Change Request Risk Model

Improving The Migration Of Networks

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Engineering and Policy Analysis**

Faculty of Technology, Policy and Management

by

Thomas Broens

Student number: 4080351

To be defended in public on December 19th 2019

Graduation Committee

First supervisor: Dr.ir. G.A. Mark de Reuver - TU Delft
Second supervisor: Dr. P.W.G. Pieter Bots - TU Delft
External supervisor: Pim van Tilburg - KPN

Summary

Internet and mobile phones have become essential in our lives. Without the internet and our smart phones, large parts of our society would stop functioning or even collapse completely. It is therefore of critical importance that the service is of the highest quality and that the delivery of service is not interrupted. Telecommunication providers are responsible for exploiting and maintaining the infrastructure necessary for delivering mobile and internet connections. It is not an easy market to survive in. Competition is fierce and the clientele demands constant service of the highest quality. This is a big challenge for telecommunication providers. In order to be able to deliver the best quality, maintenance is necessary. But maintenance is often the cause of service interruption. Combined with the fact that technology is evolving at such a pace that upgrades are coming faster and faster, the demand for maintenance has never been higher. Efficiently organising these maintenance activities has therefore become a priority.

The largest telecommunication provider in the Netherlands is facing the same challenges and has therefore commissioned this research. Using KPN as a case study, the goal of this research is to expand on the knowledge of efficiently organising maintenance activities in the telecommunication sector. In the specific case of KPN, efficiently organising maintenance activities means increasing the maintenance pace, without increasing the risks of impacting clients. Currently, maintenance that can impact the clients of telecommunication providers is performed at times when the impact is lowest. It is performed during so called maintenance windows. These windows are in the middle of night, usually between 04:00 and 7:00 in the morning. Determining what type of maintenance is performed during these windows is pretty basic. If the maintenance activity has impacted the client in the last year, it will be classified as a 'Normal' change. This means it needs to be done during maintenance windows. But because the amount of maintenance is growing and it often impacts clients, the windows are getting crowded. This leads to an increase in costs and the threat of not reaching goals set by KPN. The goal of this research is to find a way to unburden the maintenance windows of less riskful activities, in order to create room for riskful maintenance activities that really need to be done during maintenance windows. To achieve this goal, the following research question is formulated:

How can the use of a low-level/micro risk model legitimise the classification of changes in the telecommunication sector, in order to make change planning more efficient?

The selected research approach to create an artifact which can answer the research question is 'Design Science Research'. By structuring the research following six activities, the necessary objectives can be defined, the artifact can be developed, the artifact can be demonstrated

and the results evaluated. Using risk based maintenance methodology, which has been proven efficient in other comparable sectors, the objective is to create a risk model which analyses maintenance activities in more detail. This can then be used to reclassify maintenance activities in such a way that they don't need to be performed during maintenance windows. The type of risk model that fits the goals of this research is a Bow tie model. Based on historic data an overview of threats, consequences and damage categories has been created for four types of maintenance activities, as well as probabilities of these threats and consequences happening. Using these probabilities, risk ratings have been calculated. The risk ratings can then be used to compare maintenance activities with each other and define classifications. The results of creating these bow tie models and calculating the risk ratings have led to four recommendations for KPN.

The first recommendation is to start recording performance data on a micro level. Performance data refers to data that shows how changes are being performed. Examples of this are reasons of failure and consequences of failure. Because this data is detailed information and varies for every change type, it classifies as micro level data. This is not yet happening at KPN and the results of this research point out that recording and using micro data can help improve the success rate of maintenance activities. Which in turn makes the change planning more efficient. The second recommendation is that to be able to fully confirm that using micro risk models legitimises classifications of changes, a more in depth evaluation is necessary. While it has been shown that compared to the current method of classification, using the a micro risk model provides more insight based on historic data, it has not yet been decisively shown that is can actually be used to achieve its initial goal: increasing the efficiency of the change planning. To prove it can actually increase the efficiency of change planning, the method most be tested on more types of changes. For that to be possible, more micro performance data needs to be recorded. The third recommendation is to make the risk rating calculations automatic. This can be achieved in several ways, such as creating a piece of software. An automated process would make using the method more applicable in the organisation. The last recommendation is to combine the results of this research (and any expansion on this research) with research in other domains. Looking at client management, contract management and process optimisation in order to improve on change planning efficiency, could provide the missing pieces of the puzzle to solve the problems KPN is facing.

Contents

List of Figures

List of Tables

Chapter 1

Introduction & approach

While a world where internet and mobile phones were not considered main necessities existed a merely 25 odd years ago, this would now be unimaginable (Castells, 2014; Sarwar & Soomro, 2013). As businesses, governments and all organisations that play a role in making day to day life as we know it possible could not function properly without internet, our whole society would collapse if the internet would disappear (Aceto, Botta, Marchetta, Persico, & Pescapé, 2018). But even 'normal' consumers would have a tough time adjusting to a life without internet. Especially considering the impact of smart phones, who made access to the internet possible for individuals even when on the move. Communicating with others would be a lot slower, research and studying would be a lot more work, any act of administration would become more complicated and the list goes on. Basically, life would get tougher to manage.

The infrastructure to make this all possible is provided by telecommunication providers. These companies lay and maintain the necessary equipment to connect users, corporate and regular, to the internet and each other. Losing connection to the internet completely would be catastrophic, but even a loss of connection for a couple of hours is considered by many as potentially problematic. Therefore maintenance of the network is an essential task performed by telecommunications companies. This creates a challenge for providers. While activities such as updates, migrations and maintenance are important to prevent outages, preforming these activities also cause disturbances in service provision. Combined with the fact that technology is developing at an ever growing pace, it results in a bigger need for maintenance activities to be performed. But the risks involved need to be managed carefully.

An issue telecommunication providers are facing because of this, is how to best organise these activities. Most corporate clients have agreements in their contract which prohibits work on the services they acquire outside of certain time windows. During those windows, providers are free to perform the activities they need do, as long as the clients are warned in advance. These windows are limited and with the amount of activities that need to be done and will need to be done in the future, they run the risk of becoming bottlenecks. Performing these activities outside of the agreed upon windows could be a potential solution, but comes paired with risks. These risks need to be carefully managed, but should not restrict efficient organisation of maintenance activities. It is in light of this that, the Koninklijke PTT Nederland N.V. (KPN), the biggest communications service provider in the Netherlands, has an interest in optimising the organisation of these activities. Therefore the goal of this thesis is to improve on the efficiency of maintenance planning in the telecommunication sector, balancing the importance of the maintenance activities with the risks. The following sections will expand on the factors that have lead to this situation. Then the core concepts used during this research are defined, which will lead to the knowledge gap that forms the foundation of the research. This will serve as the basis for the justification of the research, research questions, methods and tools.

1.1 Competitiveness in the telecommunication industry

The telecommunication market is facing many challenges. One of the main challenges is that there is fierce competition to win and retain consumers. Combined with the consumer demands and increasingly complex technologies, it is getting harder to attract new clients and keep the current clients happy (Spiess, T'Joens, Dragnea, Spencer, & Philippart, 2014). This situation is present in the consumer market, aswell as in the corporate market. Between convincing new clients to join and focusing on keeping their current client base, many companies have devoted their time in making their previous clients associated with them (Dahiya & Bhatia, 2015). The choice for this course is understandable, as a survey done in the Telecom industry and literature have shown that the cost of acquiring new customers is far higher than the cost for retaining existing ones. (Van den Poel & Lariviere, 2004; Verbeke, Dejaeger, Martens, Hur, & Baesens, 2012).

There are different ways to maintain the current client base. The main of goal of all these measures is to keep the client happy by increasing the quality of experience (QoE). In the article 'Using big data to improve customer experience and business performance' by Jeffery Spies, simple representations of the customer and communications service provider (CSP) lifecycle are given (Spiess et al., 2014). With a model proposed by Alcatel-Lucent, that represents a comprehensive view of the QoE, key drivers of customer satisfaction are identified across these lifecycles (Alcatel-Lucent, 2012).

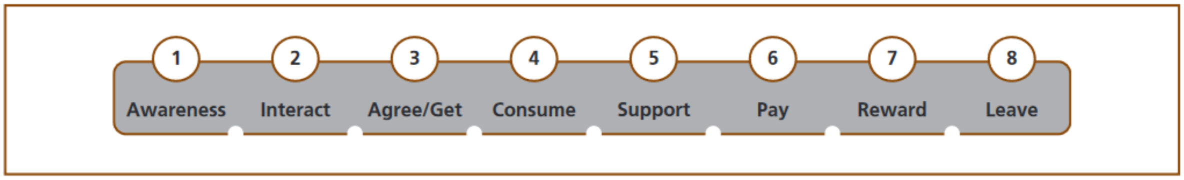


Figure 1.1: Customer Lifecycle

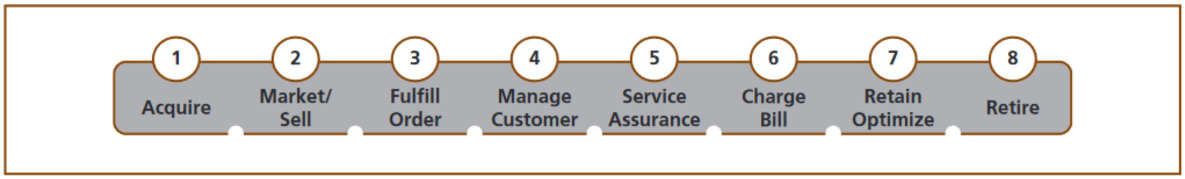


Figure 1.2: CSP Lifecycle

It is in the consume phase of the customer lifecycle (Figure 1.1) where a large component of QoE is determined (Spiess et al., 2014). This is the "in-service" experience of the client. Meaning the quality of the network, quality of the service, the performance and the ease of operation. The next important part for QoE is located in the support part. This is the "care" experience for the client. Care stands for the categories of problems that impact the customer experience. The next component of the holistic view is "perception", which relates to the the awareness, interact and reward phases of the lifecycle. A big part of this is the brands image, the perception of the offered value, loyalty programs and promotions. The last component is "ease", which touches on the agree/get phase (activation) and the pay phase.

Knowing this helps organisations in the telecommunication market to know where and what to focus on. As a large component of the QoE is determined in the "in-service" experience of the client, many organisations put a lot of effort into improving the quality of their network and services. This means trying to have clients, consumers and corporate clients, on the best possible networks. Increasing reliability, speed and quality of their connection. With the goal to have better performing networks than their competition. The main difficulty of this is the fast pace in which technology is evolving. Leading to an exponential increase in volume, velocity and variety of data from both users and communication networks (Musolesi, 2014). Meaning that new and better technology is available so fast, that organisations in the telecommunication sector are in constant need of upgrading their network to handle all this data. A consequence of this is that migrations, maintenance and upgrade activities are increasing. This was already starting to be a problem 10 to 15 years ago and is only becoming a bigger issues for the telecommunication market (Kamoun, 2005).

Another reason for wanting to migrate and update their networks is because of the amount of legacy systems that are still being used. Wanting to have the highest quality and speed is an important motivator, but decreasing the risk of network failure is just as important. Legacy systems run a higher risk of malfunctioning and potentially putting down big parts of the network. The problem of legacy systems overlaps with two other important factors for why telecommunication service providers are putting a lot of effort into network maintenance. It is important for the image of a telecommunication provider to have no failures. In case of massive or regular interruption of service, this reflects badly on the image of the provider. Which makes attracting and retaining new customers even more difficult. The second factor is power consumption of legacy systems. Estimations say that ICT is responsible for two to four percent of the world wide carbon emission (Lubritto et al., 2011; Vereecken et al., 2011). New technology is more energy efficient. With the attention on the environment having massively increased, many providers try to minimise the power consumption of their network. This also has a big impact on the image of the provider.

High costs and never ending maintenance on the network in a market were it is already difficult to thrive, are not the only concerns for the telecom providers. Another issue is the disruption of service delivery because of the maintenance performed on the network. Any form of maintenance, upgrade or migration of an old network to a new network affects the clients by creating short periods of down time. This could be a longer period when any of these activities fail and cause errors.

It is for this reason that many providers in the Netherlands make use of what is called a maintenance or service window. These windows are time slots in which maintenance work can be performed with minimal impact on users and are different for every provider. Koninklijke PTT Nederland N.V. (KPN), the biggest communications service provider in the Netherlands, have defined their time slots either between 05:00 - 07:00 or between 00:00 - 07:00, depending on the type of maintenance. The idea is that between those hours, a minimal amount of users are actively using the network. So a disturbance in service delivery or an all out failure because of maintenance work will have the least amount of impact. While this is a good idea, several problems have come up for KPN. First of all, it is difficult to find enough mechanics who are willing to work those hours. Which means not all work planned during these windows can be performed. In addition, the costs are much higher for night work than for work done during the day time. Another issue is that the time periods are fairly limited. Combined with the increasing amount of work, these maintenance windows are becoming the bottlenecks for certain goals to be reached. It is therefore that KPN is looking for a way to decrease the amount of work being done during those windows.

1.2 Maintenance activities

To understand the problem telecommunication providers are facing, one needs to understand what maintenance activities entails. A definition used by the European Federation of National Maintenance Societies (EFNMS) and inline with ISO standards, states that maintenance activities are "all actions which have the objective of retaining or restoring an item in or to a state in which it can perform its required function. These include the combination of all technical and corresponding administrative, managerial and supervisions actions"(EFMNS, 2019; ISO/IEC, 2006). These can include checks, servicing and repairs or replacing of necessary devices. All together, this has often been referred to as Maintenance, Repair and Overhaul (MRO). The four types of basic maintenance identified by MRO are preventive maintenance, corrective maintenance, predictive maintenance and reinforcement.

Translating this to the telecommunication sector and their infrastructure results in the following. Preventive maintenance would be the migration of old networks to newer networks. These types of migrations are done to improve performance by utilising newer technology and to prevent older technology from failing. Corrective maintenance is replacing equipment that has already malfunctioned. This happens for example, when older technology has not been replaced on time. Predictive and reinforcement maintenance is not used in the telecommunication sector yet.

In order to go into more detail for these type of maintenance activities, information about how this is done by telecommunications providers is necessary. But no such method, standardisation or information is available. Therefore we can only rely on informal talks at KPN, who commissioned this research. One reason for the lack of this information that is often mentioned during such talks is the competitiveness of the telecommunication market. Being able to perform maintenance and migration activities more efficiently is believed to increase the competitiveness of a telecommunication provider. The consequence of companies refraining to share this information, is that there is no research available. This means that there are only two valid sources of information. KPN themselves and other industries where research about maintenance activities are more readily available.

1.3 Core concepts

This section focuses on the concepts of maintenance and risks in the telecommunication sector. Because no public information is available on this subject, concepts used by KPN will be used to describe, quantify and explain the process of maintenance and risks management. These concepts form the foundation of the solutions to the problems KPN is facing in regards to maintenance and risks. The first concept, maintenance windows, is essential for understanding what is being researched and why. To be able to understand the delimitation of the research, understanding the KPN network is important. The last concept that is important to this research is the current policy and process in regards to the maintenance planning.

1.3.1 Maintenance windows

There are two types of windows in use by KPN, service and maintenance windows. Service windows are time periods where any kind of work is done on the network. These windows are used when work has no impact on clients, it has no risks of impacting clients, no warnings are needed and the work has been done many times before. Therefore they can be planned during the day. Meaning more mechanics are available and the hourly rate is normal/lower.

Maintenance windows are used when the work has an impact on the client, there are risks of higher impact than expected (time wise and/or extent of impact) and communication with the client is needed so they can prepare for possible disruptions. To minimise impact on the client side, these windows are planned at night. The expectation is that clients are not (less) active in the middle of the night and can therefore better process a disruption of the service. Important to note is that there has been no research done by KPN, internally or externally with clients, to determine the ideal time to perform these activities. The most common maintenance window at KPN is between 04:00 and 07:00. But depending on the type of maintenance and agreements with client, windows can vary. The hour this kind of work is performed has an impact on mechanic availability and hourly rate, as night shifts are more expensive. Another important limitation related to maintenance windows, is that because of having to work during certain time frames, the amount work that can be planned is restricted. This does not have to be a problem, but needs care full planning and clear requirements to be used efficiently.

1.3.2 Network layers

The KPN network exists out of five layers, the access layer, the metro-bridge layer, the metro-core layer, the back-bone and the ZARA layer. The 'lowest' layer, closest to the client is the access layer. Each location is around 200 to 300 clients. The metro-bridge layer aggregates different access locations. At this layer, maintenance can impact more than 10000 clients. The metro-core layer is basically the same as the metro-bridge layer, except that is is another scale level higher. Servicing even more clients. The back-bone and the ZARA layer are the 'highest' layers in the network and are the origin points of all services KPN delivers to its clients. In section 3.2.1, this is explained in more detail.

1.3.3 Change request process

Throughout the organisation departments need to be able to request changes to be made. KPN uses the 'Information Technology Infrastructure Library' (ITIL) definition for a change (Hanna & Rance, 2011, p. 12): *"The addition, modification or removal of anything that could have an effect on IT/TI services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT/TI services and other configuration items."* These requests vary from maintenance to creating new access points. The department in charge of managing all the request is called the 'Service Quality Centre' (SQC). Depended on the type of request, its risks, its impact and experience with that type of request, the request is classified. The planning and amount of security checks is based on that classification. The following types of classification exist (KPN, 2016):

- **Standard change:** A change which is pre-authorised. Requirements for a standard change are that the change has been executed successfully in the past, will be executed on regular basis, has no impact on clients, often classified as low risk and follows a predefined procedure or instruction.
- **Normal change:** A change that will follow the Change Management procedure starting with a request for change, will be authorised conform the agreed governance, afterwards the change will be planned, implemented and evaluated.
- **Emergency change:** Emergent changes are changes that must be introduced as soon as possible to resolve a major incident or to prevent a major incident.
- **Urgent change:** Urgent changes needs to be introduced before standard lead time and can wait for at least 24 hours.
- **Service request:** Generic varying types of demands that are placed upon the IT department by users.

When a change has been classified as a standard change, it means that most of the time it can be planned outside maintenance windows and won't go through severe security checks and discussions. A lists exists of the current changes that are classified as standard. For normal changes a run book is filled in and delivered with the request. An important aspect of the run book are the questions that relate to impact, experience, complexity and precautions. These criteria are measured through KPIs, of which the following are the most important:

- **Change triggered Be Alerts (CTBA):** When a situation arises which has a certain impact on service delivery for clients, has an impact on KPN or an impact on clients aswell as KPN, it is called a Be Alert. There are five levels of severity of a Be Alert, which is represented by the colour of the Be Alert. The colours that are used are green, blue, yellow, orange and red and their severity are minor, moderate, significant, major and critical respectively. The criteria that decides which colour Be Alert a problem is classified as, can be found in the classification matrix in Appendix A. Through weekly and monthly reports of how many changes and what type of changes have led to a Be Alert, the change request process is managed. This is done by looking at weighted and unweigthed numbers of change triggered Be alerts and the weighted down time because of the Be Alert.
- **First time right (FTR):** A change is considered FTR when its has been implemented in the communicated window, impacting customers as predicted and not rescheduled or cancelled after communication. When looking at IT changes, the change should have no impact on IT services and needs to be completed, without a rollback being necessary. When a change has been labelled nFTR (not First time right), it does not necessarily results in a Be-Alert. Consequences can vary from a change having to be rescheduled to a red Be-Alert,
- **Lead time:** The time between starting and finishing a change is a crucial indicator for the risk and impact of a change. This criteria also plays a role in deciding if a change needs to be done during a maintenance window, as a long lead time means a long time

when service delivery is interrupted. Changes that cause clients to be impacted for a longer time are less likely to happen during daytime.

The current way of determining the classification of a change is to look at the risks and impact. This is done from a macro perspective, as it is based on a yearly performance of a change. If a certain type of change has not resulted in client impact for over a year, it becomes eligible to be classified as a standard change. Other factors, such as reasons for a change type failing, probabilities of it happening again or the actual impact are not taken in account. While this does not create problems when there is enough room during maintenance windows, it does potentially put unnecessary pressure on the windows and increases the costs of performing the change.

