In this step, we will transform the data model representation into code. The dashboard now consists of two main parts: the set of files containing the code for the dashboard and the database tables necessary to structure the dashboard. These involve the SQL scripts for reading data from the data sources and loading them into the dashboard program. We will be using Qlik Sense to create our dashboards. Qlik Sense uses the data load editor to load data from the data sources into the application.

The model-driven dashboard design makes use of several artifacts. Most of the modelling aspects of the framework use the Unified Modelling Language (UML) to visualise the design. We will use UML class diagrams to represent a logical structure of the data present at the company.

2.4 Dashboard design

To create a high quality dashboard, the designer should spend time and effort in thinking about the purpose of the solution. Why are we building this dashboard and what should it represent? It is also important to prevent interpretation mistakes from happening and therefore it is essential to select the right charts for the metrics in the dashboard. Some visualisations present certain data sets better than others, thus knowing the differences will help to design a useful dashboard. This section serves to answer research question 3.2:

3.2 How to visualise the KPIs and metrics on the dashboard?

One of the objectives and deliverables defined at the beginning of this thesis formulates that the dashboard should be easy to use by the stakeholders. We will conduct research to find out how to develop a user-friendly dashboard and keep this in mind during the design process.

2.4.1 User-friendly design

In this section, we describe the best practices retrieved from literature to build a dashboard that is user-friendly.

Attractiveness
The dashboard must be attractive and pleasing to the eye of the user. Good design combines power, functionality, and simplicity with a pleasing appearance [12].

Comprehensibility
A dashboard should present the information in a comprehensible and meaningful order. This includes the composition of the whole dashboard as well as the order within visualisations. Furthermore, reading and digesting long explanations should never be necessary [12]. However, explanations are important in order to understand the dashboard. Data without text, labels or instructions cause misinterpretations and confusion [7].

Compactness
A dashboard should be compact, simple and easy to understand. Compact dashboards feel pleasant to use and make a user more productive [7].

Customisability
It is important to build in flexibility in the dashboard to become relevant for different users [7]. Flexibility is "the system's ability to respond to individual differences in people" [12]. Different users are interested in particular metrics. A customisable dashboard permits the users to search for and select information of their interest. Easy customisation of the dashboard encourages an active role in understanding and allows for personal preferences in experience levels [12]. A common way to make a dashboard customisable is to define the scope of the data using filters [7].

Consistency
Consistency within a dashboard is essential, since it allows the user to make decisions easier. Inconsistencies may cause misinterpretations or misunderstandings of the data. It is important for most dashboards to be consistent in many aspects of their appearance, such as the fonts and colours, but also the actions required to access details [13].

2.4.2 Data visualisation

Literature describes a dashboard design process: define, prototype, build and deploy [8]. The process is based on existing design processes, but the output will always be a dashboard. We will use the first two phases of the design process to structure the *Design & Development* phase of the DSRM used throughout this thesis. The latter phases, build and deploy, will not be described, since they are already included in the Design Science Research Methodology.

1. Define
A central step in building an effective dashboard is understanding the central purpose for building the dashboard [8]. This understanding starts at the beginning of this research by formulating a core problem and by interviewing users. When constructing the dashboards, the designer should remember who the users are and what information they require. The

point of a dashboard is to help people find insights and make decisions [8]. At the company the users of the dashboard want insight in the cybersecurity performance in order to provide reporting and directions. The individual dashboards that will be constructed have their own goals contributing to the bigger purpose.

While keeping the purpose of the dashboards in mind, the metrics have to be defined. We have to figure out which metrics and KPIs would best support the user decisions [8]. In this step, it is important to understand the motivation of the user and use it to state a specific goal for the dashboard.

2. Prototype

When the metrics are clear, we have to find the best visualisations for the metrics. Placing the data in a visual context helps people understand the significance of the data. However, selecting the wrong visualisations may be disastrous. Another consideration to take in mind during this step is the composition of the visualisations. Qlik Sense provides a visualisation manual that we can use while creating the dashboard [15].

During the prototyping step, we must keep our dashboard objectives in mind, defined at the beginning of this thesis. In the previous section, we have explained the design principles to develop a user-friendly dashboard.

Prototypes and ideas of the dashboard can be discussed with the user. It allows the designer to focus on the design of the dashboard instead of the numbers.

3 Design and implementation

In Chapter 2 we have elaborated a concept-matrix describing KPIs based on a systematic literature review. In this Chapter, we make the final KPI selection, discuss the design and implementation process of the dashboards and collect relevant data in a structured way and load these into the dashboard application. We are not allowed to present all information, but we will try to explain the most relevant steps of the design and implementation process.

3.1 KPI selection

We have shown the concept-matrix in Figure 4 describing cybersecurity KPIs to stakeholders during semi structured interviews. This type of interview enabled us to maintain some structure, but it also created some flexibility for additional probing to get more details. KPIs were removed from or added to the matrix, based on the stakeholder preferences. The KPIs to be implemented in the dashboard are selected from the adjusted concept matrix.

According to the stakeholders, all KPIs are of relevance for the company, but it is impossible to implement all of them into the dashboard within the given time. The stakeholders are interested in additional Key Performance Indicators, specific for the company. Those KPIs were added to the concept-matrix. We have determined the preferences of the stakeholders, after which priorities could be given to the KPIs.

At different organisational levels the KPIs vary in level of abstraction. At the operational level, stakeholders are interested in concrete and detailed information, while the strategic level is devoted to more abstract information. The highest priority KPIs selected from the concept-matrix are reformulated into KPIs ranging from abstract to concrete levels. Unfortunately, we cannot provide the final KPI selection in this summary.

The highest priority KPIs were categorized into five topics serving as a basis for the eventual dashboards. During conversations with the stakeholders, we were able to determine useful metrics to measure performance of the final categories.

3.2 Data modelling

The data related to the five categories are stored in databases. It is important to collect these data in a structured way, and load them into the dashboard application. Section 2.3 describes three modelling categories: pre-modelling, modelling and post-modelling.

During the first phase, the goal is to understand the components that will be included in the eventual dashboards.
The second phase concerns the actual modelling of the reporting requirements. We have created UML class diagrams for the dashboards and identified user roles that need access to the dashboard portal. We also discussed the first two steps of the dashboard design for each individual dashboard.

3.3 Dashboard development

The post-modelling activity of the model-driven dashboard design concerns the transformation of the data model representation into code [5]. To create high quality dashboards, we should spend time and effort thinking about the purpose of the solution. Why are we building the dashboard and what should it represent? It is also important to prevent interpretation mistakes from happening and therefore it is essential to select the right charts for the metrics in the dashboard. We will use code and visualisation techniques in Qlik Sense to create the actual dashboards.