1.3.4 RBM & Risk models

A method often used when discussing maintenance is 'Risk Based Maintenance' (RBM). In sectors comparable to the telecommunication sector, RBM is used to efficiently plan maintenance of machinery based on the risks of machinery malfunctioning. The risk and impact of malfunctioning machinery is compared to the impact of planned maintenance and based on the results a maintenance plan is made. To be able to compare the risks and impacts, risk models are used. Risk models describe drivers that influence the probabilities of an occurrence and of an impact (Gericke, Klimentew, & Blessing, 2009). These risk models exists of hazards, events, threats, consequences and barriers. By using those probabilities, an optimal planning can made to decrease down time and increase performance. These methods are discussed in more detail in chapter 2.

1.3.5 Conclusion

These core concepts are important to understand the problem telecommunication providers are facing. The usage of the maintenance windows in the change request process and the location of the maintenance works all play a big role in managing the risks and impact of maintenance work. While the details have been taken from KPN, all telecommunication providers face the same kind of problem, in which these concepts play an essential role. Applying relevant methodology and theory in order to improve performance is the next step.

1.4 Research gap & research questions

The following section will discuss the research gap and the research questions that were inferred from the research gap. This section will also be used to discuss the practicable problem that this research is trying to solve.

1.4.1 Research gap

Maintenance of the hardware and software that make the network of telecommunication providers run is essential for qualitative service delivery. Managing the risk and impact that maintenance carries with it is equally important. Looking at comparable sectors shows that there is an abundance of literature that looks into maintenance and risk management. Surprisingly enough, this is not the case for the telecommunication sector. Using risk based maintenance (RBM) as main search term results in a lot of literature. There are many different papers on RBM methodology, each with examples from different sectors. But when combined with terms related to the telecommunication sector, there are no results related to risk based maintenance. While there is much to find about the competitiveness of the market and the important role the quality of the network plays in it (Dahiya & Bhatia, 2015; Spiess et al., 2014; Van den Poel & Lariviere, 2004; Verbeke et al., 2012), optimising the upgrade and maintenance of the network is not much discussed.

This research has been commissioned by KPN because of the problems they experience in practice organising maintenance. The maintenance workload of KPN is increasing and the current method of determining risks and impact is leading to overfull maintenance windows. This is slowing down maintenance goals and is all over a less efficient way of working. Maintenance windows are more expensive and are limited in time compared to day time windows. One of the main reasons that in the current way of determining risks and impact, maintenance windows are not being used effectively, is that risks and impact are determined on a macro scale level. This has as a result that many changes are not performed as efficiently as possible, as well as that changes the might not need to be planned during maintenance windows are still planned during maintenance windows. In order to be able to change the classification of those changes, the method to determine risks and impact needs to legitimise a change in classification. Because the current method does not provide any means to legitimise new classifications based on more detailed information, a new method needs to be used.

Therefore the goal of this research is to use existing literature of other sectors to develop/extend on risk based maintenance planning on a micro scale for KPN. By testing this method at KPN, new insights can be generated for risk and maintenance management in the telecommunication sector. The results can be used in two ways. This research expands on RBM methodology within a new sector and depending on the results gives an idea if it is a viable methodology for the sector. The second way it expands on literature is that in current RBM methodology, the planning phase is focused on maintenance that impacts internal procedures. In the telecommunication sector the risks and impact that are being managed are focused on external impact. This results in a different focus and therefore outcome of the method. Whereas in standard RBM the result is a maintenance schedule based on the results of the risk assessment, the results of this research will be a way for telecommunication providers to classify their changes based on risks. Which in turn will affect how maintenance is planned in the future.

As KPN is the largest telecommunication provider in the Netherlands that is facing difficulties with their maintenance planning, this case is well suited to create and test similar methods as used in comparable sectors.

1.4.2 Research questions

With the problem, concepts and research goals being set, the research questions and objective for this thesis can be formulated. In order to find an answer to the main research question, several sub questions will be answered first. They will help form the structure which will help answer the main question.

The main goal of this research is to improve change planning in the telecommunication sector by implementing Risk Based Maintenance methodology. Thereby extending on RBM methodology in the telecommunication sector by providing an example of RBM being implemented in this sector. To achieve this a risk model is developed that entails the risk assessment steps discussed in RBM literature. This risk model (adjusted to the company) can then be used by telecommunication providers to help them classify their changes. For this thesis, the case of KPN is used, making the model in this research tailored to KPN's context. The risk model can then be used to answer the main research question of this thesis.

How can the use of a low-level/micro risk model legitimise the classification of changes in the telecommunication sector, in order to make change planning more efficient?

Making the change planning more efficient can mean different things. The Oxford dictionary defines efficient as *"achieving maximum productivity with minimum wasted effort or expense"*. Being able to classify changes based on a micro level of detail can lead to productivity increase and will lead to a decrease of effort and expense. The first way this can lead to an increase in productivity, is that by working on a micro scale provides insight into what is causing a change to be performed nFTR. Action can then be undertaken to improve on these causes. The second way it can increase productivity is by giving numerical substantiation for a change to be reclassified. Meaning changes that are currently being planned in maintenance windows, while their risks and impacts don't need them to be, can be planned during the day. Opening up space for other changes in the maintenance windows and increasing the amount of work that can be done. The sub questions that help answer the main research question are as follows.

Sub questions:

1. **What micro risk model is appropriate to achieve the required results?**

   In the world of risk assessment there are many different risk models that each have their advantages and disadvantages. In order to determine which model can best be used for this research, the researchers need to look at the available information and the desired results and insight.

2. **What information is needed to create the risk model?**

   (a) *What kind of changes exist and how do they differ?*

   In order to make a risk model, different information is necessary. The first step is to determine what is going to be modelled. In this case, the goal is to make risk models for a selection of changes that have been chosen to represent most changes done at KPN. This means that an overview of all changes has to be made in order to be able to make a representative selection.

   (b) *What hazards, events, threats and consequences are identified for the different changes?*

   For each of the selected changes, the components of the risk model need to be identified. As shortly discussed in section 1.3.4, those are hazards, events, threats and consequences. This will provide the necessary insight into improving FTR percentages.

(c) *What are the chances of these threats and consequences happening and what is their potential impact?*

The next step in the risk model is determining the probabilities of each threat and consequences happening and what their potential impact is. This makes it possible to compare the risks and impact of changes.

(d) *What barriers are in place and what barriers could be put in place?*

Barriers are another component of some risk models. The give extra insight into what is already been done to prevent or mitigate threats and consequences. Determining what barriers are in place to prevent or mitigate threats and consequences is important to determine what can still be done to improve.

(e) *What are acceptable risks for KPN?*

Based on the risk level KPN finds acceptable and the results of the risk model, classification of changes can be made.

3. **How does a micro risk model help classify changes differently?**

   The current macro method of determining the classification of changes is resulting in complications for KPN. Comparing it to the new micro method, using the created risk models, will show how it improves on the current method and increase efficiency.

4. **How does changing classification of changes make change planning more efficient?**

   The goal of the the risk model is to help improve how changes are classified. But it needs to be clear in what way this helps to more efficient. Answering this question, in combination with the answer to how the new model improves change classification compared to the old method, explains the value of this model.

5. **Does the risk model legitimise changing the classification of changes?**

   For this model and method to be used, managers need to trust the results. This means that in someway, the model needs to legitimise changes in the current classification. As in the current way of working, risk and impact are minimised at the cost of efficiency, while the new method tries to increase efficiency at a minimal cost of risk. Answering this question is crucial for its practical implementation.

The second question consists of five sub questions, which will lead to the construction of a risk model. The risk model itself has two functions that will help improve efficiency of change planning:

1. Provide insight in what can be done to improve current change activity in maintenance windows.

2. Provide numerical substantiation for discussions about why certain changes have to be planned during maintenance windows and others don't.

The first point relates to the information that is gathered to be able to create the model. Identifying all the threats of a type of change, calculating for each of them how often they lead to a failed migration and the possible consequences gives insight in how your current approach is functioning. Knowing this, gives the user of the model (most likely the project manager in charge of this migration) the necessary information to act and improve. The user will know on what kind threat he will need to focus to increase his success rate, in turn wasting less effort and expenses.

After expanding the model with statistics, calculation can be done to calculate chances. These can be further used to give risk and impact ratings to different types of changes. Comparing these rating can then lead to new classification of changes based on a companies threshold value for risks. This can be used to define how much of risk a company is willing to take to be able to perform maintenance and migrations more efficiently. This is useful as it makes comparing different types of changes easier.

1.5 Approach and method

Now that it is clear what the problem is and what the scope of the research entails, the next section will explain what method and steps will be taken to create a more extensive risk model.

1.5.1 Research approach

The selected research approach to address the research question is the design science research (DSR) approach. Design science has been defined as *"a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem"* by Alan Hevner and Samir Chatterjee (Hevner & Chatterjee, 2010, p. 5). Design science research has been an important paradigm of information systems and its acceptance as a legitimate approach to IS research is increasing (Gregor & Hevner, 2013).

In *"positioning Design Science Research for Maximum Impact"* by Gregor and Hevner, a DSR knowledge contribution framework is presented (Gregor & Hevner, 2013). Based on the solution maturity and application domain maturity, a 2 by 2 matrix of research projects contexts is created. The quadrant created when the solution maturity is high and the application domain maturity is low is called the Exaptation quadrant. Research where knowledge and solutions of other sectors is refined and used in a new sector falls into this category. As other sectors than the telecommunication sector have successfully used RBM and one of the goals of this research is to improve a part of the the maintenance process, it was fitting to use this methodology in order to adapt RBM to be useful in a new field. The artefact being the new process, based on a risk model.

There are several different DSR approaches developed for information system research. One methodology presented by Peffers et al in 'A Design Science Research Methodology for Information Systems Research' suggests six activities for carrying out research based on design science research principles (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). These activities are problem identification and motivation, defining the objectives for a solution, design and development, demonstration, evaluation and communication. A brief explanation will be given for each activity. An explanation of how this will be implemented for this research question will follow.

Activity 1. Problem identification and motivation. During this activity a specific research problem is formulated. This research problem will serve as a basis for developing an artefact. The goal of the artefact is to provide an effective solution. In order to achieve this, knowledge of the state of the problem and the value of solving it is necessary. No literature exists on risk based maintenance for the telecommunication sector. Combined with the knowledge that maintenance for telecommunication providers is difficult and that there is a lot of competition for clients, the lack of research in this methodology is problematic. Case related information can be added to this, which is that KPN is struggling with performing their maintenance efficiently. All of this information leads to the problem of maintenance planning in the telecommunication sector. Comparable sectors used RBM to increase efficiency, therefore the lack of research and implementation of RBM in this sector is problematic.

Activity 2. Define the objectives for a solution. The second activity serves to define what solutions are possible and feasible. The objectives can be quantitative or qualitative. This helps define what data collection will be necessary. The goal of the created artefact is to improve the change request processes in such a way, that it will help relieve the maintenance windows. One way to achieve this, is by improving the request processes through the usage of data. By using known data like risks and impact of a change request, the improved processes will be able to distinguish what change request need to be handled during maintenance windows. But more importantly, which change requests don't need to happen during the maintenance windows. For this to be successful, the current process will need to be analysed, data about risks and impact will need to be gathered and a risk analysis framework will need to be put in place. This activity provides the theory and sets all the conditions for answering sub question one.

Activity 3. Design and development. The core activity in any design science discipline is designing and developing the artifact. Such an artifact can be any designed object, that contributes to solving the problem, as well as contributes to literature. To be able to this, its desired functionality and architecture need to be determined. The desired artifact for KPN is a risk analysis model which can be used to compare risks and impact of different changes. By collecting historic data about the changes that have already been performed in the past, all hazards, threats and consequences can be identified. Based on that information, classifications can be made of changes that need to be performed in and outside of maintenance windows, which could help relieve the maintenance windows. Activity three provides the answers to sub question two.

Activity 4. Demonstration. When the artifact has been developed, a demonstration through experimentation, simulation, case study or other appropriate activities must be done to show that it works. Important to do this activity right, is to know how to best use/implement the artifact to solve the problem. To demonstrate the new risk model, the four types of migration activities are given a rating calculated by the new model. These ratings can then be used to reclassify these migrations as standard or normal changes. Showing that if the necessary data is collected and put into the model, calculations can be made to give each type of migration a rating on which they can be classified. By demonstrating how the model rates changes and how the rates can be compared, sub question 3 is answered.

Activity 5. Evaluation. The evaluation activity is needed to evaluate if the created artefact actually contributes to solving the problem. To evaluate the effectiveness of the new risk model, a comparison is made between the old risk classification and the new risk rating. This will show if the new risk model results match with the old model, while also showing how they are different. The main objective of the new process would be to reduce the amount of work planned during maintenance windows. That would be the first evaluation criteria for comparing the solution objectives to the functionality of the artifact. Based on the result, the decision can be made to return to activity three to improve the artifact or to continue to the next activity. Evaluating the model and its results provides the answer to sub question four. Comparing the new process and the old process shows how changing the classification can improve the efficiency of the change planning. By combining the theory, the demonstration and the evaluation an answer can be formulated to sub question five.

Activity 6. Communication. The results of the whole process need to be communicated to all relevant audiences. The problem, its importance, the artifact, its effectiveness and its utility. This can be used by practising professionals as well as by other researchers. In this case, the relevant audiences are the professionals at KPN that might implement the new risk model and the academic community that might want to use this research. The way the results will be communicated is by a a report in the form of a thesis.

To summarise, the fist step will be a literature research into risk management and risk based maintenance in different sectors. This will result in a specific research problem. The second step will be to define the objectives and methods to reach those objectives. Step three will be creating the artifact that has been chosen to reach the set objectives. In this case, that will be a risk model intended to rate different types of changes in order to classify them. Step four will be performing the calculation to rate the four example change types. The results will be ratings and impact on different damage categories. Step five will consist of comparing these results with the current method and classification. Concluding en reflecting in step six about this research's limitations and results.

1.6 Structure

The activities described in section 1.5.1 will form the structure of this research. Chapter one and two contain activity one and provides the necessary context for activity two. In these chapters the problem identification and motivation is given, as well as the necessary background to provide theory and objectives for a solution. Chapter three describes the case related context, necessary to understand and define the objectives for solving the problem KPN is facing. Therefore it contains activity two. Chapter four will contain activity three and four, design and development and the demonstration respectively. The information from chapter three is implemented in the model, which is explained in chapter two. This will be done for the selected changes. Chapter five will contain the evaluation activity, which will be comparing the new model and methodology with the old way of working. This will be followed by chapter six, containing the answers to the research questions and the conclusions. The last chapter will contain the communication activity as well as a reflection. This will be in the form of recommendations and limitations of the research. This structure can be seen in Figure 1.3.

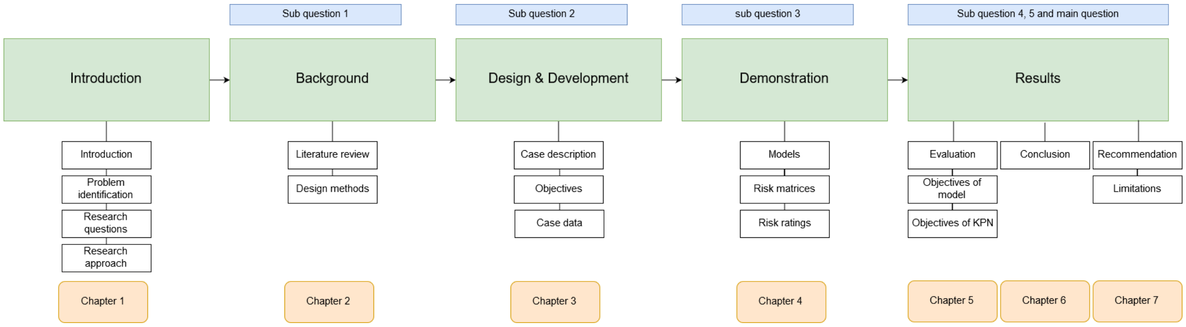


Figure 1.3: Structure of thesis

Chapter 2

Background

This chapter covers the literature needed to understand the problem and the methods used during the research. It helps put the problem and its possible solutions in context. The theory needed to answer sub questions one and two is explained here.

2.1 Risk management and maintenance in general

Organising maintenance activities and managing risks is an essential task for telecommunication providers. But there are many other sectors where this plays a big role. Looking into how these sectors organise their maintenance activities can provide insight in what could work for the telecommunication sector and why this has not played a bigger role yet in the telecommunication market. Therefore a comparison of how other sectors manage their maintenance activities and risks will be detailed. The focus will be put into comparable sectors. These are service based businesses such as the energy production sector.

The energy sector has a comparable network and service to the telecommunication sector. Clients pay a monthly fee to receive the service, in this case electricity, gas, internet and mobile connectivity. This is provided by equipment and an infrastructure network in hands of the providers. A difference is that in the energy market, the infrastructure network is often the responsibility of another party, while in telecommunication sector the infrastructure is a big part of the equipment. A large amount of money is spent in maintenance of production equipment. For the US industries, it is estimated that over $300 billion is spent each year on maintenance. This is the case, while it has been proven that a reduction in operating costs of about 40-60% is obtainable through maintenance strategies (Dhillon, 2002).

That is why Risk-based maintenance methodology (RBM) has been designed and implemented. It is a tool used to reduce the chance of equipment failure. Thereby reducing the probability of consequences due to failure. RBM achieves this by supporting maintenance planning and decision making (Krishnasamy, Khan, & Haddara, 2005). The idea is to identify the scope of the system, make a risk assessment and do a risk evaluation. Based on the results the maintenance planning can be optimised. Meaning that the probability of failure is affected through changing the maintenance interval. In turn influencing the risk. It can also be used to look at how maintenance is done. The purpose of that is to understand what leads to failure during maintenance, what the consequences are and how these can be mitigated and/or prevented.

A sector that also uses RBM is the oil and gas sector. Offshore production platforms operate wells and separate fluid form those wells into oil, gas and water. This is done by using different kinds of machinery. Each of these machines can break down, slowing down the process and potentially causing harm. This harm can be done to people, nature or other equipment. In order to minimise the risk of that happening and optimising maintenance RBM is used (Bhandari, Arzaghi, Abbassi, Garaniya, & Khan, 2016).

Comparable to offshore oil platforms are offshore windmills. The operation and maintenance costs of offshore wind turbines are a major contributor to the energy cost (Nielsen & Sorensen, 2011). Corrective maintenance is mostly used, as it is the most simple strategy. But as minor parts malfunctioning can damage bigger parts and thereby increase the repair/replacement cost, it is paired with larger uncertainty than preventive maintenance. Research has shown that doing risk based preventive maintenance, decreases the amount of corrective maintenance, decreasing total costs (Sorensen, 2009).

Another business sector where risk management plays an important role is the construction industry. Everyone knows of construction projects that have exceeded the budget and time frame that were set for the projects. This is a major issue in the business and has therefore generated a lot of attention. There are many books, papers and research to be found about how to best manage risk for construction projects. Many agree that risk assessment plays a critical role in managing risk. (KarimiAzari, Mousavi, Mousavi, & Hosseini, 2011). An important difference here is that maintenance does not play a role in the risks. They do however, make use of risk assessment techniques to decrease and control risks.

The important difference with these sectors compared to the telecommunication sector, is that most risk management and maintenance planning in these sectors are done to reduce expenditure. Whereas the main motivation in the telecommunication sector for risk and maintenance planning is to reduce impact on the client. There is a financial motivation aswell, because failing to deliver service to clients can lead to fines. But the main fear is the impact on reputation. The telecommunication sector is very competitive and losing clients to the competition because of a bad reputation is a real risk, as discussed in section 1.1. It is therefore that maintaining hardware, software and the network is crucial. But maintenance activities come with risks of also impacting the clients. This situation shows how important risk and maintenance planning is for telecommunication providers. That is why it is surprising that there is almost no literature on risk management of maintenance planning in this sector. While literature can be found on other forms of risk management in the telecommunication sector. Examples of this are focused mainly on information security, such as *"Sector-Based Improvement of the Information Security Risk Management Process in the Context of Telecommunications Regulation"* by Mayer et al. (Mayer, Aubert, Cholez, & Grandry, 2013). Other forms of risk management include compliance, technical, reputational, competition, health, country, asset impairment, liquidity, exchange rate, counterparty, interest rate, equity, corporate governance, personnel, credit, market, weather and fraud risk as discussed in *"Risk Management and Sustainable Development of Telecommunications Companies"* by Gandini et al. (2014) (Gandini, Bosetti, & Almici, 2014).

2.2 Risk based maintenance methodology

Risk management has been defined by ISO (The international Organisation for Standardisation) as "coordinated activities to direct and control organisation with regards to risk", where risk is defined as an "effect of uncertainty on objectives" (ISO 31000: 2018, 2018). A crucial element for successful risk management is risk assessment. This is defined as the "overall process of risk analysis and risk evaluation" (Rausand, 2013). Where risk analysis exists out of risk identification and risk estimation, as can be seen in Figure 2.1 (White, 1995). This section discusses RBM, a risk management method, in more detail. Certain methods that are relevant to this research are expanded on.

2.2.1 RBM

As shortly mentioned in section 2.1, risk based maintenance methodology has been designed to manage the risks and costs of maintenance more efficiently. It was first proposed in 2003 by Faisal Khan and Mahmoud Haddara in *"Risk-based maintenance (RBM): a quantitative approach for maintenance/inspection scheduling and planning"* (Khan & Haddara, 2003). According to this paper, the goal was to be be able to answer five questions related to integrity and fault free operation of the system:

1. What can cause the system to fail?
2. How can it cause the system to fail?
3. What would be the consequence if it fails?
4. How probable is it to occur?
5. How frequent an inspection/maintenance of what components would avert such failure?

Answering these five questions can lead to cost effective maintenance and minimising the consequences of a failure. The way to answer these questions is to follow the proposed methodology. It consists of three main modules: risk estimation module, risk evaluation module and maintenance planning module (Khan & Haddara, 2004). Each of these modules exists out of several steps. These modules can be split into two main phases, risk assessment and maintenance planning based on risk. The first two modules are part of the risk assessment phase and the third module is the maintenance planning(Arunraj & Maiti, 2007). It is the risk assessment phase that is the most relevant for this research. RBM was initially designed for plants and equipment, making the maintenance planning phase less relevant for the telecommunication market. The difference between both sectors is that most maintenance in plants has an internal impact, while maintenance in the telecommunication sector often impacts the clients. This makes the planning phase in RBM less interesting for the telecommunications sector, as it does not account for client impact. Therefore the steps in the risk assessment phase will be discussed in more detail.

2.2.2 Risk assessment

Risk has been defined by Kushnir as *"the considered expected loss or damage associated with the occurrence of a possible undesired event"* (Kushnir, 1985, p. 183). The goal of performing a risk assessment is to identify potential threats, estimate their likelihood and estimating the consequences. This can be done quantitatively or qualitatively. Choosing which is more appropriate depends on the cost and the availability of the necessary data or information. Arunraj and Maiti share a list of risk analysis methodologies in their paper, categorised into deterministic approach, probabilistic approach and a combination of both approaches (Arunraj & Maiti, 2007). The methods that have been selected to be used in this research are discussed in the following sections.

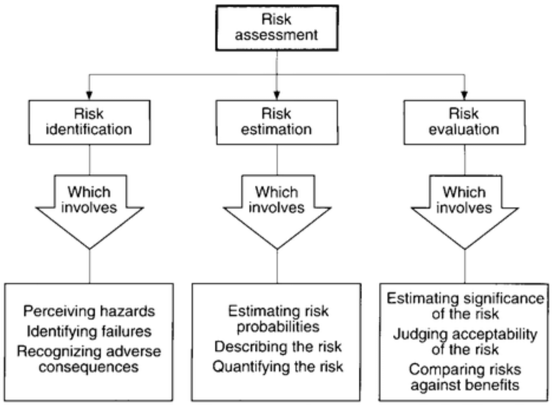


Figure 2.1: The process of risk assessment

Fault tree analysis

A Fault tree analysis (FTA) is a directed acyclic graph. This means that it is a finite directed graph. It consists of two types of nodes, events and gates. The top events is located at the top of the tree and is the event being analysed. Gates are used to model what combination of events propagate through the system, eventually leading to the top event (Ruijters & Stoelinga, 2015). This systematic method encourages analyst to identify what events or conditions can lead to undesired outcomes (Jain, Pasman, Waldram, Pistikopoulos, & Mannan, 2018). In the case of FTA, the focus in on identifying causes of potential failures (Ray-Bennett, 2018). The main goal is to provide qualitative insights, but the series of events can be quantified if necessary, to allow probabilities of events to be obtained (Anvarifar, Voorendt, Zevenbergen, & Thissen, 2017).

There are several difficulties when performing a FTA. Analyst need to have a good understanding of the system, the cause-effect process and the possible failures (de Oliveira, Marins, Rocha, & Salomon, 2017). This approach also assumes that each branch exists out of mutually exclusive, independent events. As failures seldom have a single cause, FTA can fail to identify common cause failures (Ray-Bennett, 2018). Fault tree, aswell as event trees, are simplified models of systems. They cut down systems in to detailed, separate parts, which has as a consequence that emergent properties from the whole system can go unrecognised(Jain et al., 2018).

Event tree analysis

An event tree analysis (ETA) is used to develop the consequences of an event. It starts with an event (often taken from a FTA) and the possible consequences for it. This can be done qualitatively or quantitatively, where the event is often expressed as a frequency and the subsequent splits as probabilities (Lees, 2012). Just like with a FTA, the main difficulties lie in the need of having a thorough understanding of the system, the cause-effect process and the possible failures.

Bowtie diagrams

The bowtie diagram is a combination of the FTA and the ETA and adds to it in the form of barrier thinking (CGE Risk Management Solutions, 2015). The left part of the bow-tie diagram is a simplified fault tree analysis. This leads to the top event of the Event tree, which is shown in the right part of the bow-tie diagram in a simplified form. Added to both part parts are barriers. In the left part, barriers are preventive measures, focused on preventing the threats from happening. On the right, barriers are recovery measures, focused on mitigating the consequences and/or the resulting losses and damage. Escalation factors and escalation barriers can then be added. Escalation factors are factors that make barriers fail. The main goal of a bow-tie diagram it to communicate, qualitatively, the risk. It is possible to add quantification to a bow-tie diagram, just like with a FTA or an ETA, but the limitations of this need to be taken into account. Combined with risk matrices and other techniques such as ALARP (As low as Reasonably Practicable), a overview can be given of what measures can best be taken to decrease risk and increase productivity.

2.3 Design & Development

This section explains the Bow-tie model in detail. To understand the results that will be discussed in the following chapters, it is important to have a good understanding of how the bow-tie model works and where the data in the model originates from.

2.3.1 Basic bowtie diagram

As explained in section 2.2, a bowtie model combines a fault tree and an event tree analysis. This means that on one side of the model there will be threats and on the other side consequences. The middle consists of what is called a hazard and a top event. This is the starting point for any bow-tie model. When this is complete for a top event, barriers and escalations barriers can be added to the model to finish a basic bow-tie model. To completely understand what these terms mean and how they interact with each other, an example is given in figure 2.2 which is followed by a detailed explanation of each facet of the diagram.

- **Hazard:** While they have a negative connotation in daily life, a hazard in a bowtie diagram is part of normal business. It is a situation that is necessary for a business to work, but because of this situation there exists the possibility for harm to occur. Examples of hazards are operating machinery or working with chemicals. They will not lead to harm as long as they are under control, but there are ways for them to do harm.

- **Top event:** The event leading to the point that a hazard is not under control anymore is called the top event. The moment a normal situation turns into an abnormal situation. Nothing has has happened yet, but the company is exposed to potential harm. The situation can still be brought back into control.

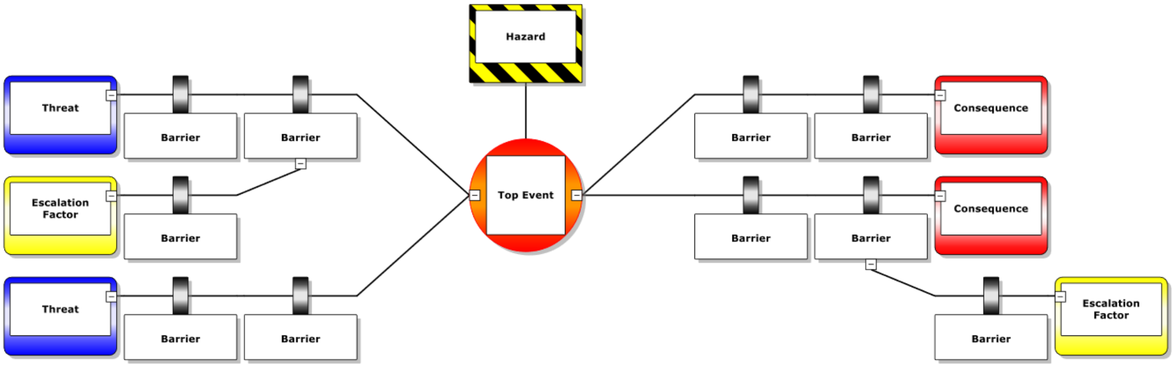


Figure 2.2: Example bowtie diagram showing all elements (CGE Risk Management Solutions, 2015)

- **Threat:** Factors leading to the top event are called threats. Threats lead directly to top events and do that independently of each other.
- **Consequence:** Any unwanted scenario after the top event happening, caused by the loss of control, is called a consequence. They are unwanted because consequences lead to losses and/or damages.
- **Barrier:** To make sure the top event is not reached, so control is not lost, preventive barriers can be put in place. These can take the form of hardware systems, design aspects, human behaviour, etc. When the top event is reached and control is lost, recovery barriers can be put in place to prevent consequences or mitigate them.
- **Escalation Factor:** These are the last facet of a basic bowtie. When preventive or recovery barriers have been identified, escalation factors can be determined. These are factors or conditions that make it more likely that a barrier fails. Escalation factors can also have barriers put in place for them.

A basic bowtie diagram containing all these parts can already be put to use. The process of gathering the necessary information and putting it into the diagram gives a easy to understand overview of the situation. Having identified what possible threats are and the current barriers in place (or not in place) to prevent them shows where potential improvements can be made. The same can be said for the consequences side, as seeing what the potential consequences are and what is in place to prevent or mitigate them gives a good impression of where improvements are possible. In the case that more information is necessary to be able to make decisions, such as the impact of certain consequences, more details can be added to the diagram.

2.3.2 Detailed bowtie diagram

When a mere overview of the hazard is not enough, more detail in the form of a risk assessment can be added to a bowtie diagram. Often with a bowtie diagram, the concept of ALARP (As Low As Reasonably Practicable) is used. Risk can always be reduced further, but depending on the cost and impact this can become impracticable. Therefore the amount of risk is a trade-off between what is possible with available resources, the amount of risk reduction and the original risk (Baybutt, 2014). As the main idea of the bowtie diagram is to identify and determine what barriers are in place and what barriers could be put in place, ALARP can be used to see if the cost (time, money, trouble) of adding a new barrier is acceptable. This is done by looking at the inherent risk level, the risk reduction gained by introducing a new barrier for that risk and the cost in time, money and trouble needed to implement that new barrier.

Combining the concept of ALARP with a bowtie is a process of five steps. Steps one to three are for determining current risks and risks reduction. Steps four to five are for conducting the ALARP evaluation.

1. Determine the inherent risk present in the bowtie
2. Identify the risk reduction achieved by existing barriers.
3. Determine the residual risk by adjusting the inherent risk with the risk reduction of the barriers.
4. Investigate additional barriers to reduce risks further and estimate the cost to implement them.
5. Weigh the residual risk against risk reduction and cost of additional barriers to determine if the residual risk is ALARP or additional barriers need to be implemented.

To determine the inherent risk for the threat side (left side) of the diagram, two aspects need to be taken in account. The likelihood of the threat occurring and its causal power. The causal power of a threat is an indication of how likely the top event will occur if the threat occurs. These two combined give an idea of how serious a specific threat is. On the consequence side of the diagram it is similar. The top event has the same likelihood for each consequence, but a different causal power. This difference leads to different scores of likelihood on each consequence. Then comes the damage caused by each consequence on different categories. The classic four categories are people, assets, environment and reputation. These scores are then put into a risk matrix of which the two axes are likelihood and severity. This is visualised in the Figure 2.3 and Figure 2.4.

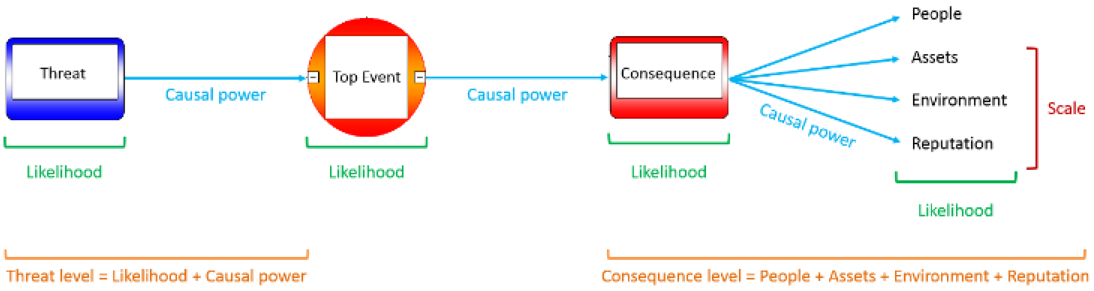


Figure 2.3: Causality bow tie diagram (CGE Risk Management Solutions, 2015)

Having determined the inherent risk, the net step is to determine the residual risk by looking at potential risk reduction through implementing new barriers. Adding barrier to the left side of the diagram will lower the likelihood of the top event or threat happening, indirectly lowering the likelihood of all consequences. Adding a barrier to the right side of the diagram will directly influence the consequence the barrier is added to. This will either prevent the consequence of happening, or mitigate the damage done. Influencing the likelihood will reduce the risk of something happening, while mitigating measures will impact the scale or likelihood of the damage. Bringing this together and determining the cost of implementing new barriers is the final step to be able to decide if the risks are ALARP or not. If a risk is determined to be ALARP, no action is necessary. When the risk is not considered ALARP, a selection of barriers can be implemented. As this is not an exact science, there is a grey area where the three variables (residual risk, estimated risk reduction and the cost to implement) interact.

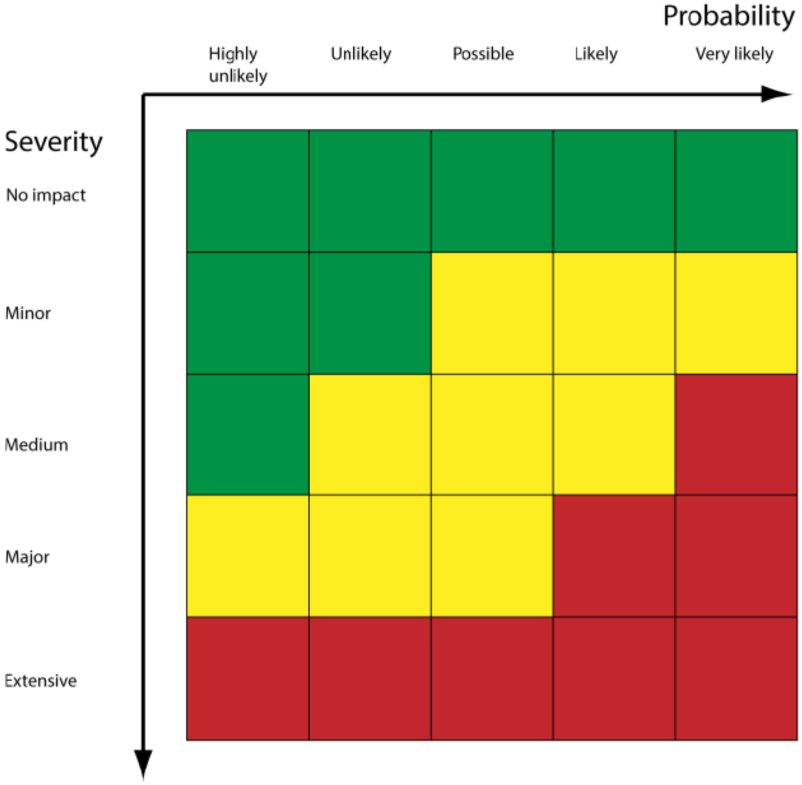


Figure 2.4: Example of a risk matrix (CGE Risk Management Solutions, 2015)

The bow tie diagram is, as its main function, a visualisation tool. A well made bow tie diagram should be able to communicate the threats, events, barriers and consequences to somebody that is not an expert. Creating a complete overview of either the current situation or an improved situation of a hazard in the business. Therefore there are many options to add more detail to the diagram. Examples of this are classifications of the severity of consequences or the effectiveness of barriers. While filling in these details in the diagram can be useful to communicate more details, modellers should not forget that showing more details can also lead to unnecessarily complicating the model. The most useful and most used options are explained below:

- **Linking management system activities to barrier:** A management system is a collection of all documentation to ensure safe operations. A bow tie diagram provides an option to link relevant parts of management systems to barriers. This is used to create insight in how the company ensures adequate operation and availability.

- **Barrier categories:** Barriers can be classified into five categories. These are Behavioural, socio-technical, active hardware, continuous hardware and passive hardware.
- **Barrier responsible person:** The name of the responsible person can be added to a barrier.
- **Barrier effectiveness:** Through a colouring scheme the effectiveness of a barrier can be shown. Effectiveness is defined as reliability and adequacy.
- **Category of a threat:** Threats can be categorised based on their contribution.
- **Type of a threat:** Threats can be given a type.
- **Frequency of a threat:** Threats can be given a frequency.
- **Category of a consequence:** Consequence can be categorised based on their level of concern.
- **Type of a consequence:** Consequences can be given a type.
- **Risk assessment:** The risk assessment part can be added to consequences. This means that for each risk matrix made, a level of risk can be determined for that consequence. This is done for each damage category.

After having added all the information to the diagram, the modeller can choose what level of detail to show. The information can also be exported in different parts if the amount of information is cluttering the total picture.

2.4 Risk management in the telecommunication industry

The techniques described above and risk management overall have been used for a long time in many sectors. While risk management, in many forms, plays a big role in supply chain, banking, healthcare, projects, construction, financial institutions,power plants and other sectors, not much can be found about it in the telecommunication sector. Especially when comparing service based industries such as construction, power plants and telecommunications, where maintenance and maintenance planning are essential parts of the business models and processes, it is remarkable that no research is available or has been conducted in risk management for maintenance in the telecommunication sector.

To say that risk management is not used in telecommunication is an exaggeration. In contrary, when discussed with telecommunication provider employees they state it plays a big role. But the lack of research on maintenance planning and its risks is a big gap in the current literature. It is in this aspect that the research will add to the literature. Focusing on how risk management in maintenance planning can help the continuation of service delivery, reduce the down time and reduce this risks and impact of changes.

Chapter 3

Case & Objectives

The following chapter discusses the case of KPN. What the exact problems are they are facing and what objectives need to be reached to solve those problems. The necessary case data is explained, as well as where it originates from. This provides the answer to sub question two.

3.1 KPN case

In order to extend on RBM literature in the telecommunication sector, research has to be done on implementing RBM methodology for a telecommunication provider. One way to do this is by doing a case study at a provider. KPN is currently struggling with the maintenance planning of their network. The problem is best summarised by the problem statement KPN has put out themselves:

"We are increasingly moving towards a 24x7 economy. This increases the need to always be able to use our services. KPN therefore wants advice on how we can use our maintenance Windows even better and thus serve our customers better. The desired result is that this does not limit our migration pace, but can even be accelerated in collaboration with our customers. Also consider the impact on customers, processes, resources, technology and organisation."