Qlik Sense makes use of a data load script that can be managed by the data load editor. The data load editor enables us to retrieve data from data sources or databases. Another option is to load data into Qlik Sense through the data manager, but this is not preferable, since we will not be able to edit and run the data load script.

In the data load editor, we define the absolute path of the network location. The script connects the application to the data source including the data files and loads these data into the application.

The data will be reloaded and updated every morning. When the data are loaded into Qlik Sense, they are available for analysis. In this phase we start to create and visualise our metrics. An important function in Qlik Sense is the 'expression editor'. When creating dimensions or measures, expressions can be inserted to make certain selections or calculations on the data. In Section 2.4 we have described several techniques and practices to design a dashboard that is easy to use. The individual dashboards are constructed using the first two phases of the dashboard design process:

1. *Define - understand the motivation of the user and use it to define the purpose of the dashboard.*

2. *Prototype - chose the right visualisation objectives and discuss prototypes with the users.*

As mentioned before, we will not discuss the development process in detail for each individual dashboard. In the actual thesis, we demonstrate the final dashboards in the next chapter. However, this is also left out of consideration, because of confidentiality.

4 Evaluation

The fifth phase of the Design Science Research Methodology evaluates the artifact. This phase observes and measures the performance of the dashboard. The activity involves the comparison between the objectives and required functionalities of the solution to the actual results received by the demonstration of the dashboard.

In Section 2.4 the dashboard design process has been explained. We have used this process to build high quality dashboards efficiently. The central purpose for building the individual dashboards was determined first. During the second phase, we have constructed several prototypes. These prototypes and optional ideas were discussed with the stakeholders. The early samples of the dashboard enabled us to test the concept in early stages. The prototype was used to evaluate the visualisations and test whether the requirements were met. The feedback was used to improve the dashboards further. After some last improvements and adjustments, the final dashboards were constructed. The prototype phase helped us to create five dashboards meeting the requirements of the user.

4.1 Validation

We have conducted an interview with the central user of the dashboard to evaluate and validate the final construction. Broadly, the following three questions were discussed with the stakeholder:

- To what extent is the dashboard meeting the formulated requirements?
- Are the metrics in the dashboard representing the variables we wanted to measure?
- Is there any information/knowledge missing from the dashboard?

All dashboards were discussed with the user separately. In general, the stakeholder is satisfied with the results. The dashboards meet the expectations of the stakeholders and contribute to increasing cybersecurity resilience. Reporting regarding cybersecurity could be improved. The insights provided by the dashboard give an appropriate solution for this defined problem. With the visualisations and metrics of the dashboard, the stakeholders are able to report on different organisational levels.

In the actual thesis, we describe the validation of each of the dashboards separately.

4.2 Evaluation of objectives

As described in Chapter 1, the fifth phase of the DSRM concerns the evaluation of the dashboard. This involves the comparison between the objectives and required functionalities of the solution to the actual results received by the demonstration of the dashboard. The objectives of our research were determined in Chapter 1 and formulated as follows:

- The dashboard should provide insight in cybersecurity performance based on existing security processes and information.
- The dashboard should be easy to use by the stakeholders related to cybersecurity processes.
- The dashboard should be built within the platform often used by the company, Qlik Sense.

The first objective of the dashboards was to provide insight in the cybersecurity performance based on existing security processes and information. Relevant KPIs were selected from the literature and based on stakeholder preferences. The KPIs were used to represent part of the cybersecurity performance within the company. The stakeholders are really happy with the result. They think the dashboards have a high valued contribution to practice.

The second objective states that the dashboard should be easy to use by the stakeholders related to the cybersecurity processes. In Chapter 2 we have discussed the best practices to build a dashboard that is user-friendly. The first key principle is attractiveness. Each of the dashboards is pleasing to the eye of the user. We have used the company colours within the graphics and the visualisations are aligned symmetrically were possible. No more than four or five graphs are displayed on a dashboard sheet and enough empty spaces are created between the visualisations. Furthermore, the dashboards are comprehensible. The information is presented in a logical order. The most relevant Key Performance Indicators are always situated at the centre of the dashboard to draw attention. Labels and descriptions are added to explain the visualisations. The third practice is compactness of data. Our dashboards are simple and easy to understand. Detailed information is mostly hided at first sight, but can be reached easily when required. Filter panes allow the user to make selections and limit the data to his or her preference. Fourth, the dashboard must be customisable. Our tool permits the users to search for and select information of their interest. By the implementation of filter panes in the dashboards, the scope of the data can easily be defined based on individual preference. The fifth and last key practice to discuss is consistency. We have tried to construct comparable performance measures in a similar way. We make consistent use of colours and fonts. Throughout the dashboards, visualisation techniques are used for the same purposes.

The third objective is to build the dashboard within Qlik Sense. This platform is often used within the company and therefore preferred by the stakeholders.

All in all, we may conclude the dashboard meets the formulated objectives. The dashboard provides insight in cybersecurity performance, is user-friendly and constructed in the preferred application, namely Qlik Sense.

5 Conclusion

The goal of the thesis was to solve the core problem: no accurate reporting regarding cybersecurity is provided for management. The company wants to have a dashboard providing a clear overview of the vulnerabilities and activities related to cybersecurity. Management wishes to detect easily which cybersecurity systems or processes must be improved and how to improve them. At the beginning of the research, we have formulated a research goal:

Determine Key Performance Indicators based on the preferences of stakeholders and related to cybersecurity and portray the findings onto a dashboard in order to provide accurate reporting of the cybersecurity performance.

We have decided to use the Design Science research methodology (DSRM) for conducting our research. The DSRM focuses on two activities: designing an artefact that improves something for stakeholders and empirically investigating the performance of an artefact in context. In our research, the dashboard is the artefact and the context consists of stakeholders of the company wanting to have insight in the cybersecurity performance.

In this research, we have determined several Key Performance Indicators to measure cybersecurity performance. This list of KPIs was shown to relevant stakeholders during interviews and updated based on their preferences. The final selection of indicators and metrics serves as a basis for the eventual dashboards. Our dashboards were created in Qlik Sense, because this application is used by the company often. We have established databases to structure the available data and load it into the Qlik Sense application. Several visualisation techniques were used to create a functioning dashboard. The dashboard has been demonstrated to and evaluated by the users.

In this chapter, we discuss whether the research questions formulated at the beginning of my research have been answered and whether the core problem has been solved. Afterwards, we provide some recommendations for the company.

5.1 Research Questions

In Section 1.4.2 we have formulated several research questions in order to solve the core problem of this research. We discuss each of the research questions briefly in this section.

1. What is the current situation at the company regarding the security processes?
The purpose of the first research question is to gain understanding of the systems and cybersecurity processes within the company. First, we have performed qualitative research to achieve an in-depth understanding of the systems and processes related to a domain of the organisation. Information about the functionalities and architecture of this domain was gathered from company documents. We have used Bizagi Modeler to create a business process diagram of the domain and visualize the related processes and systems. Furthermore,

we have conducted some internal research to learn about important cybersecurity processes of the organisation. We have used the NIST framework to structure the information.

These insights about key systems and processes were of importance to determine relevant KPIs later on in the research.

2. Which KPIs can be used for reporting on cybersecurity?
The dashboard must provide an overview of cybersecurity indicators at different organisational levels. The goal of this research question is to determine relevant KPIs for the dashboard. We have conducted a systematic literature review to summarize Key Performance Indicators from several studies. A concept-matrix classifies the KPIs along the five perspectives of NIST: identify, protect, detect, respond and recover. During semi structured interviews with stakeholders, we were able to discuss the list of indicators. Based on stakeholder preferences, KPIs were reformulated, added or removed. The highest priority KPIs were categorized into five topics. For each topic we have determined useful metrics to measure performance, serving as a basis for the eventual dashboards.

3. How can we use data to report on KPIs on the dashboard?
The purpose of the third research question is to collect data properly and visualise the KPIs in the right way. We have conducted qualitative research to gain understanding on the design of appropriate data models. In Chapter 2, we describe a framework for model-driven dashboard design, covering the facets of the dashboard design process.

In Chapter 4 we have used the framework to structure the data modelling process. First of all, we gained insight in the components that would be included in the dashboards. Data for the KPI categories were stored mostly in rather simple databases, so we decided to use these as a basis for the dashboard databases. We have added metrics to the templates and restructured the existing data. In order to represent a logical structure of the data present at the company, we have created UML class diagrams. During the last activity, we have transformed the data model into code in Qlik Sense.

We have also conducted a literature review to learn about visualisation techniques of KPIs. One of the objectives and deliverables defined at the beginning of my research formulates that the dashboard should be easy to use by the stakeholders. Literature describes principles to build a dashboard that is user friendly: attractiveness, comprehensible, compactness, customisability and consistency. We have constructed the final dashboards using the first two phases of a dashboard design process: define and prototype.

Insights in the data modelling and design processes enabled us to create high quality and effective dashboards. By answering this research question we have spent time and effort thinking about the purpose and design of the solution. With the knowledge obtained from literature about different visualisation techniques, we were able to select the right charts for the metrics, preventing misinterpretations or misunderstandings from happening.

4. ***How can we use the dashboard to provide accurate reporting?***
The last research question serves to explain the information on the dashboard. The stakeholders at different business levels should be able to report easily and accurately on cybersecurity processes and analyses. In the actual thesis we describe the implementation process of the actual dashboards and motivate the choices for the visualisation types. We have also explained the use of expressions in Qlik Sense in order to create dimensions or measures. We have also demonstrated the actual dashboards and their functionalities. Unfortunately, we are not able to show the implementation and demonstration phases in this summary.

We have created graphs and measures in such a way that the users of the dashboard obtain an immediate overview of the status of processes. For more detailed information, the user can apply selections in the filter panes or use so-called drill-down functions. These allow the users to search for information selectively. In this way, reporting is possible at different levels of abstraction.

At the start of this research, we had divided the research goal into four research questions. Each of the research questions contributed to achieving the main research goal. We have created five functioning dashboards providing an overview of cybersecurity status. These findings and indicators can be used to report about the performance of cybersecurity processes and activities.

5.2 Company conclusion

The stakeholders are really happy with the final results. They believe the dashboards have a high valued contribution to practice. Each of the dashboards provide insight in different cybersecurity processes. The defined metrics and visualisations serve as applicable solutions for the core problem of this research. At the beginning of this research we determined objectives of the dashboard in cooperation with the company. We have evaluated the dashboards and their objectives. The final dashboards enable accurate reporting on both abstract and concrete levels of cybersecurity performance. Furthermore, the Qlik Sense dashboards are easy to use.

Stage 6 of the DSRM concerns the communication of the dashboard. We have given a presentation of the dashboards to the employees of the department. During this presentation we explained the different phases of our research, motivated the final selection of KPIs and demonstrated the dashboards and their functionalities. We have shown the restructuring steps of the databases and explained the importance of consistent data updating of the databases. The employees were enthusiastic about the results and curious to use the dashboards in practice.

All in all, we may conclude that our research goal has been achieved: the research questions have been answered, the dashboards have been evaluated and the objectives are met.

5.3 Recommendations

The most important objectives and requirements of the dashboards are met. However, in this section we will provide some recommendations. We will not make the connection to the actual dashboard examples, as we have done in the actual thesis.

First of all, we did not make a connection to the risks related to the findings of the dashboards. The measures and metrics provide insight in cybersecurity processes, but no risks or actions are determined based on their values. Identification and assessing of risks helps the user to control threats, as well as reporting about these threats accurately.

Furthermore, it might be interesting to determine benchmarks and goals to actually measure progress and encourage further actions based on the results. The benchmakrs could be set on different levels: for the organisation, a department, certain systems or even employees. A suggestion would be to make sure the goals comply with the SMART model, so the goal setting will not be too optimistic. The benchmarks could be integrated into the dashboards, allowing the user to compare the actual performance to the set targets. Reporting about benchmarks can encourage managers to provide new directions or actions based on the results.

Third, more Key Performance Indicators may be added to the dashboards. We have constructed a concept-matrix showing relevant KPIs related to cybersecurity performance. According to the interviewed stakeholders, all KPIs are of relevance for the company, but it was impossible to implement all of them during my research due to time constraints. We have decided to select the KPIs with the highest priority according to the stakeholders. In order to measure total cybersecurity performance, more KPIs must be implemented. This could be taken into consideration for further research. The organisation can use the remaining KPIs of the concept-matrix. They can also introduce new KPIs based on their security processes. The organisation might also add KPIs to the existing dashboards. These could include the risks or benchmarks discussed earlier. It is important to create an overview of all cybersecurity processes in order to measure total cybersecurity performance.