There are many ways to approach this problem. Process optimisation, client side research and risk based planning are a couple of examples. To decide if RBM methodology might be effective, the problems KPN are facing need to be clearly defined. The next step is to define objectives that will help solve the problems defined in the first step.

3.1.1 Problems

The problem statement created by KPN was the starting point for this research. In order to determine how many different parts the problem exists of, internal talks were held within different departments. More than 30 people spreading over five departments have been talked to and have given their view on the problem. The conclusion of these talks is that there are many aspects to the problem. Which means many different possible solutions. The main aspects are client management (corporate and consumers), contract management and process optimisation. Determining which aspect to focus on was the following step.

Based on the researchers education and experience, the impact and the time frame of the research and the department issuing this research, the scope was determined on process optimisation. As the background of the researcher is not legal nor business and the time frame for the research is limited, client and contract management are left out of this research. The department who issued the problem statement, MDD (Migration, Decommissioning and Disassembly), are a department who manage and perform the changes. Therefore they have a larger interest in the process, as they make use of it. Finally, there is much room for improvement with potential high impact on the objectives in the current processes. The final step was to determine what processes would most interesting to optimise. In consultation with the department in charge of the change processes (the service quality centre), the decision was made to focus on change classification based on risks.

In the problem statement set out by KPN, the main problem KPN is facing is how to use their maintenance windows more efficiently, in order to better serve their clients, while improving or at least not impacting their maintenance pace. This problem exists of three important parts.

The first part is making better use of their maintenance windows. Comparing the amount of time available in the maintenance windows and the work that needs to be performed now and in the future shows that maintenance windows run the risk of becoming bottlenecks for achieving certain goals. These goals are phasing out old equipment and networks. An example of this is that KPN is aiming to have all their client migrated from the outdated copper network to newer networks and stop providing ISDN by 2021 (KPN, 2017). But as maintenance windows are limited and the time in a maintenance window is limited as well, achieving this will become more and more difficult. Making better use of maintenance windows in this context can mean two things. Either creating more room in the maintenance windows, or using the time that is available more efficiently.

The second part is to better serve their clients. This reflects on two things. Clients need to be able to use the service they buy from the provider 24/7. But the providers also want to improve their network to be able to provide more stable and faster service to their clients. These are difficult goals to combine, as performing maintenance to improve the network impacts client service provision. This makes it difficult to perform a lot of maintenance work outside certain hours.

As comes forward quite clearly in the first two parts, the last part of the problem is not limiting the migration pace, even rather increasing the pace if possible. In the current situation, these three aspects clash, creating the problem KPN is facing.

3.1.2 Objectives

Now that the problems KPN is facing have been defined, objectives can be determined. Looking at the three parts of their problem, each objective can be focused on one of the problems.

1. **KPN needs to increase the percentages of FTR performed changes.**

   This means that the methodology used to solve these problems needs to be able to improve performance of maintenance activities. The focus for this objectives is to improve on how the current changes are being performed and analysed. Instead of taking a macro look, a micro approach will create insight in what needs to be improved in order to increase the success rate.

2. **KPN needs to minimise the risk of impact on the clients.**

   Improving the use of maintenance windows is important, but this cannot come at the cost of the clients. This means that down time experienced by the clients need to be minimised or prevented, risks of impact or larger impact than anticipated are prevented and that the clients receive the best possible service.

3. **KPN needs to increase the maintenance pace.**

   This means finding a way to increase the amount of work being done outside of maintenance windows. Working during the day means that changes can be done more often, for a longer time and are cheaper to do. It also creates more room during maintenance windows for work that is to risk full to do it any other time.

Having objectives helps define what the artifact will need to achieve. This makes it possible to select a method for creating the artifact. Increasing the amount of maintenance activities and improving the effectiveness of current activities while decreasing the risks of impact on clients points to risk management methodologies (as discussed in section 2.1). Therefore this case lends itself adequately to research if RBM methodology is an effective method for increasing efficiency while decreasing risks. Using risk assessment will lend the insight necessary to increase FTR percentages. The results can then be used to provide an overview of the different risks and impacts. Comparing these results with current classifying methods can help increase the maintenance pace by changing the classification of changes.

3.1.3 Artefact objectives

Having determined what KPN's objectives are, provides the necessary information to determine what the artefacts objectives need to be. The risk model that will be created will need to achieve two things.

1. **Increase the success rate of changes by providing insight into threats and consequences**

   By collecting, structuring and visualising information about the threats and consequences, project managers gain understanding of what problems they need to focus on. With that knowledge, project managers can better react to threats.

2. **Provide numerical substantiation for discussion**

   Using the collected data to calculate probabilities of impact happening, can be used to devise risk ratings. These can then be used to compare different change types to decide how riskful the change types are and in what way they are riskful.

Providing insight can be used to increase the success rate of performed changes at KPN. Whereas calculating probabilities, impact and risk ratings can help to minimise client impact while increasing the maintenance pace of KPN. Creating an artefact that can reach these objectives would be helpful to reach the goals set by KPN. But without tailoring the artefact objectives to KPN, both objectives can be valuable for any telecommunication provider. Having a more detailed insight into risks and calculating risks are essential for RBM in any sector. Therefore it has value for RBM methodology application in the telecommunication sector and helps in solving the problem of organising change planning in the telecommunication sector efficiently.

3.2 Case data

A bow tie diagram is only as good as the data that is used to make it. Therefore it is important to use the right data. For a good bow tie diagram, detailed information is necessary. This means that an organisation needs to document information on a very low scale level. Making a bow tie diagram for the whole change process would not be useful, if even possible. That is why in the demarcation process of this research, the choice was made to look at specific migration changes. The difficulty of this, is that KPN as an organisation currently makes their risk assessments on a higher scale level. As a result, detailed information is hard to come by. Most project managers in charge of their migration process might be able to make estimations, but many don't document the necessary information for making a bow tie. This obstacle has played a big role in deciding what changes to model. For each of the parts of a bow tie diagram an explanation is given how the information was obtained.

3.2.1 KPN network

The KPN network has five layers, as can be seen in Figure 3.1. The lowest layer is called the access layer and consists of 1G DSLAMs, mobile sites and CPEs.

- **DSLAM:** stands for Digital Subscriber Line Access Multiplexer. It is a network device. Which can connect numerous customer digital subscriber line (DSL) interfaces to a high-speed digital communications channel. This is done by using multiplexing techniques. A DSLAM acts like a network switch and enables telecommunication providers to offer clients the fastest phone line technology with the fastest backbone network technology.

- **CPE:** stands for Customer-premises equipment. It is a terminal and all of its equipment can be found on a subscriber's land. The terminal is connected to the provider's telecommunications circuit. CPE refer to devices such as routers, network switches and internet access gateways that enable users to access their providers communication services.

- **Mobile sites:** Locations where antennae and electronic communications equipment are placed to crate a cell in a cellular network.

It is in the access layer that all customers are connected to the KPN network. These devices are located in street cabinets and connect around 150 to 300 clients to the network. CPE connect big corporate clients to the network. The street cabinets and CPEs are in turn connected to central offices. These are in the Metro-Acess/Metro Bridge layer. Depending on the amount of connection aggregated at at central office, a central office is directly connected through to the Metro-Core or connected to another central office. When a central office is connected directly to the Metro-Core, it is referred to as the Metro-Access layer, else it is called the Metro-Bridge layer. The Metro-Core layer is another aggregation step to bring connections together. There are about 180 Metro-Core locations and about 1500 Metro-Bridge locations (1100 Metro-Access and 400 Metro-Bridge locations).

The Back-Bone layer is slowly being faced out as the ETN network is being replaced by the FCN network. In Figure 3.1, the new and old architectures are both shown. On the right is the old architecture, where the Metro-Core locations are set up in a ring, each time aggregating the connections. This has as a result that for reaching the ETN-Core, more capacity is needed. With the new architecture, a one to one connection between Metro-Core locations and the Peta-Core are created. Decreasing the amount of capacity needed to transport the amount of connections. The Peta-Core is located in the ZARA layer, which is the top layer of the network. It stand for the Zwolle, Amsterdam, Rotterdam and Arnhem. These are the locations where the main servers of KPN are located and all services provided by KPN are distributed around the Netherlands. Below The top four layers is the OTP network which stand for "Optical transportation network". This network is used for fast and reliable connections over long distances. The different networks like ETN, FCN and PETA regulate the data transported over OTP. A good comparison to help understand how the network is comparing it to a highway. The OPT is the highway, the logistical network. Where ETN, FCN and PETA can be compared to the traffic controllers.

Knowing the basics of how the network of KPN works helps to understand the scaling each layer brings. This is important as each layer represents an increase in the amount of clients impacted by maintenance work. It also provides some visualisation of where the migrations discussed in this research take place and their potential impact.

3.2.2 Scope

In order to make a logical demarcation of what changes to look at during this research, three factors were looked at. The first factor is the department this research is being done for. Migration, Decommissioning and Disassembly (MDD) is in charge of managing different types of change activities. Migrating DSLAMs is one of their main activities. As discussed in chapter 3.2.1, these are mostly located in the access layer. But there are also types of DSLAMs located in the Metro-Core and ZARA layer. Therefore it was decided to demarcate the scope to these type of migrations. The second factor that was taken in account was the availability of information. The information needed for the risk model is not readily available for many changes. The reason for this is that KPN, in their current system, does not use micro information to classify their changes. If a change or maintenance activity causes any form of disturbance in service delivery, it is never classified as a standard change. Therefore project managers are not instructed to collect micro information. Luckily, it is available for the type of DSLAM migration MDD is responsible for. The last factor was the representativity value of the research. Creating a risk model for a type of change that is not representative for the changes done by KPN would not be of scientific value. Because these migrations take place in different layers (see section 3.2.3) and they are the third most performed migrations, there is no doubt that the results will be representative. Appendix E shows the distribution of change types at KPN.

Another choice that was made in regards to the scope of this research, was to look at TI (technische infrastructure) and not IT. At KPN, TI is defined as fixed hardware. This means that the changes this research is looking at, have to do with hardware changes. Where mechanics have to travel to the location of the hardware to be able to perform their work.

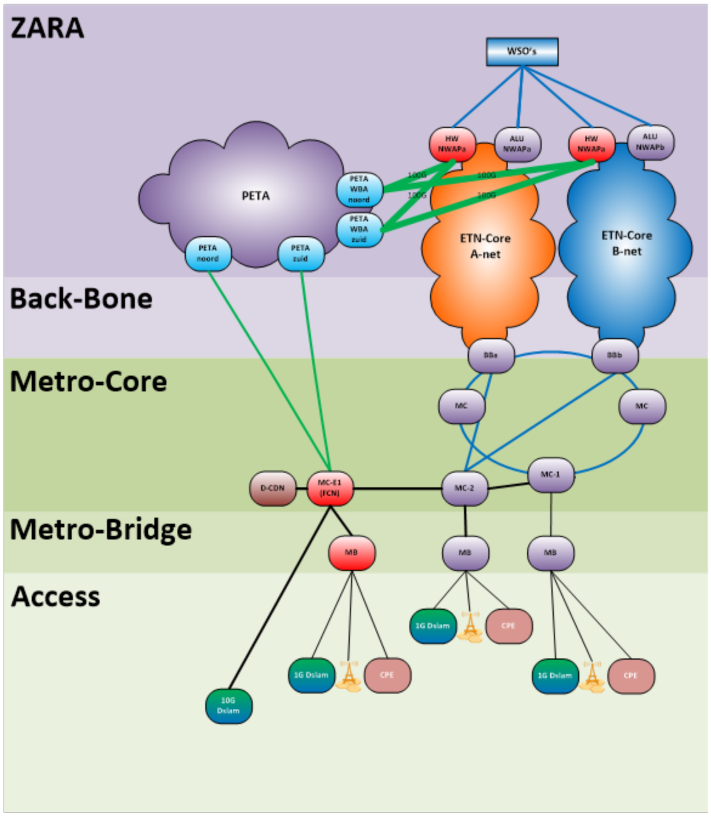


Figure 3.1: KPN network

When talking about IT at KPN, it means it is software related. The work is often done from distance, sometimes even outsourced to foreign countries. Technicians don't hinder each other and it the work they do is rarely the reason maintenance windows are becoming more and more packed. The MDD department also focuses on TI changes, making the demarcation a logical choice.

3.2.3 Hazards and top events

Selecting the hazard in this case is the same as selecting what migrations are going to be modelled. Much of the reasoning for the choices can be found in section 3.2.2. Figure 3.1 in section 3.2.1 can be used to understand where in the network these changes are performed. To summarise, based on the demarcation the selected changes are related to the department of KPN that requested this research, the availability of information on a certain level of detail and the representativity of the research. These criteria led to the following migration changes:

1. **1-10G migrations:** The main reason these migrations happen is because of capacity management. The DSLAMs located in the access layer, metro-bridge layer and the metro-core layer need to be upgraded from 1G to 10G. This is because clients that have fiber to the home need more capacity. The switches located in the DSLAMs are 'upgraded' to have 10G gates and during the migration client are taken from 1G gates and plugged into 10G gates.

2. **1 G migrations:** These migrations are comparable to 1-10G migration as they happen

on the same locations and DSLAMs. The difference is that the reason behind the migrations is life cycle management. Clients are migrated from old switches to new switches. The older models have a higher risk of malfunctioning and repairing them can be difficult because some of them are from old suppliers. Therefore it is better to change them to new hardware.

3. **NT migrations:** NANT cards are located in DSLAMs and depending on the type of card regulate the amount of uplinks. A DSLAM can be upgraded from two 1G uplinks to four 1G uplinks. This is done to increase capacity. This happens when a NANT A card is replaced by a NANT D card. When a DLSAM gets upgraded to have 10G gates, the NANT card also needs to be replaced with a NANT E card. Therefore the main idea to do this is capacity management. It also helps making the network more redundant. When for example two of the four uplinks fail, the traffic can be rerouted over the remaining two links.

4. **WAP migrations:** NWAPs are located in the ZARA layer. They connect the wholesale parties to the Peta core of KPN. This is done for life cycle management. Wholesale clients are disconnected from old hardware and connected to new hardware.

Each of these migration changes are a hazard because it is work that needs to be done on a daily basis, but can inflict damage if they go wrong. They all share the same top event, the event that leads to loss of control, which is when the migration is not performed FTR.

3.2.4 Threats

For each of these migration changes, threats leading to the change being performed nFTR (not First Time Right) need to be identified. This information is an example of detailed data that is not standerdly recorded for every type of change that is done. Project managers might have an idea, but no detailed records. In this case, since 2018, an engineer/project manager at KPN has recorded everything that led to these changes being performed nFTR. Barry Klasens was partly in charge of organising the changes used as examples in this research. He recorded the reasons that led to nFTR performed changes and organised them in to categories. This not only gives an overview of all the threats, but also a frequency of each threat for the four migrations change types. Listed below are all the possible threats with a short explanation of what they entail.

1. **Cabling:** Any kind of problem with the cabling. This can be because of bringing the wrong cabling, not having it in stock or having applied the cables in the right way.

2. **BOP:** BOP is the name of a piece of software that is needed during the migration. When it malfunctions it can disrupt the migration.

3. **DSLAM isolated:** Because of the migration, some DSLAM lose connection and can't function anymore. This means that a rollback is necessary.

4. **Material:** When the the wrong material has been brought to the job or the right material is not available due to supplier problems.

5. **Gates:** The gates are occupied, hindering the migration.

6. **Pre-check:** A problem has occurred during the pre-check or no pre-check has been done. This means that the migration has to be rescheduled.

7. **Switch:** The switch is the hardware were all the cables are plugged in. It needs to be activated before the cables are plugged in. When this has not happened yet but the switches get plugged, it is not able to create an uplink.

8. **System:** The systems needed to migrate are not accessible/reachable.

9. **Migration running late:** Because of minor problems during the process, the migration takes longer and not everything can be done before the end of the window.

10. **Fiber:** Either the fiber is defect or there is another issue with the fiber.

11. **Agama:** Software used during migration. Sometimes no session can be held.

12. **DHCP:** Dynamic Host Configuration Protocol needs connection to the server to function. Sometimes a connection with the server cannot be made. A mistake can also be made during the DHCP request process in preparation of the change.

13. **Post-check:** During the post-check a problem is discovered and the change has to be rolled back.

14. **Flashcard:** The flashcard that needs to be installed does not have the correct software on it. The results is a mechanic that came to the job site for no reason, as the flashcard needs to be updated.

15. **Mechanic:** There are a lot of different reasons why mechanics can cause a nFTR. Everything that has to do with mechanics being late, starting late and planning problems involving mechanics are put together in this threat. The reason for this is because these threats never lead to big problems and are often unique or rare (car problems due to running over a deer for example).

16. **Cancelled:** The change is cancelled because of a variety of reasons. (e.g. Freeze)

17. **Engineering:** This is the term used for a part of the preparation. When it is not done properly, the mechanic arrives and cannot perform his job.

18. **Script error:** During the migration a script is used which can generate errors for different reasons. Can be related to other systems, but also an error related specifically to the current change.

19. **Bop Down:** This code is used when BOP is completely down. It does not generate errors, but cannot be used.

20. **No Permission:** Permission for the change is not given. This can be because of misinformation, wrong input or a change in situation.

21. **Incorrectly scheduled:** Mistakes made during the scheduling of the change leading to the change being rescheduled.

22. **SFP:** Small form-factor pluggable transceiver is not in stock.

23. **BOP CA:** This error code happens during preparation. CA stands for 'create alternative end points' and means the migration needs to be rescheduled. This happens before a mechanic is sent out.

24. **BOP SWAP:** When BOP gives an error because of the change. This has nothing to do with BOP self, but when there is a problem during the change itself BOP gives an error. This means a roll back is necessary.

25. **Unknown:** The reason for the change being performed nFTR is not know or has not been properly recorded.

These are all the threats that have led to nFTR performance for the four hazards that are being modelled. In Appendix B a table is shown in which can be read the percentage of times a threat has led to a nFTR performance for each type of migration. The percentage represents the share of each threat to the total failed migrations.

3.2.5 Consequences

To define all the possible consequence of a nFTR performance, two important sources of information are looked at. Most importantly are the performance reports. Of which the critical report is called the 'Change triggered be alert' report. As discussed in section 1.3.3, this report shows what changes have led to a Be Alert situation. Appendix A shows what the possible Be-Alert situations are. The second source is what the project manager has defined as a consequence. That has led to the following list of consequences.

1. Reschedule: When a change has not been performed FTR, but there is no impact on service delivery to the clients because of, for example, a rollback being performed on time, the change will be rescheduled. This can impact costs when a mechanic has been sent out. It always impacts time lost, as the window is used to no effect and a new window will be necessary to finish the change.

2. Be Alert Green

3. Be Alert Blue

4. Be Alert Yellow

5. Be Alert Orange

6. Be Alert Red

The Be Alert classification is explained in Appendix A. In any case, there will be an impact on service delivery. Depending on the severity of the Be Alert, damage will be done to different critical aspects of KPN. The same document used to tally the percentages of threats has been used to calculate how often a specific threat has led to one of the consequences. The vast majority has led to a reschedule, only on two occasions has a change of these types led to a Be Alert in 2018.

3.2.6 Damage categories

If after a top event a consequence occurs, some kind of damage will be done. It is for these damages that risk matrices are made. As rescheduling does not impact clients, the damages are internal. Often unnecessary cost are made for mechanics that are not used properly, but the main damage is the loss of a maintenance window. Especially because you do not only lose the current window, but need to plan a new window to finish the change. In the case of Be-Alerts the damages are external as internal. Based on the Be Alert matrix defined by KPN in Appendix A, eight categories have been defined. Some have been grouped together, as the requirements for each step of severity is equal.

1. **IT applications en mobiele services:** When we are talking about IT applications, we are talking about all the applications that are used to service the client or the client can use. Examples are billing, delivery and service applications. But also stores, mechanics and user applications. The damage in measured by the amount of clients impacted, the severity of impact on the applications, the amount of mechanics not able to work and the amount of stores that are not accessible.