For some of the dashboards, progress or performance could be measured over a time period. Trendlines can then be implemented to quickly scan the general course of a certain measure. These insights provide concrete information about the progress immediately. If a trendline shows that no progress has been made in the past year, these findings can be reported to the managers immediately.

Lastly, we recommend the company to keep the dashboards and databases up to date. Changes or additions to the data in the database must be executed in a consistent way. Whenever columns or sheets are added to the database, the editor must check whether data is still loaded into the dashboard correctly. A user can always create new visualisations in Qlik Sense based on the new data.

References

[1] Hajdarevic K. Pattinson C. Kozaric K. Hadzic A. *Information Security Measurement Infrastructure for KPI Visualization.* URL: `https://mipro-proceedings.com/sites/miproproceedings.com/files/upload/iss/iss_015.pdf`.

[2] Heerkens H. Winden A. *Geen Probleem.* Bergman Mediagroup Gorkum, 2012.

[3] Alberto G. Rust L. F. Dutra A. C. *Enterprise Security Governance: A practical guide to implement and control Information Security Governance (ISG).* URL: `nce.ufrj.br/labnet/agris/informes/PID199098.pdf`.

[4] Habib R. Sabbagh E. *Business Process Architectures. Concepts, Formalism, and Analysis.* Potsdam: Hasso Plattner Institute, 2015.

[5] Palpanas T. Chowdhary P. Mihaila G. Pinel F. "Integrated model-driven dashboard development." In: (2007). URL: `https://link.springer.com/content/pdf/10.1007/s10796-007-9032-9.pdf`.

[6] Wieringa R. J. *Design Science Methodology for Information Systems and Software Engineering.* Heidelberg: Springer-Verlag, 2014.

[7] Juicebox. *A Guide to Creating Dashboards People Love to Use.* 2015. URL: `A%20Guide%20to%20Creating%20Dashboards%20People%20Love%20to%20Use.%20Retrieved%20from%20https://static1.squarespace.com/static/52f42657e4b0b3416ff6b831/t/55b9117ae4b060a0d84fe%20f15/1438191994754/Dashboards_People_Love_To_Use_Whitepaper_v2.pdf`.

[8] David M. *How to design a Dashboard.* 2020. URL: `https://dataschool.com/how-to-design-adashboard/dashboard-design-process/`.

[9] Weske M. *Business Process Management. Concepts, Languages, Architectures.* Heidelberg: Springer-Verlag, 2007.

[10] NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* URL: `https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf`.

[11] OMG. *Business Process Model and Notation (BPMN).* URL: `http://www.omg.org/spec/BPMN/2.0`.

[12] Bhaskar N. U. Naidu P. P. Babu S. R. R. C. Govindarajulu P. "General Principles of User Interface Design and Websites." In: *Software Engineering* 3 (2011).

[13] Few S. *With Dashboards Formatting and Layout Definitely Matter.* 2008. URL: `https://www.perceptualedge.com/articles/Whitepapers/Formatting_and_Layout_Matter.pdf`.

[14] Peffers K. Tuunanen T. Rothenberger M. A. Chaterjee S. "A Design Science Research Methodology for Information Systems Research." In: *Management Information Systems* 24 (2007), pp. 45–78.

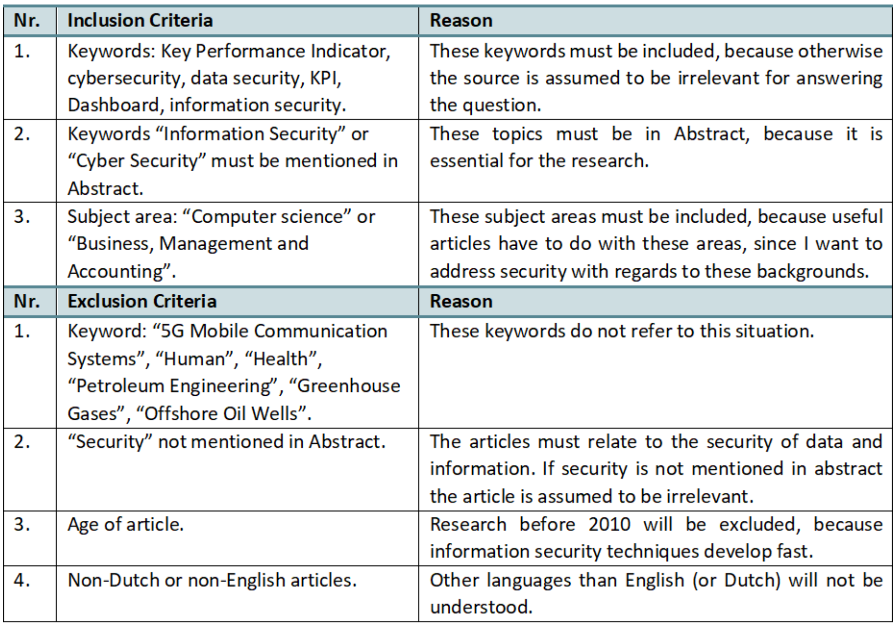
[15] Qlik Sense. *Visualisation types.* 2019. URL: https://help.qlik.com/en-US/sense-developer/November2019/Subsystems/Mashups/Content/Sense_Mashups/Create/Visualizations/visualization-types.htm.

[16] Chaudhuri S. Umeshwar D. Narasayya V. "An overview of Business Intelligence Technology." In: *Communications of the ACM* 54 (2011).

Appendix A - Steps for selecting literature

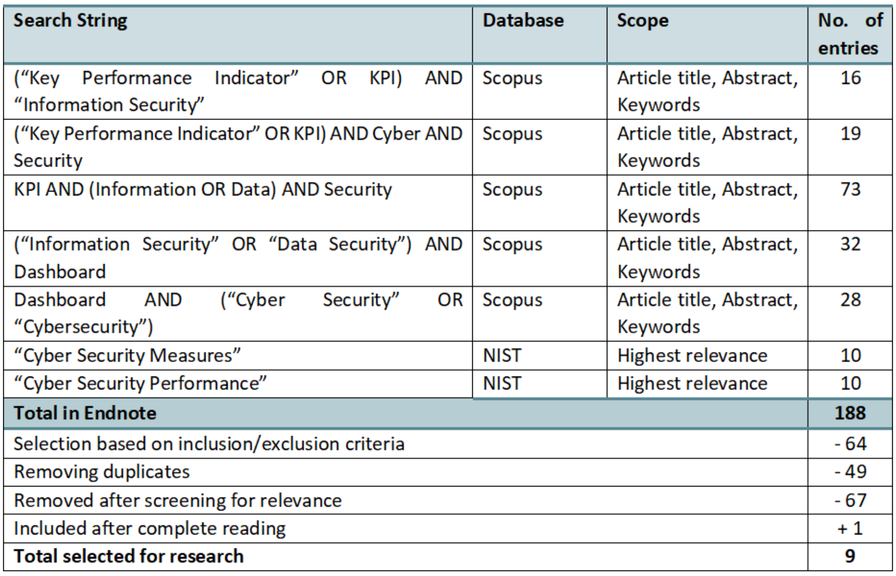
In order to select the right literature it is important to define inclusion and exclusion criteria, search strings, keywords and databases.

- **Inclusion and exclusion criteria**: criteria have to be determined in order to narrow down the scope. Figure 6 shows the defined criteria and reasons behind the selection.
- **Keywords**: Key Performance Indicators, Cyber Security, Data Security, Information Security, KPI, Dashboard.
- **Search strings**: the search strings are based on the keywords and documented in Figure 7 on the next page. Similar words for 'cybersecurity' are used. Only a few search terms were used in order to find the right articles.
- **Databases**: Due to experience gained from other modules, Scopus is preferred above the other search engines, because it contains a lot of scientific, peer-reviewed articles. Furthermore, Scopus provides a more structured search than other databases. NIST also provides useful articles related to cybersecurity and KPIs in these fields. The company makes use of the NIST cybersecurity framework in order to structure relevant cybersecurity implementations. Therefore, this database will be used as search engine as well.



Nr.	Inclusion Criteria	Reason
1.	Keywords: Key Performance Indicator, cybersecurity, data security, KPI, Dashboard, information security.	These keywords must be included, because otherwise the source is assumed to be irrelevant for answering the question.
2.	Keywords “Information Security” or “Cyber Security” must be mentioned in Abstract.	These topics must be in Abstract, because it is essential for the research.
3.	Subject area: “Computer science” or “Business, Management and Accounting”.	These subject areas must be included, because useful articles have to do with these areas, since I want to address security with regards to these backgrounds.
Nr.	**Exclusion Criteria**	**Reason**
1.	Keyword: “5G Mobile Communication Systems”, “Human”, “Health”, “Petroleum Engineering”, “Greenhouse Gases”, “Offshore Oil Wells”.	These keywords do not refer to this situation.
2.	“Security” not mentioned in Abstract.	The articles must relate to the security of data and information. If security is not mentioned in abstract the article is assumed to be irrelevant.
3.	Age of article.	Research before 2010 will be excluded, because information security techniques develop fast.
4.	Non-Dutch or non-English articles.	Other languages than English (or Dutch) will not be understood.

Figure 6: Inclusion and exclusion criteria.

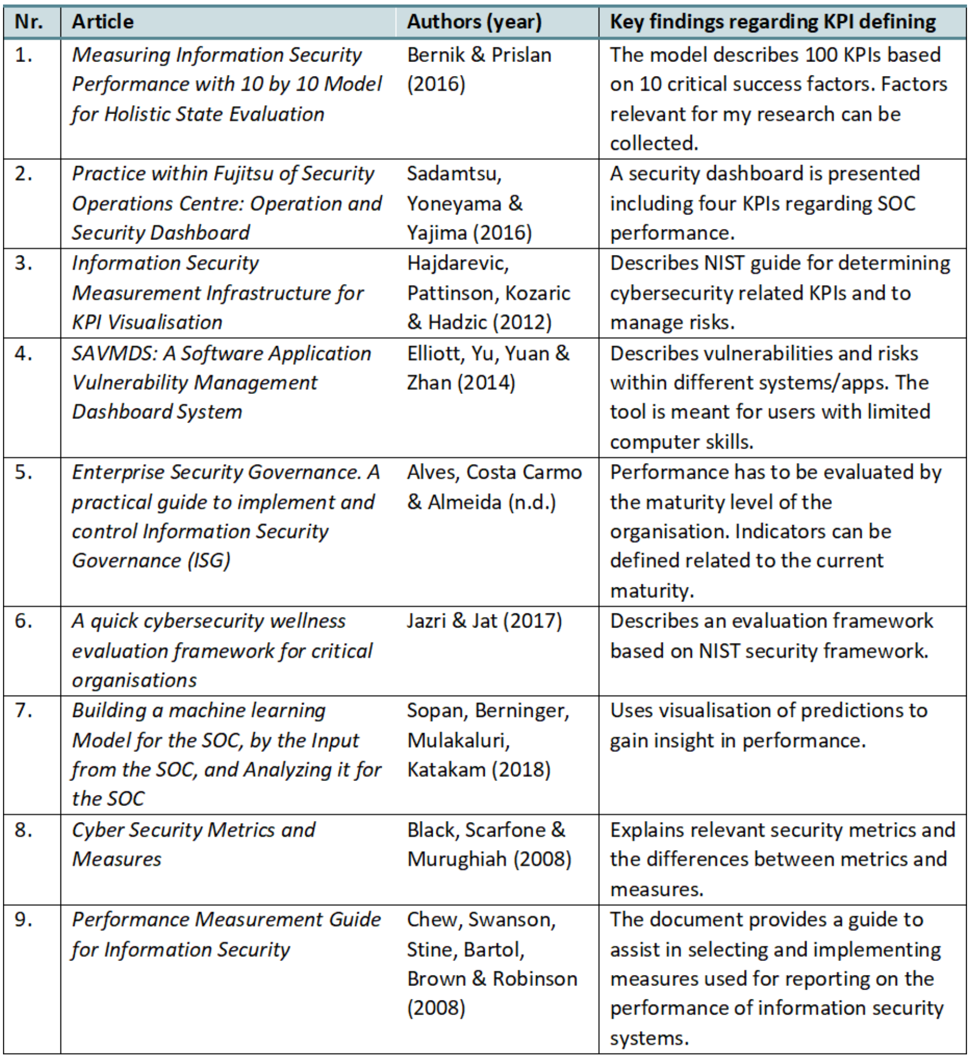


Search String	Database	Scope	No. of entries
("Key Performance Indicator" OR KPI) AND "Information Security"	Scopus	Article title, Abstract, Keywords	16
("Key Performance Indicator" OR KPI) AND Cyber AND Security	Scopus	Article title, Abstract, Keywords	19
KPI AND (Information OR Data) AND Security	Scopus	Article title, Abstract, Keywords	73
("Information Security" OR "Data Security") AND Dashboard	Scopus	Article title, Abstract, Keywords	32
Dashboard AND ("Cyber Security" OR "Cybersecurity")	Scopus	Article title, Abstract, Keywords	28
"Cyber Security Measures"	NIST	Highest relevance	10
"Cyber Security Performance"	NIST	Highest relevance	10
Total in Endnote			**188**
Selection based on inclusion/exclusion criteria			- 64
Removing duplicates			- 49
Removed after screening for relevance			- 67
Included after complete reading			+ 1
Total selected for research			**9**

Figure 7: Search terms.