2. **Services: telefonie,internet, iTV, Digitenne, Wholesale transport & access services:** These are all the main services KPN delivers to its clients. As soon as one or more of these services are not being delivered, damage for the clients aswell as damage for KPN is a fact. It is measured by the amount of impacted client.

3. **Services secundair:** These are less important services, like being to pause live tv or ordering movies through KPN. This is also measured by impacted clients, but the threshold value is much higher compared to the threshold value of primary services.

4. **Reputation:** All of these damages have an impact on reputation. Depending on how many clients are impacted or how important the client/service is, the worse the damage on the reputation. An example that happened not long ago, KPNs firewall disrupted the connection to 112. Police was therefore not reachable. This has a major impact on reputation.

5. **Cost:** Comparable to reputation, every Be Alert has a cost associated to it. Depending on what has been impacted and how long, certain fines can be given to KPN.

6. **Security:** Telecommunication providers are interesting targets for hackers. They can either disrupt the lives of many people or companies by taking out services, or they can try and steal data.

7. **Business impact:** When critical services are disrupted, this has a major impact. The example of the police is related to business impact. Other critical services are described in the 'Business Critical list'(BCL).

8. **Services, telefonie en internet grootzakelijk:** This is basically the same as primary services, but for big corporate clients. As they are more important and have stricter SLAs and contract, the threshold value is lower than for other clients.

3.2.7 Barriers

The value of adding barriers in a bow-tie diagram is to show what measures have been taken to counter certain threats and mitigate certain consequences. As looking at changes at a micro level is not common at KPN, specific barriers have not been recorded. There might be some barriers put in place, but that kind of data is not available. Standard preventive measures, such as basic training for mechanics, are in place. But these do not add value to the diagram like, for example, specialised training for a recurring problem. Therefore no barriers have been added in the models. One of the added values of creating these bow-tie diagrams, is that by creating the models, project managers create insight into what barriers might be useful in order to improve on nFTR percentages. Examples of this will be given in Chapter 4, where the created models are discussed.

Chapter 4

Demonstration

This chapter contains the Bow-tie models of the selected changes, the risk matrices and an explanation of how to use the results to compare the risks and impacts of changes. The four Bow tie models are explained. This will be related to the first objective. Then, the risk matrices are explained. These are the same for all the changes and are essential for comparing the changes. This will be related to objective two. This provides the answer the sub question three. For both the bow tie models and the risk matrices some limitations are explained in the fist section.

4.1 Limitations

To understand the level of detail of the models and the numbers being used to calculate the risk ratings, some explanation has to be given about their nature. The following two sub sections explain what the limitations are for the models and the used data during this research. The limitations are not part of the method and are only relevant to this particular case.

4.1.1 Bow tie details

Bow tie diagrams can be made with different levels of details. In that regard, the Bow tie models in this research are limited in their details. There are no barriers, no combinations of threats that lead to a consequence or influence each other, no escalation factors and limited details about the context. No management systems or responsible persons are detailed for example. There are several reasons for that. The first and foremost reason is the limited recording of information. Finding the the data used to create these diagrams and calculate the risk ratings was already complicated. As it is not the standard way of operating at KPN to do this, the way it was recorded was simple. Every time a change of one of these types was performed, it was recorded in an Excel sheet. If it went wrong, one reason was put down as the cause and every month the results were tallied. These results were then combined and categories of threats were created. It is those threat categories that are used in this research. Also, in the discussions about these records, no mention was made of two or more threats leading to a failed migration. Without speculating, it is not possible to extend on the diagram in this way.

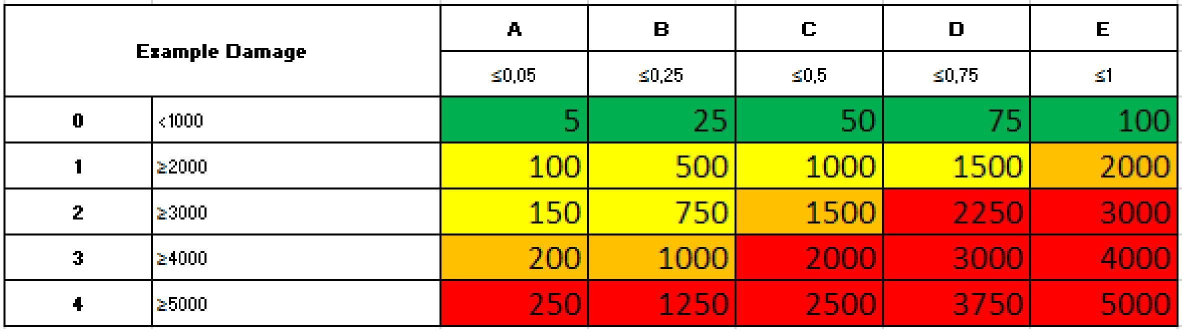
The same reason can be used for the lack of barriers. As the recorded data was limited, different people in the organisation were talked to, to try and increase the knowledge about this system. The only form of barrier that could be discovered was the possibility of a rollback. The possibility of performing a rollback in case something does not work as intended, is used in the current method to determine risk classification. When a rollback is performed, the final status of the change is always a reschedule. This means that it does not prevent a consequence of happening. At best it prevents a Be-Alert by redirecting the consequence. This is difficult to show in a bow tie and more importantly, it does not add to this research. This is because a rollback does not influence probabilities, because its effect are already incorporated in the recorded results. It would only be useful if everything was recorded in more detail, because then it could be used to influence the calculation and decision making.

In short, to be able to make more detailed bow tie diagrams, more information needs to be recorded at a micro level. The limited diagrams created in this model already proof the worth of doing this. If this way of working is implemented for the whole organisations, more detailed diagrams can be made, which in turn can provide more insight in how to increase performance.

4.1.2 Sensitive data

In order to make risk matrices, impact and probability information is necessary. By multiplying the impact with the probability of the impact happening, results are calculated which can then be used to rank the risks relative to each other. A complication for this research is that the necessary data needed for these risk matrices, is sensitive data from KPN. Probabilities of damage occurring and on what scale that damage is measured internally at KPN, is not supposed to be public knowledge. Therefore the results of these calculations need to be anonymised. Table 4.1 shows an example of a risk matrix. This fictive example will be used to explain how a risk matrix is made, aswell as to show how the data is anonymised.

Table 4.1: Example of a risk matrix



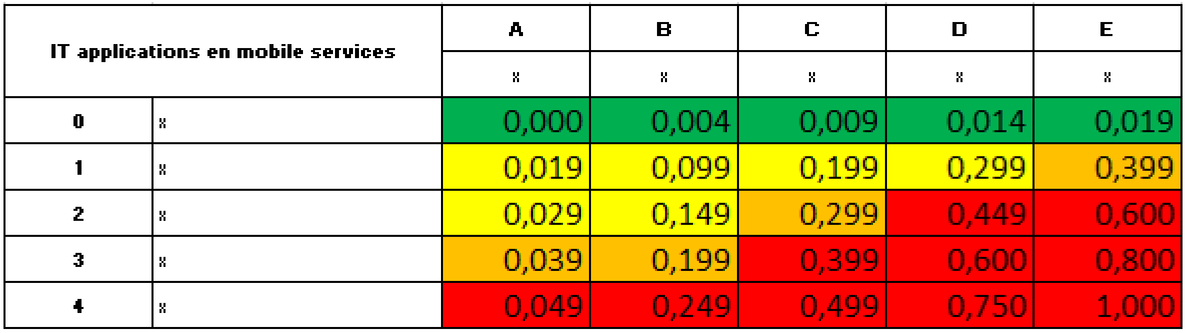
Example Damage		A	B	C	D	E
		≤0,05	≤0,25	≤0,5	≤0,75	≤1
0	<1000	5	25	50	75	100
1	≥2000	100	500	1000	1500	2000
2	≥3000	150	750	1500	2250	3000
3	≥4000	200	1000	2000	3000	4000
4	≥5000	250	1250	2500	3750	5000

Rows zero to four represent the impact and columns A to E represent the probabilities. By multiplying them with each other, the rest of the table is filled. The next step is to anonyimse the data. One effective way to do this is to scale the results between zero and one, also called normalisation. The method used to do this is called min-max feature scaling, which can be seen in equation 4.1. To calculate the normalised value (x') of an original value (x), subtract the minimal value of the results from the original value and divide that by the difference between the maximum value and the minimum value of the results.

$$x' = \frac{x - min(x)}{max(x) - min(x)} \tag{4.1}$$

The results of using this method can be seen in Table 4.2. The lowest value in the top left corner (A0) is equal to zero and the highest value in the bottom right corner(E4) is equal to one. Anonymising the results this way, gives the options to hide the the sensitive data, while still working with relevant results.

Table 4.2: Example of a risk matrix scaled between [0,1]



IT applications en mobile services		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,004	0,009	0,014	0,019
1	x	0,019	0,099	0,199	0,299	0,399
2	x	0,029	0,149	0,299	0,449	0,600
3	x	0,039	0,199	0,399	0,600	0,800
4	x	0,049	0,249	0,499	0,750	1,000

4.2 Bow-tie models

In the following section, each subsection will discuss one of the four models. Thereby showing how the first goal, providing insight in how to improve current change activity, of the risk model is reached.

4.2.1 1-10G model

In 2018, fourteen different threats have been identified for the 1-10G migration, which can be seen in Figure 4.1. The main four threats are 'Cabling' (19%), 'BOP' (20%), 'Fibers' (11%) and 'BOP CA'(18%). These threats are responsible for 68% of the nFTR performed 1-10G migrations. The first objective is to decrease the nFTR percentage. To achieve this, barriers can be implemented as discussed in 3.2.7. In this case, barriers such as better inventory planning could have an impact on decreasing the nFTR percentage. A more detailed view is given in Appendix C.1.

4.2.2 1G model

For the 1G migrations in 2018, sixteen threats have been identified. The two main threats are 'Mechanics' (14%) and 'Bop CA' (27%). Combined they are responsible for 41% of the nFTR performed migrations. The second group of threats that is responsible for 16% exists out of 'Cabling' (8%) and 'Fiber' (8%). This can be seen in Figure 4.2. Creating barriers focused on these threats will be the first step in decreasing the nFTR percentage. Appendix C.2 contains more charts for a total overview.

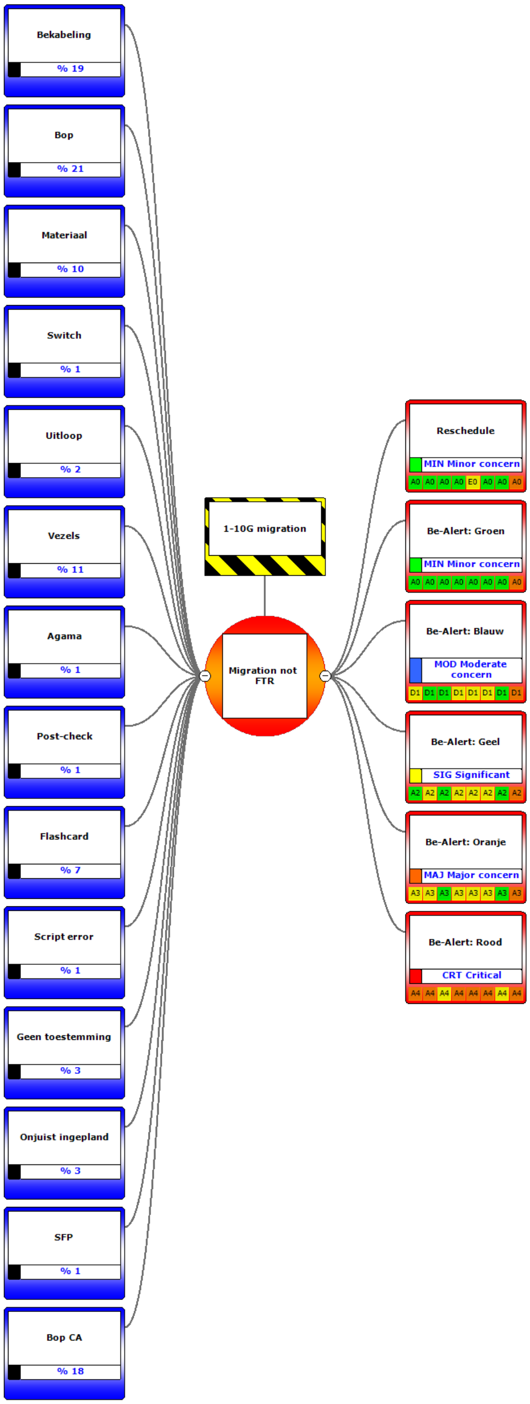


Figure 4.1: 1-10G bow tie model

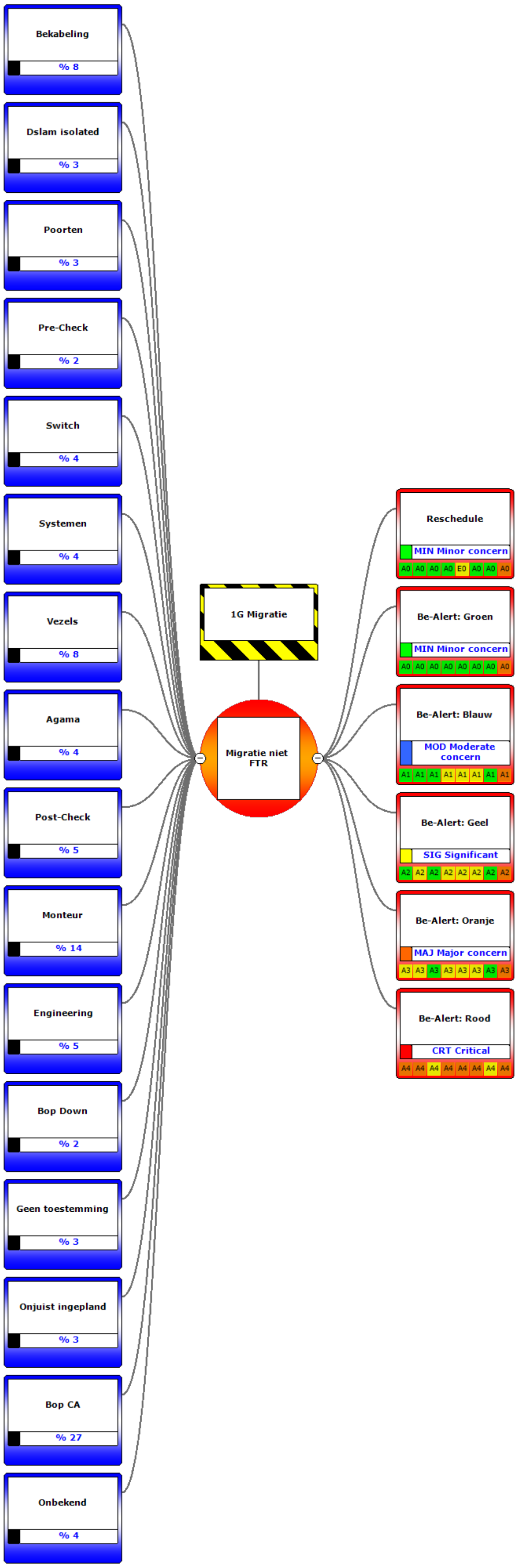


Figure 4.2: 1G bow tie model

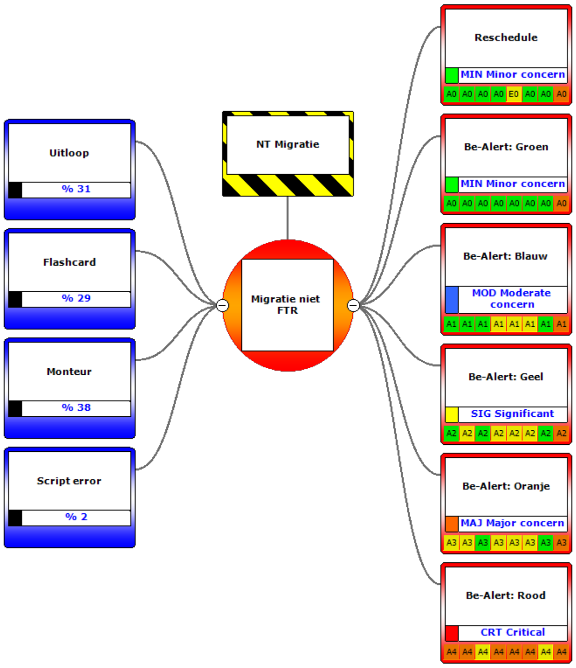


Figure 4.3: NT migration bow tie model

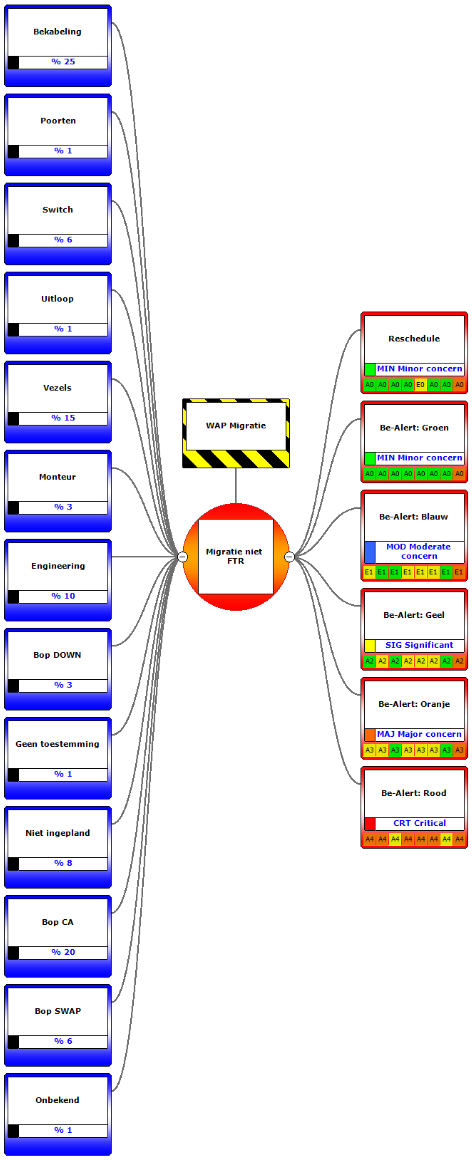


Figure 4.4: WAP bow tie model

4.2.3 NT model

The NT migration Bow-tie model is different to the others, as only four threats have been identified for 2018. The large majority (98%) of the nFTR percentage is caused by three of the four threats, these are 'Migrations running late' (31%), 'Flashcard' (29%) and 'Mechanics' (38%). The last 2% is caused by 'Script error', which is not a recurring problem for this migration. Improving on any of these three threats in the form of barriers will have a major influence. The Bow-tie model can be seen in Figure 4.3 and a more detailed overview can be found in Appendix C.3.

4.2.4 WAP model

As can be seen in Figure 4.4, thirteen threats were identified in 2018. The main four threats are 'Cabling' (25%), 'Fibers' (15%), 'Engineering' (10%) and 'Bop CA' (20%), totalling to 70% of nFTR percentage. Creating barriers for these threats can potentially improve the nFTR percentage. The other 30% are caused by occasional problems and mistakes, which are difficult to solve with barriers. For a better overview, see Appendix C.4.

4.3 Risk matrices

Risk matrices are part of a risk assessment, as explained in section 2.3.2. This section will explain the eight matrices that were made for the eight types of damage that were identified in section 3.2.6. The method used to calculate and compare these results will first be explained.

4.3.1 The Z-score

Having anonymised the results , the next step is to make sure the results can be compared. Every damage category has its own severity scale. This means that the results need to be standardised in order to be able to compare them. There are different methods to standardise values in order to compare them. The two most common methods are the Z-score and min-max feature scaling, of which one has already been used to anonymise the results. The Z-score is a measure of how many standard deviations below or above the population (of results) mean a "raw" score is. The main difference between the two methods is that the min-max feature scaling guarantees all features will have the exact same scale, but does not handle outliers well. While the Z-score is better in handling outliers, but does not provide normalised data with the exact same scale.