Appendix B - Selected literature

After removal of the duplicates and selecting articles based on inclusion and exclusion criteria, the remaining articles are scanned. One article was included from the reference list of another published article. An overview of the most relevant and selected literature is provided in Figure 8.

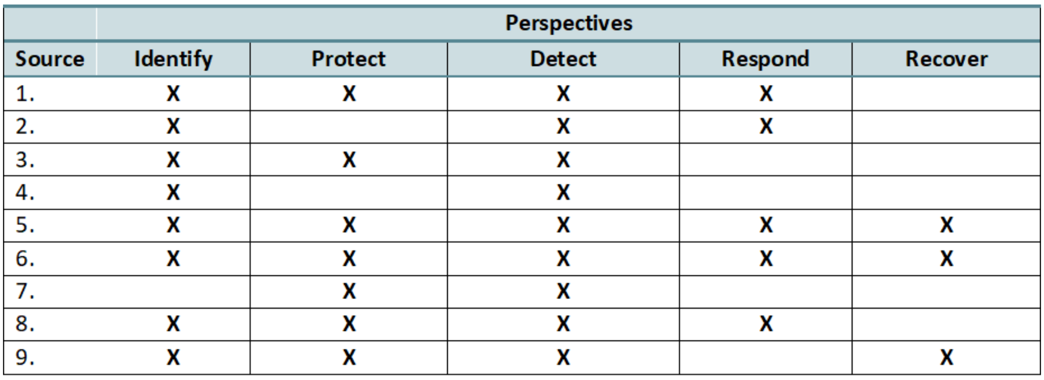


Nr.	Article	Authors (year)	Key findings regarding KPI defining
1.	*Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation*	Bernik & Prislan (2016)	The model describes 100 KPIs based on 10 critical success factors. Factors relevant for my research can be collected.
2.	*Practice within Fujitsu of Security Operations Centre: Operation and Security Dashboard*	Sadamtsu, Yoneyama & Yajima (2016)	A security dashboard is presented including four KPIs regarding SOC performance.
3.	*Information Security Measurement Infrastructure for KPI Visualisation*	Hajdarevic, Pattinson, Kozaric & Hadzic (2012)	Describes NIST guide for determining cybersecurity related KPIs and to manage risks.
4.	*SAVMDS: A Software Application Vulnerability Management Dashboard System*	Elliott, Yu, Yuan & Zhan (2014)	Describes vulnerabilities and risks within different systems/apps. The tool is meant for users with limited computer skills.
5.	*Enterprise Security Governance. A practical guide to implement and control Information Security Governance (ISG)*	Alves, Costa Carmo & Almeida (n.d.)	Performance has to be evaluated by the maturity level of the organisation. Indicators can be defined related to the current maturity.
6.	*A quick cybersecurity wellness evaluation framework for critical organisations*	Jazri & Jat (2017)	Describes an evaluation framework based on NIST security framework.
7.	*Building a machine learning Model for the SOC, by the Input from the SOC, and Analyzing it for the SOC*	Sopan, Berninger, Mulakaluri, Katakam (2018)	Uses visualisation of predictions to gain insight in performance.
8.	*Cyber Security Metrics and Measures*	Black, Scarfone & Murughiah (2008)	Explains relevant security metrics and the differences between metrics and measures.
9.	*Performance Measurement Guide for Information Security*	Chew, Swanson, Stine, Bartol, Brown & Robinson (2008)	The document provides a guide to assist in selecting and implementing measures used for reporting on the performance of information security systems.

Figure 8: Literature list.

Appendix C - Concept-Matrices

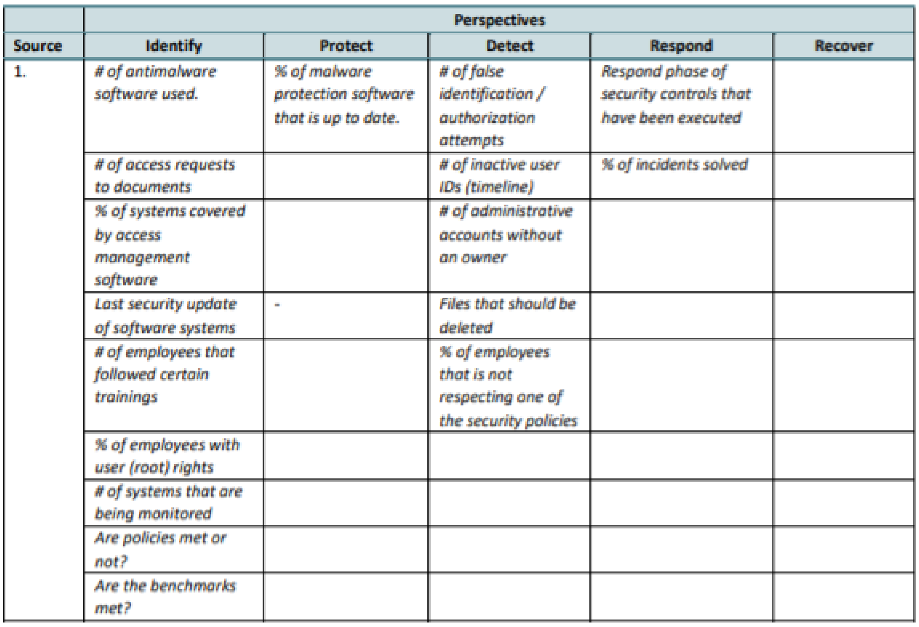
In the theory several aspects were identified in order to categorize the KPIs. All aspects form a different perspective to provide insight in security performance. These different perspectives will be summarized and organized along the relevant literature. This is shown in Figure 9.