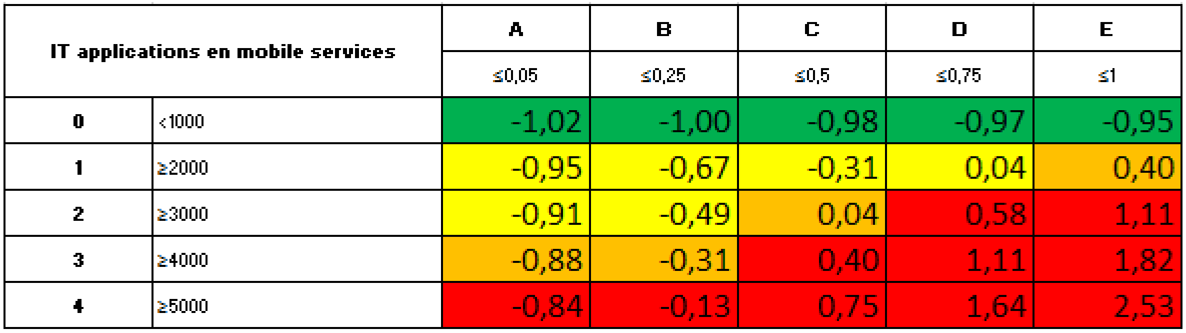
The method that has been selected to standardise these results is the Z-score. The reason for this is that the results contain some outliers that have an influence on the results. This makes the Z-score a more reliable method to standardise these results. Therefore the results will first be normalised with the min-max feature scaling method and then standardised by calculating the Z-scores. The Z-score is calculated by taking the mean of the population of the raw score and dividing it by the standard deviation of the population, which can be seen in equation 4.2.

$$z = \frac{x - \mu}{\sigma} \tag{4.2}$$

The z-score results, which can be seen in Table 4.3, represent the distance between the original value ('raw score') and the population mean, measured in standard deviation. Z-scores provide a way to compare the results to a normal population. It can be used to determine where the results of the risk rating is compared to the average results mean risk rating (Abdi, 2007). A negative score represents that the original value is equal to z times the standard deviation lower than the mean. In this case, scoring lower than the mean, means that the risk rating is safer. A positive score represents a higher value than the mean and thus a more dangerous risk rating.

There are some potential problems caused by using z-scores. Using z-scores can influence the meaningfulness of the original 'raw' scores. The original results often easier to interpret, whereas z-scores don't speak to the imagination. Another potential problem is that z-scores

Table 4.3: Example of a standardised risk matrix



IT applications en mobile services		A	B	C	D	E
		≤0,05	≤0,25	≤0,5	≤0,75	≤1
0	<1000	-1,02	-1,00	-0,98	-0,97	-0,95
1	≥2000	-0,95	-0,67	-0,31	0,04	0,40
2	≥3000	-0,91	-0,49	0,04	0,58	1,11
3	≥4000	-0,88	-0,31	0,40	1,11	1,82
4	≥5000	-0,84	-0,13	0,75	1,64	2,53

can magnify small differences between the raw scores. Thereby creating unintended weights for certain results. In this case, the results have been anonymised, which has already taken away any meaningfulness of the raw scores. In the case of magnifying small differences, the ranges of the different damage categories are comparable. Because the ranges don't differ to much, this does not cause a problem. Only when comparing the damage categories measured in euros to damage categories measured in clients impacted, does it have a minor influence. When the z-scores of these damage categories have been compared only with damage categories measured in the same units, the results were altered slightly. The difference in results was minimal and did not have any influence in the end result. Therefore the usages of the z-score method was deemed applicable for this research.

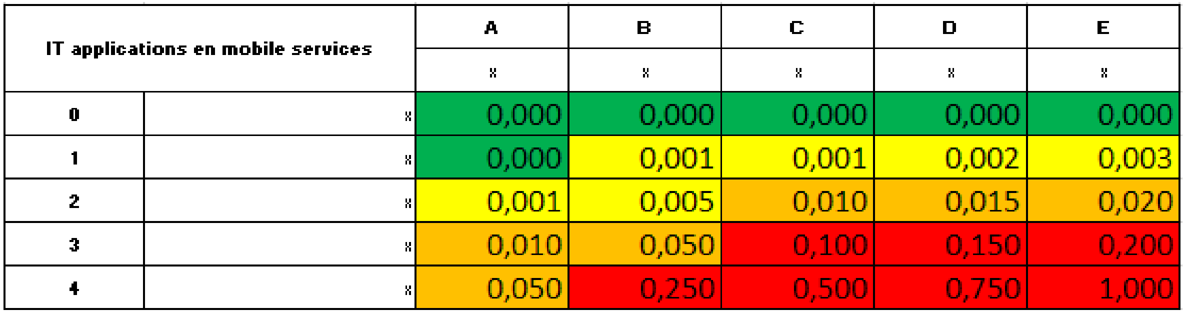
4.3.2 Colouring scheme

Risk matrices make use of colours in order to convey if results are acceptable or not. The risk matrices used in this research make use of four colours, green, yellow, orange and red. Green is used for results that are considered acceptable risk for performing the migration outside of maintenance windows. Yellow results can be discussed. This means that depending on how much influence changing the classification has on improving maintenance windows efficiency, one could decide to accept the somewhat higher risks. Orange results are too risky and impactfull, but could be improved by taking measures. If these measures (implementing barriers for example) prove to be effective for a certain period of time, changing the classification could be a viable decision in the future. Red results imply high risks and high impact. This means that if a change scores in the red area, it is deemed to riskful to change its classification. One change type will score differently on these eight categories of damage. This should be taken in account when comparing the final results. It could be that the results for cost end up being red, but that the criteria of cost is less important than for example the risk of services failing. Therefore the results and their colour should not be taken as a final result. Different aspects need to be taken into consideration in order to determine the possibility of changing the classification of a change request. Appendix D explains this in more detail.

4.3.3 IT applications and mobile services risk matrix

Table 4.4 shows the normalised results for the IT applications and mobile services. The impact severity is measured in clients impacted. The mean and standard deviation are given in order to calculate the Z-score. As explained in Equation 4.2, the mean and standard deviation of the population, in this case the results, are used to calculate the Z-score. As can be seen in the table, the results are fairly close to each other up till row three. The differences between the results become larger from then on, showing that the highest few results can be considered outliers. This justifies the decision to standardise the results through calculating the Z-score, to be able to better compare results.

Table 4.4: IT applications and mobile services risk matrix

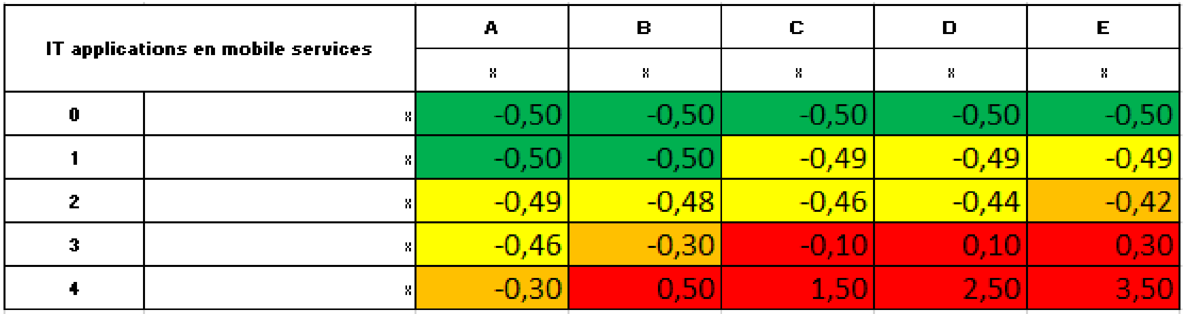


IT applications en mobile services		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,000	0,000	0,000	0,000
1	x	0,000	0,001	0,001	0,002	0,003
2	x	0,001	0,005	0,010	0,015	0,020
3	x	0,010	0,050	0,100	0,150	0,200
4	x	0,050	0,250	0,500	0,750	1,000

Mean: 0,125
Stand deviation: 0,250

The second table, Table 4.5, shows the standardised score calculated by using the Z-score method. Based on those results and the comparison made between all categories, the colouring scheme has been adjusted, as explained in Appendix D. The initial colouring represents a standard colouring scheme. The colouring used in Table 4.5 is the results of comparing the results of the eight categories of damages. The best way to interpret these results is as follows. If a change type scores in a green area for a category of damage, it means that the risks and impacts are acceptable for the change to become a standard change. When the results are yellow, it means that risks and impact are slightly higher than what would normally be accepted, but depending on the impact of changing the classification might be worth taking the risk. Orange results mean that the risks are too high and might be improved in the future, but are not ready yet for changing the classification. Red scores are not likely to change to anything acceptable now or in the future and could therefore better be done during maintenance windows.

Table 4.5: IT applications and mobile services risk matrix Z-score

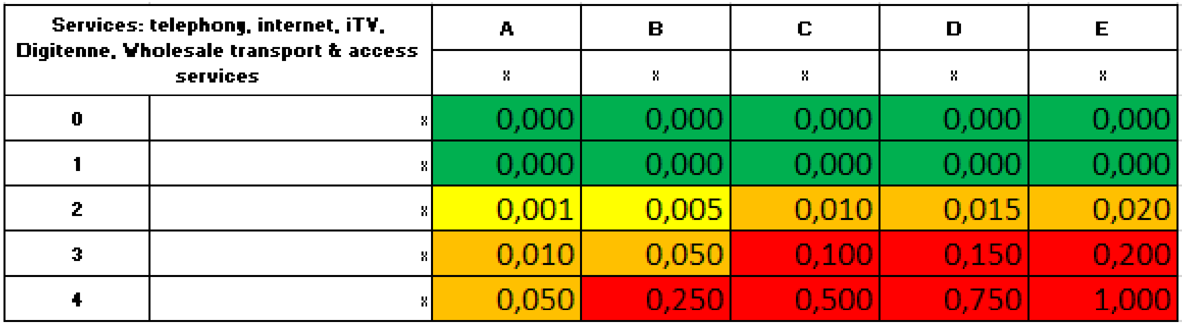


IT applications en mobile services		A	B	C	D	E
		x	x	x	x	x
0	x	-0,50	-0,50	-0,50	-0,50	-0,50
1	x	-0,50	-0,50	-0,49	-0,49	-0,49
2	x	-0,49	-0,48	-0,46	-0,44	-0,42
3	x	-0,46	-0,30	-0,10	0,10	0,30
4	x	-0,30	0,50	1,50	2,50	3,50

4.3.4 Services: telefonie,internet, iTV, Digitenne, Wholesale transport & access services

The results for the next damage category can be seen in Table 4.6. They are very similar to the results for IT applications and mobile services, but has more green rated ratings in the first two rows. It is also measured in clients impacted. While this could be used to argue that the impact or the chance of impact is smaller than for IT applications and mobile services, one should always keep in mind that you are comparing two different damage categories. It is very much possible that IT applications and mobile services is viewed as a less important damage category in general. As the results match a lot with the first damage category, the same conclusion can be made about the outlying values.

Table 4.6: Services: telefonie,internet, iTV, Digitenne, Wholesale transport & access services risk matrix

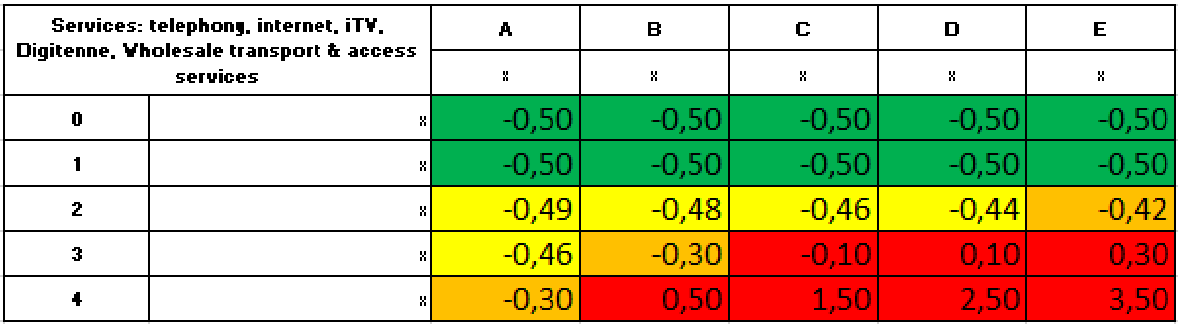


Services: telephony, internet, iTV, Digitenne, Wholesale transport & access services		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,000	0,000	0,000	0,000
1	x	0,000	0,000	0,000	0,000	0,000
2	x	0,001	0,005	0,010	0,015	0,020
3	x	0,010	0,050	0,100	0,150	0,200
4	x	0,050	0,250	0,500	0,750	1,000

Mean: 0,124
Stand deviation: 0,250

Using the mean and standard deviation of these results shown in Table 4.6, the Z-score is calculated. The results and the new colouring can be seen in Table 4.7. The Z-score results are comparable, just like the normalised results.

Table 4.7: Services: telefonie,internet, iTV, Digitenne, Wholesale transport & access services risk matrix Z-score

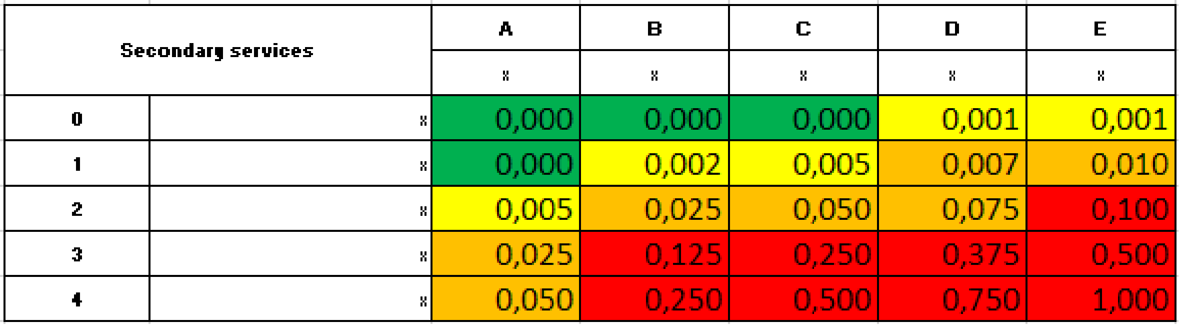


Services: telephony, internet, iTV, Digitenne, Wholesale transport & access services		A	B	C	D	E
		x	x	x	x	x
0	x	-0,50	-0,50	-0,50	-0,50	-0,50
1	x	-0,50	-0,50	-0,50	-0,50	-0,50
2	x	-0,49	-0,48	-0,46	-0,44	-0,42
3	x	-0,46	-0,30	-0,10	0,10	0,30
4	x	-0,30	0,50	1,50	2,50	3,50

4.3.5 Services secundair

The failing of the secondary services that KPN provides, like pay per view and pausing live television, is also measured in amount of clients impacted. When looking at the results in Table 4.8 and the mean of the population, one can see that the risk ratings are higher compared to the other two damage categories.

Table 4.8: Services secundair risk matrix

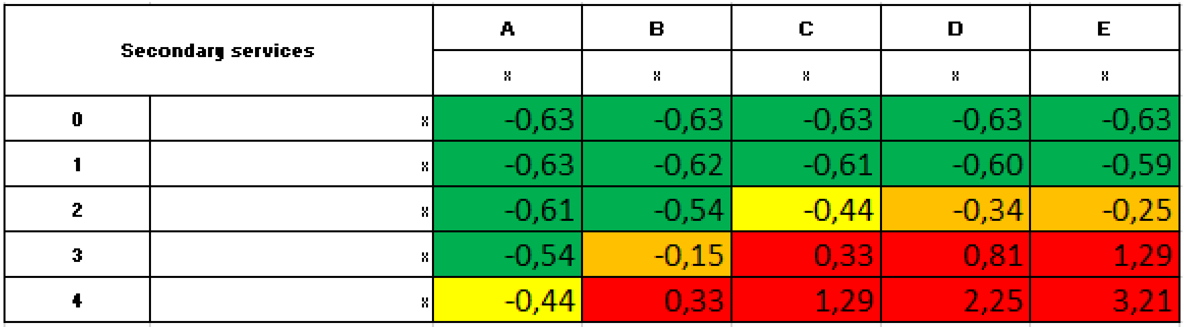


Secondary services		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,000	0,000	0,001	0,001
1	x	0,000	0,002	0,005	0,007	0,010
2	x	0,005	0,025	0,050	0,075	0,100
3	x	0,025	0,125	0,250	0,375	0,500
4	x	0,050	0,250	0,500	0,750	1,000

Mean: 0,164
Stand deviation: 0,260

The Z-score has been calculated using the mean and standard deviation, the results can be seen in Table 4.9. There is a small difference in results between this damage category and the first two. This is because both the mean and standard deviation are larger. Creating results that are mainly green or red, or in other words, creating bigger variances between results.

Table 4.9: Services secundair risk matrix Z-score

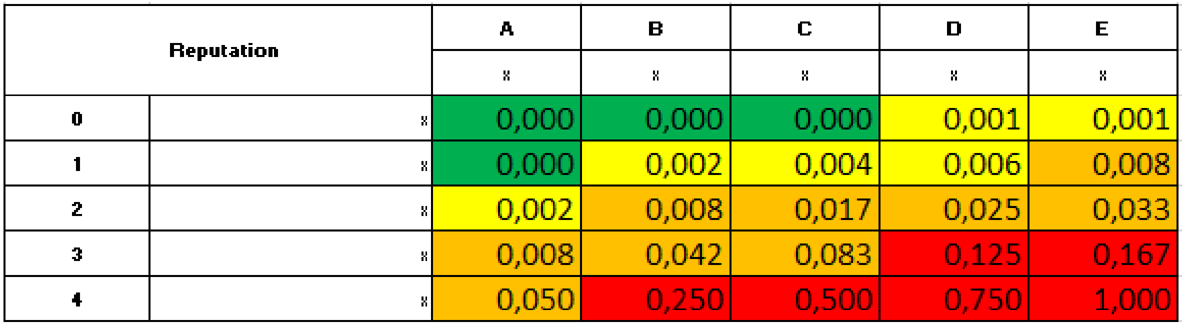


Secondary services		A	B	C	D	E
		x	x	x	x	x
0	x	-0,63	-0,63	-0,63	-0,63	-0,63
1	x	-0,63	-0,62	-0,61	-0,60	-0,59
2	x	-0,61	-0,54	-0,44	-0,34	-0,25
3	x	-0,54	-0,15	0,33	0,81	1,29
4	x	-0,44	0,33	1,29	2,25	3,21

4.3.6 Reputation

The choice was made to measure reputation damage in €. The way it is defined in the Be Alert classification matrix is by the size of the region (local, regional and national) or by the amount of clients. It falls under the category of KPN external damage, which also contains a scale measured in €. Using the scale in € to define the impact for the different Be-alerts gives workable numbers to do calculations with and effectively portrays the impact of reputational damage as stated in the Be-Alert classification matrix.

Table 4.10: Reputation risk matrix

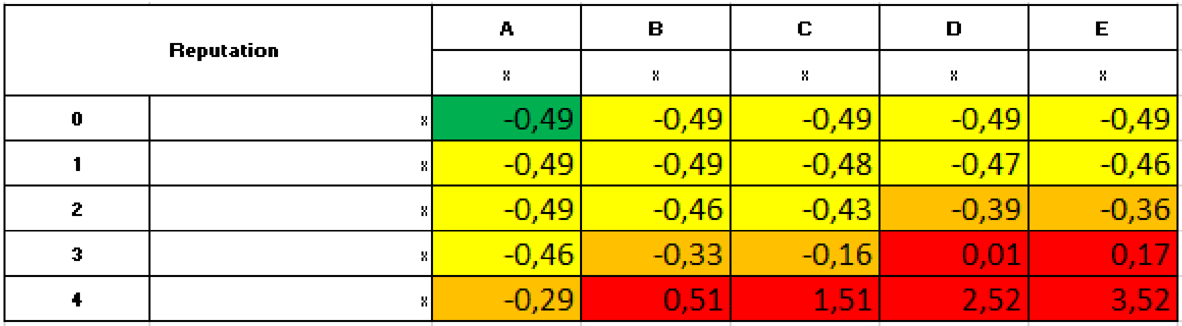


Reputation		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	0,000	0,000	0,000	0,001	0,001
1	¤	0,000	0,002	0,004	0,006	0,008
2	¤	0,002	0,008	0,017	0,025	0,033
3	¤	0,008	0,042	0,083	0,125	0,167
4	¤	0,050	0,250	0,500	0,750	1,000

Mean: 0,123
Stand deviation: 0,249

Surprising enough, Table 4.11 shows that the Z-score results are more riskful on average. While the variances between results are not that big, except for the highest results, the risk ratings are higher to begin with, resulting in more yellow and orange results.

Table 4.11: Reputation risk matrix Z-score

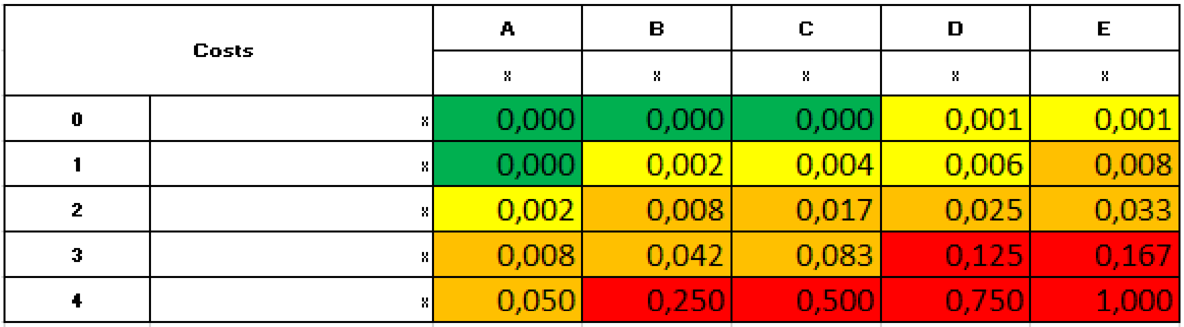


Reputation		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	-0,49	-0,49	-0,49	-0,49	-0,49
1	¤	-0,49	-0,49	-0,48	-0,47	-0,46
2	¤	-0,49	-0,46	-0,43	-0,39	-0,36
3	¤	-0,46	-0,33	-0,16	0,01	0,17
4	¤	-0,29	0,51	1,51	2,52	3,52

4.3.7 Cost

The cost damage category is exactly the same as the reputation damage category, as the Be Alert classification matrix also measures it in € and in the same amounts. This means that Tables 4.12 and 4.13 are copies of the Tables that represent the reputation category.

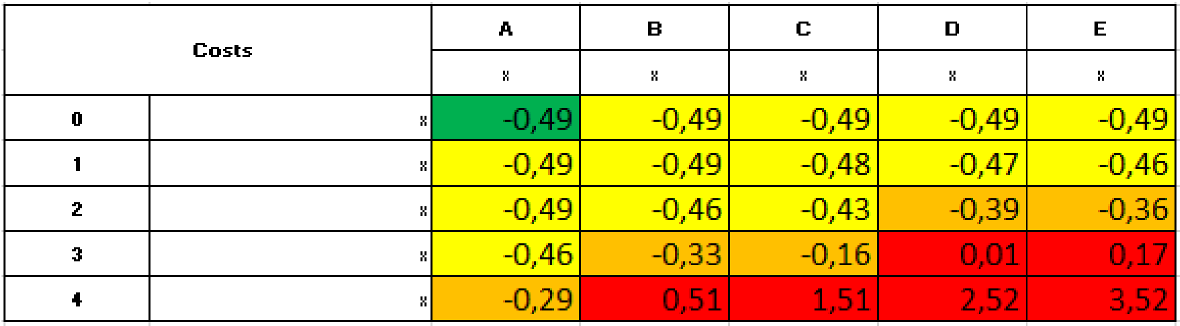
Table 4.12: Cost risk matrix



Costs		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,000	0,000	0,001	0,001
1	x	0,000	0,002	0,004	0,006	0,008
2	x	0,002	0,008	0,017	0,025	0,033
3	x	0,008	0,042	0,083	0,125	0,167
4	x	0,050	0,250	0,500	0,750	1,000

Mean: 0,123
Stand deviation: 0,249

Table 4.13: Cost risk matrix Z-score

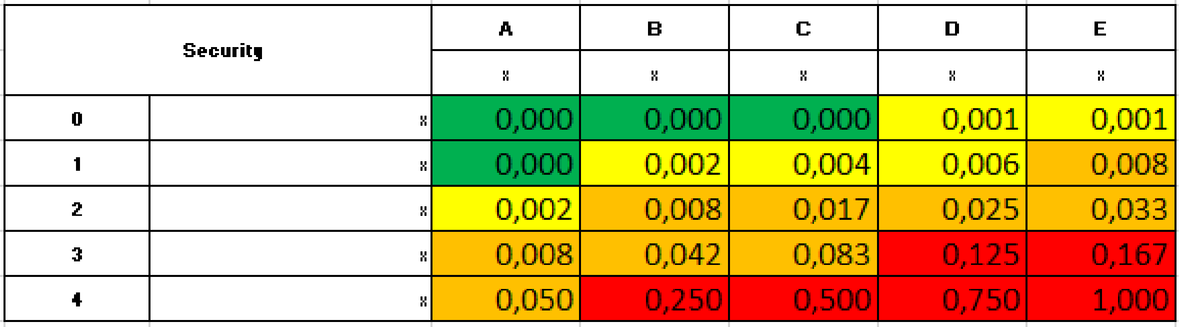


Costs		A	B	C	D	E
		x	x	x	x	x
0	x	-0,49	-0,49	-0,49	-0,49	-0,49
1	x	-0,49	-0,49	-0,48	-0,47	-0,46
2	x	-0,49	-0,46	-0,43	-0,39	-0,36
3	x	-0,46	-0,33	-0,16	0,01	0,17
4	x	-0,29	0,51	1,51	2,52	3,52

4.3.8 Security

Just like the reputation and cost category, security is measured in € and in the same amounts. Resulting in the same risk matrix for original values and Z-scores.

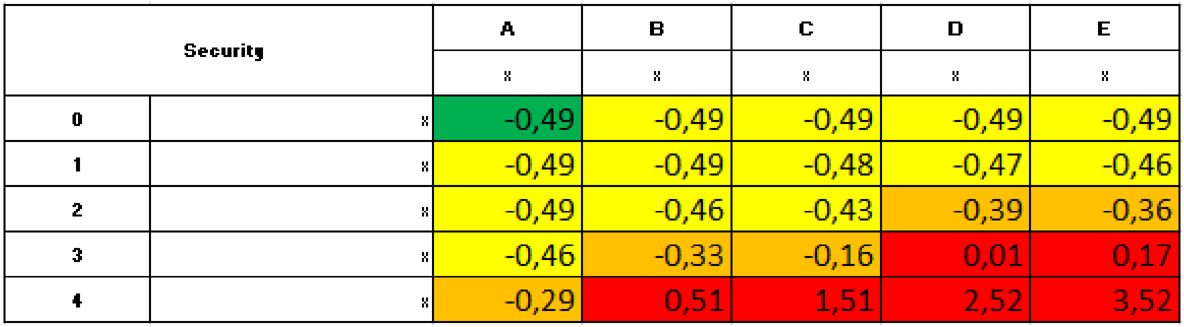
Table 4.14: Security risk matrix



Security		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	0,000	0,000	0,000	0,001	0,001
1	¤	0,000	0,002	0,004	0,006	0,008
2	¤	0,002	0,008	0,017	0,025	0,033
3	¤	0,008	0,042	0,083	0,125	0,167
4	¤	0,050	0,250	0,500	0,750	1,000

Mean: 0,123
Stand deviation: 0,249

Table 4.15: Security risk matrix Z-score

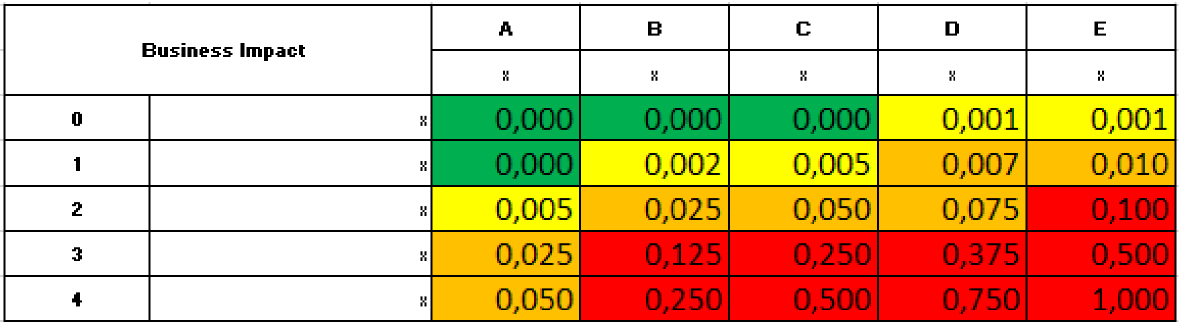


Security		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	-0,49	-0,49	-0,49	-0,49	-0,49
1	¤	-0,49	-0,49	-0,48	-0,47	-0,46
2	¤	-0,49	-0,46	-0,43	-0,39	-0,36
3	¤	-0,46	-0,33	-0,16	0,01	0,17
4	¤	-0,29	0,51	1,51	2,52	3,52

4.3.9 Business impact

Defining the severity scale for business impact through the Be Alert classification is complicated. This damage category is focused on critical services. These have been defined internally. These can be disrupted for either large corporate clients or normal consumers. In the case of a large corporate, one client being impacted is already severe enough to count as a Be Alert. But for normal consumers a lot more need to be impacted for it to count as a Be-alert. Calculating with corporate clients results in illogical results, because the numbers can't represent the importance of the client. Therefore the decision was taken to use the same severity scale as in section 4.3.4. The importance of KPNs core business and the importance of services that have been defined as critical, are comparable and the last three steps in the severity scale are already matching.

Table 4.16: Business impact risk matrix

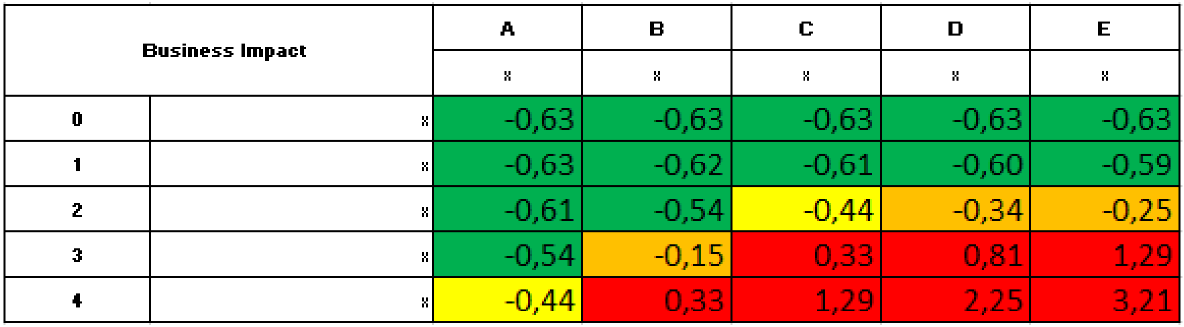


Business Impact		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	0,000	0,000	0,000	0,001	0,001
1	¤	0,000	0,002	0,005	0,007	0,010
2	¤	0,005	0,025	0,050	0,075	0,100
3	¤	0,025	0,125	0,250	0,375	0,500
4	¤	0,050	0,250	0,500	0,750	1,000

Mean: 0,164
Stand deviation: 0,260

This results in the same Z-score matrix as for services. For both these damage categories it is important to notice that while the risk ratings are relatively lower and therefore rated less riskful, the importance of the damage categories is not represented in the rating. The impact for these damage categories is measured earlier, or in other words, less clients need to be impacted for it to count as a Be-Alert. This results in relatively lower scores. The focus in these risk matrices is on amount of impact, not on the importance of impact.

Table 4.17: Business impact risk matrix Z-score

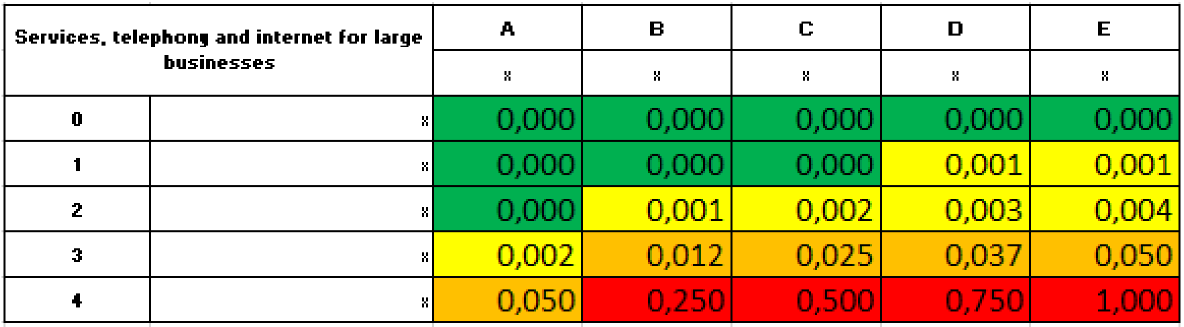


Business Impact		A	B	C	D	E
		¤	¤	¤	¤	¤
0	¤	-0,63	-0,63	-0,63	-0,63	-0,63
1	¤	-0,63	-0,62	-0,61	-0,60	-0,59
2	¤	-0,61	-0,54	-0,44	-0,34	-0,25
3	¤	-0,54	-0,15	0,33	0,81	1,29
4	¤	-0,44	0,33	1,29	2,25	3,21

4.3.10 Services, telephony and internet for large businesses

Corporate clients not receiving core services is measured in the amount of corporate clients impacted. As these are considered more important than consumers, the severity scale starts lower and ends lower compared to the other damage categories. Therefore the initial normalised results score less riskful than other damage categories. This can be seen in Table 4.18 and in the lower mean of the results.

Table 4.18: Services, telefonie en internet grootzakelijk risk matrix

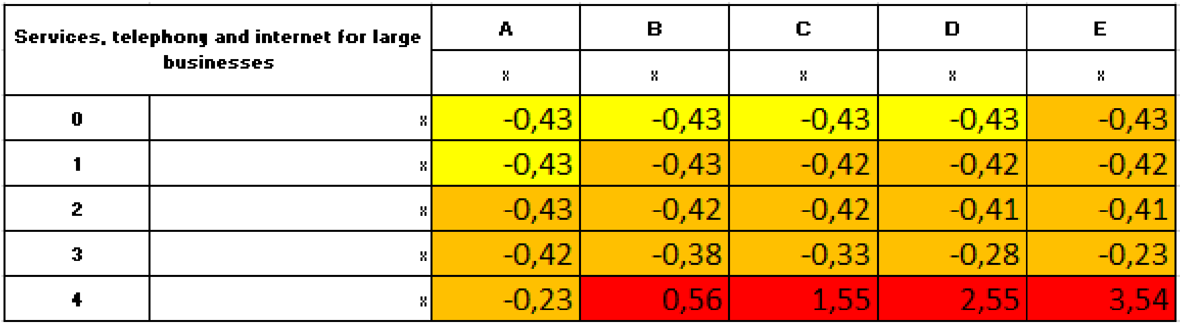


Services, telephony and internet for large businesses		A	B	C	D	E
		x	x	x	x	x
0	x	0,000	0,000	0,000	0,000	0,000
1	x	0,000	0,000	0,000	0,001	0,001
2	x	0,000	0,001	0,002	0,003	0,004
3	x	0,002	0,012	0,025	0,037	0,050
4	x	0,050	0,250	0,500	0,750	1,000

Mean: 0,108
Stand deviation: 0,252

Because the mean of the results is lower compared to the rest, but the standard deviation is comparable, this results in higher Z-scores on average. This can be seen in Table 4.19. In other words, changes that have any chance of impacting core services to corporate clients will have a difficult time having their classification changed.

Table 4.19: Services, telefonie en internet grootzakelijk risk matrix Z-score



Services, telephony and internet for large businesses		A	B	C	D	E
		x	x	x	x	x
0	x	-0,43	-0,43	-0,43	-0,43	-0,43
1	x	-0,43	-0,43	-0,42	-0,42	-0,42
2	x	-0,43	-0,42	-0,42	-0,41	-0,41
3	x	-0,42	-0,38	-0,33	-0,28	-0,23
4	x	-0,23	0,56	1,55	2,55	3,54

4.4 Risk rating

Using the probabilities and the risk matrices, a rating can be given to each damage category for each consequence. These can be seen in the Figures 4.1, 4.2, 4.3 and 4.4. The eight squares under each consequence represent the eight damage categories discussed in the section above. Based on how a consequence scores in the z-score matrices above, the eight squares are given a colour and a rating. For example, if a consequence scores A1 for Reputation , this is equal to a risk score of -0.49. This is based on the historic data of 2018. For each of these migrations, the reschedule consequence has a very low chance of impacting any of the damage categories and if it would impact them, the impact would be minimal. Therefore it scores A0 (low chance of happening, low impact) in each of the risk matrices. Only for the damage category 'Costs' does it score differently. Rescheduling incurs costs, but the costs are not very high. And because most of the time a migration is performed nFTR it ends up being rescheduled, it scores E0 (high chance of happening, low impact). This can be done for each of the migration types and each of the damage categories based on the historic data of 2018. By adding the results of each category to each other and dividing it by eight (the amount of categories), a risk rating per consequence is calculated. This can be seen in Table 4.20.

To help understand the process and calculations better, a detailed example of the consequence 'Be-Alert Blue' for 1-10G migrations is given in the following paragraph. For each damage category the z-scores have been calculated in section 4.3. Starting with the first damage category 'IT applications and mobile services'. In 2018, the level of impact and probability of this happening was so that the z-score needed to calculate the risk rating can be found in the matrix at D1. This is equal to -0.49. For the following seven damage categories, the same logic is applied and the following Z-scores can be found to calculate the risk rating: -0.50, -0.60, -0.47, -0.47, -0.47, -0.60 and -0.42. Adding these together gives the total score of -4,03. Dividing it by 8, the amount of damage categories, provides us with the risk rating for a 'Blue Be-Alert' during 1-10G migrations, -0.50. This number can be measured on the same colouring scheme the z-scores are measured on. Doing this for the four change types gives a large part of Table 4.20.