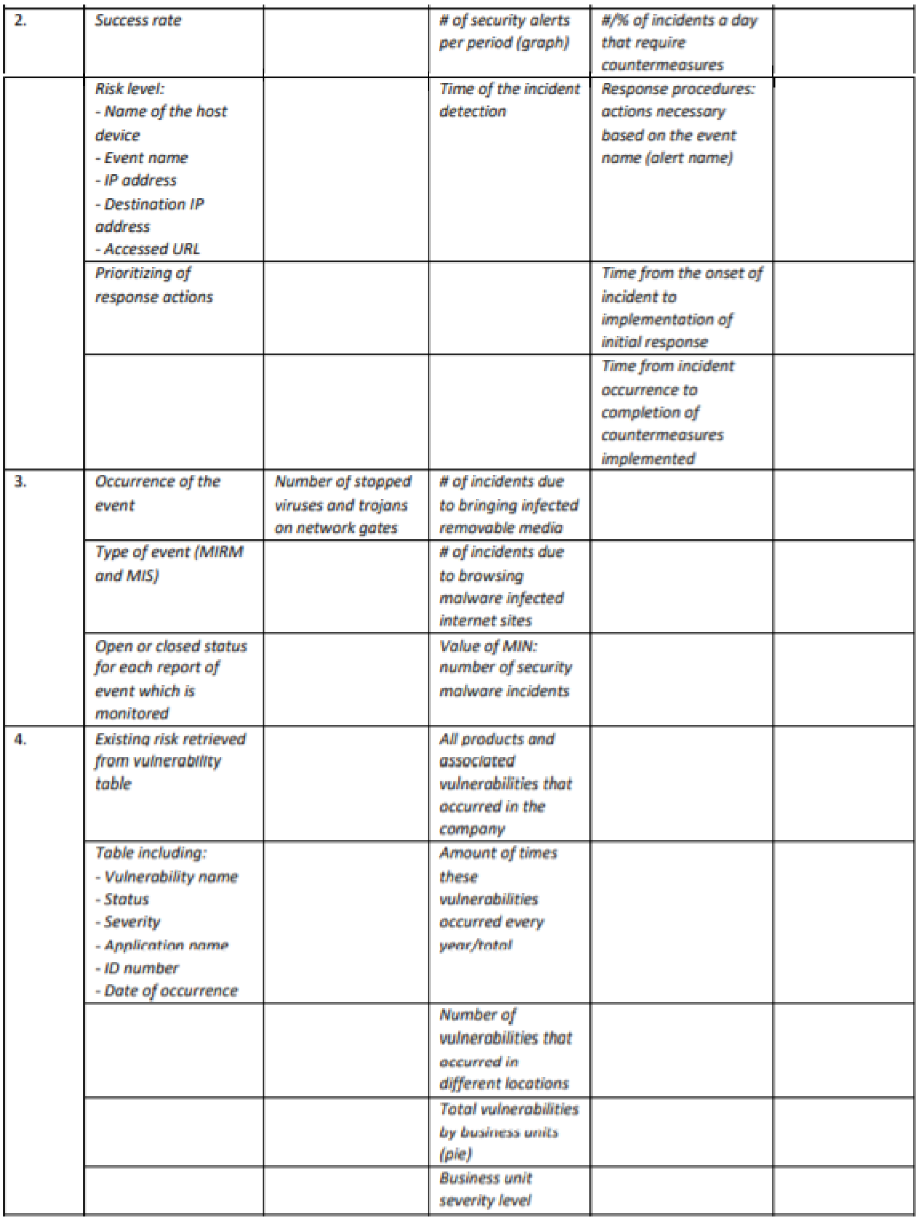
	Perspectives				
Source	Identify	Protect	Detect	Respond	Recover
1.	X	X	X	X	
2.	X		X	X	
3.	X	X	X		
4.	X		X		
5.	X	X	X	X	X
6.	X	X	X	X	X
7.		X	X		
8.	X	X	X	X	
9.	X	X	X		X

Figure 9: Perspectives from literature.

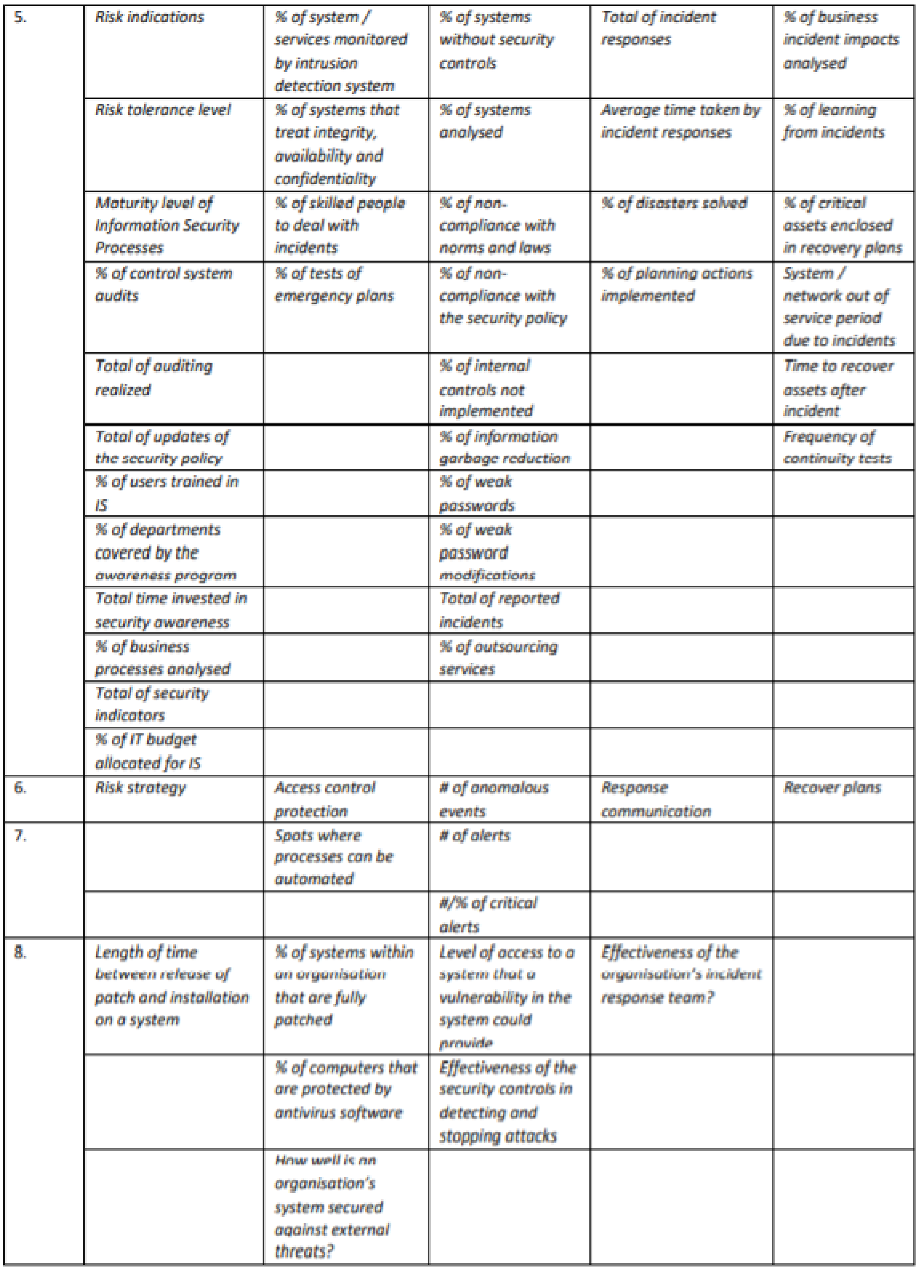
The concept-matrix providing a KPI classification and description along the NIST perspectives is included in Figure 10 below.



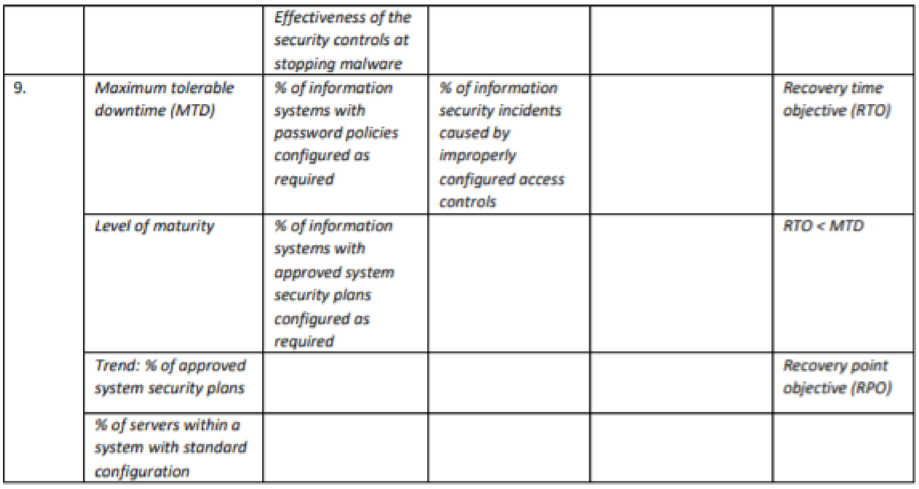
	Perspectives				
Source	Identify	Protect	Detect	Respond	Recover
1.	*# of antimalware software used.*	*% of malware protection software that is up to date.*	*# of false identification / authorization attempts*	*Respond phase of security controls that have been executed*	
	# of access requests to documents		*# of inactive user IDs (timeline)*	*% of incidents solved*	
	% of systems covered by access management software		*# of administrative accounts without an owner*		
	Last security update of software systems	-	*Files that should be deleted*		
	# of employees that followed certain trainings		*% of employees that is not respecting one of the security policies*		
	% of employees with user (root) rights				
	# of systems that are being monitored				
	Are policies met or not?				
	Are the benchmarks met?				



2.	*Success rate*		*# of security alerts per period (graph)*	*#/% of incidents a day that require countermeasures*	
	Risk level: *- Name of the host device* *- Event name* *- IP address* *- Destination IP address* *- Accessed URL*		*Time of the incident detection*	*Response procedures: actions necessary based on the event name (alert name)*	
	Prioritizing of response actions			*Time from the onset of incident to implementation of initial response*	
				Time from incident occurrence to completion of countermeasures implemented	
3.	*Occurrence of the event*	*Number of stopped viruses and trojans on network gates*	*# of incidents due to bringing infected removable media*		
	Type of event (MIRM and MIS)		*# of incidents due to browsing malware infected internet sites*		
	Open or closed status for each report of event which is monitored		*Value of MIN: number of security malware incidents*		
4.	*Existing risk retrieved from vulnerability table*		*All products and associated vulnerabilities that occurred in the company*		
	Table including: *- Vulnerability name* *- Status* *- Severity* *- Application name* *- ID number* *- Date of occurrence*		*Amount of times these vulnerabilities occurred every year/total*		
			Number of vulnerabilities that occurred in different locations		
			Total vulnerabilities by business units (pie)		
			Business unit severity level		



5.	Risk indications	% of system / services monitored by intrusion detection system	% of systems without security controls	Total of incident responses	% of business incident impacts analysed
	Risk tolerance level	% of systems that treat integrity, availability and confidentiality	% of systems analysed	Average time taken by incident responses	% of learning from incidents
	Maturity level of Information Security Processes	% of skilled people to deal with incidents	% of non-compliance with norms and laws	% of disasters solved	% of critical assets enclosed in recovery plans
	% of control system audits	% of tests of emergency plans	% of non-compliance with the security policy	% of planning actions implemented	System / network out of service period due to incidents
	Total of auditing realized		% of internal controls not implemented		Time to recover assets after incident
	Total of updates of the security policy		% of information garbage reduction		Frequency of continuity tests
	% of users trained in IS		% of weak passwords		
	% of departments covered by the awareness program		% of weak password modifications		
	Total time invested in security awareness		Total of reported incidents		
	% of business processes analysed		% of outsourcing services		
	Total of security indicators				
	% of IT budget allocated for IS				
6.	Risk strategy	Access control protection	# of anomalous events	Response communication	Recover plans
7.		Spots where processes can be automated	# of alerts		
			#/% of critical alerts		
8.	Length of time between release of patch and installation on a system	% of systems within an organisation that are fully patched	Level of access to a system that a vulnerability in the system could provide	Effectiveness of the organisation's incident response team?	
		% of computers that are protected by antivirus software	Effectiveness of the security controls in detecting and stopping attacks		
		How well is an organisation's system secured against external threats?			



		Effectiveness of the security controls at stopping malware			
9.	Maximum tolerable downtime (MTD)	% of information systems with password policies configured as required	% of information security incidents caused by improperly configured access controls		Recovery time objective (RTO)
	Level of maturity	% of information systems with approved system security plans configured as required			RTO < MTD
	Trend: % of approved system security plans				Recovery point objective (RPO)
	% of servers within a system with standard configuration				

Figure 10: Concept-matrix along the five NIST perspectives.