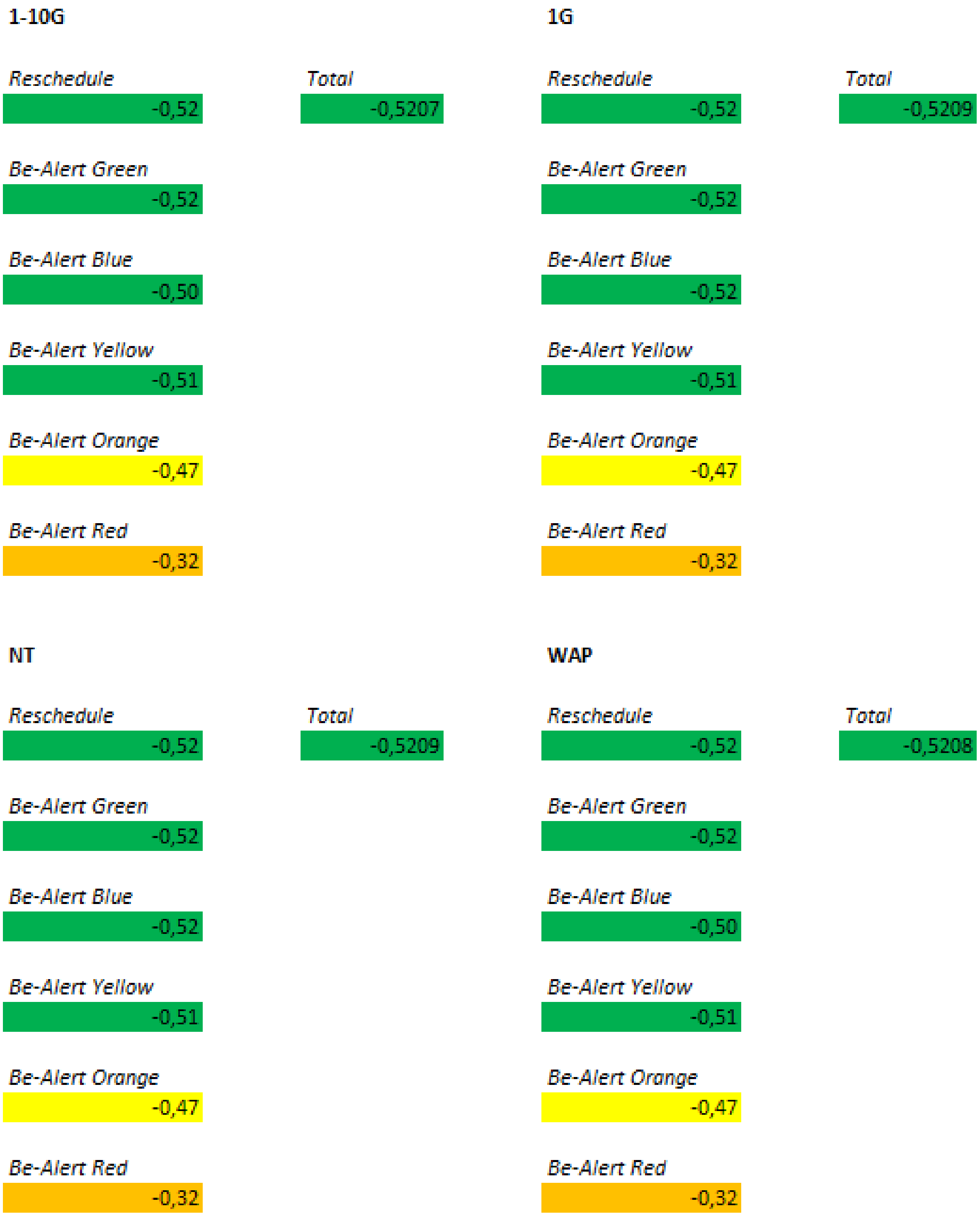
The following step is to calculate the final risk rating. The easiest way of calculating this would be to add the rating of each consequence to each other and divide by six (the amount of consequences). But this gives the Be-Alert Yellow, Be-Alert Orange and Be-Alert red a major influence in the total risk rating, while these have never been caused by these change types. It is also not very likely that they will be caused by these change types. A solution for this is to look at how often the consequences have been caused and use that to decide how heavy the ratings for each consequences "weigh". In the case of 1G and NT migrations, for the whole of 2018, nFTR have only led to reschedules. Therefore the total risk rating equals 100% * the risk rating for a reschedule. For 1-10G and WAP migrations, 99.7% and 99.5% of the nFTR performed migrations respectively, have led to reschedules. The other 0.3% and 0.5% have led to a Be-Alert Blue. This means that to calculate the total risk rating of 1-10G migrations, 99.7% * risk rating of a reschedule, will need to be added to 0.3% * the risk rating of a Be-Alert Blue. For WAP migrations that would mean 99.5% * the risk rating of a reschedule added to 0.5% * the risk rating of a Be-Alert Blue. For the 1-10G migration, the formula to calculate the total risk rating looks like equation 4.3.

$$(-0.52 * 0.997) + (-0.50 * 0.003) \tag{4.3}$$

The overall results of both these calculation for all four change types can be seen in Table 4.20. Based on these scores, change types can be compared as well as ranked in order of most to least riskful. Depending on what needs to be decided, these scores can be used to create more insight into the risks and impacts of different changes. Making decision making in maintenance of telecommunication networks more based on probabilistic calculations instead of one time occurrences.

Each of these change types score the same kind of risk rating, no to low risk (green). There are two differences that can be seen, which are the risk ratings for the blue Be-Alert of the 1-10G migrations and WAP migrations. That is because these two migrations have had a blue Be-Alert in 2018, therefore increasing the probabilities of that happening compared to the other two migrations. These scores can be used to compare the risks of different migrations. This can be done by their overall rating, but also by their rating for the different consequences or even damages. Another interesting results is that for all the migrations, the risk ratings are very alike. The main reason for this is that the these four types of changes fall under the same domain. Therefore their impact is the same on the damage categories, as they enable the delivery of the sames services. This would not be the case if they would be compared to other types of changes. Another reason for the fact that the results only differ very little, is that these changes are rather successful. Be-Alerts Blue and even Be-Alerts Yellow are not very rare, these happen regularly at KPN. But for these changes, only two Be-Alerts in more than a years time have been recorded, which has a big influence on the final risk rating.

Table 4.20: Risk ratings



	1-10G	1G	NT	WAP
Reschedule	🟩 -0,52	🟩 -0,52	🟩 -0,52	🟩 -0,52
Be-Alert Green	🟩 -0,52	🟩 -0,52	🟩 -0,52	🟩 -0,52
Be-Alert Blue	🟩 -0,50	🟩 -0,52	🟩 -0,52	🟩 -0,50
Be-Alert Yellow	🟩 -0,51	🟩 -0,51	🟩 -0,51	🟩 -0,51
Be-Alert Orange	🟨 -0,47	🟨 -0,47	🟨 -0,47	🟨 -0,47
Be-Alert Red	🟧 -0,32	🟧 -0,32	🟧 -0,32	🟧 -0,32
Total	🟩 -0,5207	🟩 -0,5209	🟩 -0,5209	🟩 -0,5208

4.5 Demonstration conclusion

This chapter demonstrates what can be done by modelling risks on a micro level. Creating the Bow-tie models provides necessary insight in order to improve on the success rate of changes. Whereas adding probability and impact severity can serve to compare different changes numerically. Comparing changes based on these results can be very useful in order to define classifications, but needs to be done carefully. For each company, type of change, category of damage and way of calculating different opinions and preferences can have an influence on how the results are interpreted. It therefore functions better as a tool to substantiate discussion, instead of giving clear cut answers. For these four migration changes it has become clear that if a change in classification can increase the productivity meaningfully, the risks are manageable. In the case that the maintenance windows are not too full and it might be useful to only perform one or two changes during the day instead of during maintenance windows, a comparison can be made. In this case the best advise would be to change the classification of the changes in the following order: NT migrations and 1G migrations first, followed by 1-10G migration and then WAP migrations.

Chapter 5

Evaluation

In the previous chapter the risk model and its results have been demonstrated. The following chapter will evaluate these results by comparing them to the current way of working. The first objective of the risk model is to increase the success rate by providing insight into what threats and consequences have a large share in the failures. To evaluate this, a comparison will be made for the four changes treated in this research, between results in 2018 and 2019. The second objective of the risk model is to provide numerical substantiation for discussions about change classification. This will be evaluated by comparing the current ratings of the changes to the results of the new risk model. The last part of this chapter will be to evaluate if the objectives for KPN can be reached by implementing this risk model. By doing this, sub question four is answered.

5.1 Objective 1 of the risk model: Providing insight

The general idea of working with bow tie models at KPN is to work with a micro approach, instead of with the current macro approach. The information needed to create these bow tie models however, is not yet standardly recorded at KPN because of the macro approach. Therefore is is difficult to find changes for which this data is readily available. In 2018 Barry Klasens, a project manager at KPN started collecting detailed records in order to analyse how his changes were performed. Every two weeks he would use the data he collected to discuss what could be improved with all the involved parties. He did this all through 2018 and continued this practice during 2019. The way of collecting this information was basic. Each time a change was performed nFTR, he asked the people involved to record the reason for the failed change. After a while he organised the different reasons into categories. It is this data that has been used in the models for the four example change types. Using the bow tie model, this data was structured and connected to the consequences. This was possible by using the reports used by KPN to monitor the amount of change related Be-Alerts. Having this data for 2018 and in part for 2019, provides the necessary data and frame of reference to evaluate the results of using a micro approach. Using the bow tie models helps users structure the data they collect and connect the different threats with consequences. But the insight created by collecting this data without putting it in a bow tie model, is enough to be able to evaluate if collecting this micro data is effective.

It was difficult finding this detailed information, as no other project manager collects this information. It was after contacting many different people that Barry Klasens was suggested, as he might have the necessary data. Getting access to his data was not easy. Apparently other colleagues had had a similar interest in his data and he did not feel at ease sharing the details of the projects he was working on. The suggestion he would be criticised or judged based on his collected data was created by his attitude. After some mediation, Barry agreed to share his Excel records and explain his process. While explaining his process, he also discussed how collecting this data helped him give insight on what to focus on to solve the main issues he was facing during changes.

In Appendix B the success rates, the failure rates and the share of each threat to the failed change activities in 2018 and 2019 are detailed. These tables can be used to compare the results of 2018 and 2019, to determine if the insight created by recording this data in 2018, have impacted the results in 2019 positively.

The first comparison to be made is between the total results for each change type in 2018 and 2019. Table B.2 in Appendix section B.1 shows the results for 2018 and will be compared to Table B.4 in Appendix section B.2, which shows the results for 2019. As can be seen, the success rates in 2018 for 1-10G, 1G, NT and WAP migrations were 63%, 85%, 87% and 62% respectively. For 2019, the success rates are 74%, 87%, 89%, 59% respectively. This means that in 2019, an increase in success rate of 11% for 1-10G migrations has been achieved, an increase in success rate of 2% for 1G migrations has been achieved, an increase in success rate of 2% for NT migrations has been achieved and a decrease in success rate of 3% for WAP migrations has been achieved in comparison to 2018. This adds up to an overal increase of success rates of 12% in 2019 for these changes.

The second comparison, which is more interesting for this research, will be made between the threat percentages that account for how many times a threat has led to a failed migration. Table B.1 in Appendix section B.1, shows for each threat how often it has lead to a failed migration in 2018 for each change type. Table B.3 in Appendix section B.2, shows the same for 2019.

5.1.1 1-10G migration comparison

Looking at 1-10G migrations in 2018, one can see that the threats that have led to failed migrations most often are 'Cabling', 'BOP', 'Fiber' and 'BOP CA'. When this is compared to the results of 2019, the percentage for 'Cabling' has been decreased by 17.7%, from 19.3% to 1.6%. The 'BOP' threat has been neutralised for all four changes, having been decreased by 21.1%. 'Fiber' has increased 7.6%, from 11.4% to 19%. The last threat, 'BOP CA', has decreased by 6.8%, from 17.9% to 11.1%. This is in line with what the project manager for these migrations has stated. Based on the data from 2018, the decision was made to focus on 'Cabling', while the 'BOP' threat was also being an important threat to other change types. Therefore solutions to the 'BOP' threat were already been looked at. Which has been proofed effective based on the results in 2019.

5.1.2 1G migration comparison

The two main threats for 1G migrations in 2018 are 'Mechanic' and 'BOP CA'. Comparing the results between 2018 and 2019, one can see that the 'Mechanic' threat has been decreased by

14.3% to 0% and the ’BOP CA’ threat has been decreased by 26.3% to 0.6%. It is important to note that the results from 2019 are not complete, which has led to the ’Unknown’ threat to be the most important threat in 2019. This might in a later stage be divided into other threat categories, influencing the results being presented at this date.

5.1.3 NT migration comparison

In 2018, the three main threats for NT migrations were ’The migration running late’, ’Flashcard’ and ’Mechanic’. These have been decreased in 2019 by 5.6%, 10.7% and 23.2% respectively. Some new threats play a role in 2019, impacting the total results, but having the insight what threats played an important role in 2018 clearly had a positive impact.

5.1.4 WAP migration comparison

For WAP migrations in 2018, the main threats were ’Cabeling’, ’Fiber’, ’Engineering’ and ’BOP CA’. These threats have been decreased by 25.1% to 0%, 14.5% to 0%, 0.1% to 10% and 13.4% to 6.7% respectively. Other threats, of which one is related to ’BOP’, have risen quite strongly.

5.1.5 Conclusion - Objective 1

What can be concluded from the comparison between the results in 2018 and 2019, is that for almost every threat that has been identified as important to the change activities in 2018, improvements have been made in 2019. Even though other threats have surfaced in 2019, sometimes even neutralising the positive increase of the success rates, the insight created by working on a micro scale has had a positive influence on increasing the success rates of these changes. Which has been confirmed in the first comparison in this section. For most of these improvements, Barry Klasens (the project manager) has confirmed that recording reasons for changes to fail (threats) has played a role in achieving better results. Therefore, it can be said that the risk model does achieve its first objective of creating insight in order to improve the success rate of change activities.

As Barry is the only project manager at KPN of who is known that he records micro details about his changes, such as threats, there is no other source which can confirm the effectiveness of recording micro data. But based on his data, recording and acting on micro data helps improve FTR percentages. Recording micro data for all the changes performed by KPN and structuring it in bow tie models could therefore help increase the average FTR percentage for KPN.

5.2 Objective 2 of the risk model: Numerical substantiation

A complete evaluation for this objective was not possible due to a lack of information availability. Therefore, this section will contain a part detailing what evaluation has been performed and a part which sets out a plan for further evaluation.

5.2.1 Risk rating comparison

The most logical step is to compare how the risk ratings are currently compiled to how that is done using the risk model. The first section will explain how it is currently performed and the second section will explain how this differs with the new method.

Current risk rating process

For each change activity that is planned, a runbook is created. This used to be an Excel sheet which was sent to the Service Quality Centre (SQC), who then reviewed the runbook and the organisation wide planning, in order to plan the change activity. Quite recently this has been integrated in the new ticketing system. In both cases, a risk and impact section needs to be filled in to determine the risk classification of that specific change activity. This risk classification must not be confused with the change type classification. The risk classification is measured for each change activity separately and results in a classification of 'low', 'medium' or 'high'. This is comparable to, what in the risk model of this research is called, the risk rating. The change type classification is a classification for a whole type of change, like the four types that have been used as examples in this research. These can be classified as 'Standard' or 'Normal' (there are other classifications, but these are not relevant to this research).

The three categories determining the risk classification are 'Impact', 'Complexity' and 'Experience'. Based on the amount of clients impacted in the worst case scenario of that change activity, impact is classified as either 'low', 'medium' or 'high'. Based on the amount of parties involved and the different technical elements being impacted, complexity is classified as either 'low', 'medium' or 'high'. Finally, experience gets the same kind of classification based on if the change has been performed before, if it has been performed successfully before and if the change has been tested or not. The three categories are then combined to give a risk classification. This classification can be influenced by the possibility of a rollback, the duration of the change activity and if the downtime for customers is lower than 30 minutes. Resulting in the final risk classification.

Differences with the new process

The main difference between the two processes is that the new method uses historic data to give an overall risk classification to the change type. Not only to a specific change activity, as in the currently used process. That is because in the current process, the risk classification and the change type classification are defined separately. A change type can only be classified as standard if there has been no client impact for at least a year due to that type of change. Using the new process, a risk rating is calculated based on historic data, which can be used as a reason to reclassify a change, aswell as give a measure of risk and impact.

Looking at the risk rating and risk classification specifically, the logic behind the calculations are comparable. Impact is handled in more detail in the new process. It does not only take in account impacted clients, but based on the damage categories you are comparing, also looks at the costs. Having the different damage categories also gives the users more insight in what is exactly being impacted. The complexity and experience are represented in the new process by the historic data. Based on the results of the past, which are influenced by the experience and complexity of the change, the probabilities for impact are redefined. Another important difference is that new process is measured on a four point scale (green, yellow, orange and red), instead of a three point scale (low, medium and high). The four point scale, like the different damage categories, go in more detail than what the current process does. This is because the new process needs more detail in order to be able to be used as substantiation for reclassifying change types. Also, the four point scale is based on a numerical result. Which means that changes that share the same classification, can be compared and ranked in order of most riskful.

When comparing the new risk ratings to the current risk classification, the results match. This means that for the four example change types (1-10G, 1G, NT and WAP migrations), the risk classification and risk rating, are both classified as low. These results have been discussed and tested further in cooperation with two stakeholders from the SQC department. This is the department that manages everything that has to do with change requests in the organisation. By varying the historic data used to calculate the risk rating and making similar changes in the runbooks, the impact on the risk classification and rating can be further compared. The impact on the risk classification and rating has been proved comparable for the four change types used during this research.

Conclusion so far

After having performed and discussed this evaluation with the relevant stakeholders, the following can be concluded about the second objective of the model. The risk ratings calculated with the micro risk model for the four example change types have been tested and seem to overlap with current risk classification results. This means that the way risks are calculated in the risk model matches with the expectations of KPN. But by using the new process, a more detailed insight is provided on which decisions can be made. The different damage categories and numerical values as rating, give the means to discuss in more depth how riskful a change really is, compared to the current process. Therefore it can be concluded that objective two has been achieved in part. It does not however, provide an idea of how usable this process is for reclassifying changes, as that has not been evaluated.

5.2.2 Plan for further evaluation

To be able to conclude the evaluation, further steps need to be taken. Therefore the following section will contain a plan on how to further evaluate the risk model. Assuming the necessary information is available.

To test how usable and effective this process is at reclassifying changes, the risk rating of a standard change needs to be calculated. There is a list where all the standard changes are recorded and most of those are performed outside of maintenance windows. Some exceptions, that have no client impact but are potentially very riskful, are still performed in maintenance windows. Calculating the risk rating of those changes using this process would be the perfect test to see how effective this process can be. The necessary information to be able to do this evaluation is a list of these changes and their historic data. The difficulty is mainly in getting the historic data to make the risk model.

After having performed this step, another evaluation step that would be of value is measuring the effectiveness of moving changes out of the maintenance windows. This could be measured in multiple ways. Calculating the difference in cost of doing the work during the day instead of during the night provides the potential cost reduction. The second way effectiveness can be measured is seeing how much space is created in maintenance windows to perform other change activity. Potentially taking goals that are in danger of not being met on time, out of the danger zone. This would result in a more comprehensive evaluation.

5.3 Objectives for KPN

To see if the created artefact has reached the objectives set for KPN, the objectives will be recapped and for each objective a short explanation is given.

5.3.1 Objective 1: Increase the percentages of FTR performed changes

If KPN decides to start using this method to do all their risk assessments for their changes, this will improve the percentage of FTR performed changes. The threats that were identified for the four change types in 2018 have been taken in account and measures have been taken to bring them down. This has achieved the objective of increasing the FTR percentages of these Changes. Would this method be applied throughout the organisation, it could have a significant influence on increasing FTR percentages for all changes.

5.3.2 Objective 2: Minimise the risk of impact on the clients

Using this method gives a more in dept risk assessment of the performed changes compared to the current method of working. However, because the current process classifies every change that has had impact on clients in the last year as a normal change, using the new method could be considered as increasing the risk for clients. This is a logical consequence, as the current method trades in efficiency for risk reduction, while the new method tries to increase efficiency at the cost of taken a bit more risk. But because of the more in depth risk assessment, the taken risk is minimised and almost negligible. In the case of the four examples, for two of the four changes only once in 2018 would there have been extra impact on clients (a blue Be-alert). In order to see if taking that risk would be worth it, the impact of doing these changes during day time would have to be calculated. This could be measured in costs as well as amount of work done compared to what has been achieved now.

5.3.3 Objective 3: Increase the maintenance pace

Based on the examples in this research, the possibility to change the classification of one or more changes has been created by using the proposed method. A more comprehensive evaluation is necessary in order to fully ensure the value of this risk model and process in this regard. But it does already provide a more detailed view, which can be better compared than in the current process. Would this be done for the whole organisation, the best possible set of changes could be calculated based on preferences of the organisation. Increasing the pace of maintenance as well as decreasing the cost, while increasing the risk by a minimum.

5.4 Evaluation conclusion

A good start has been made in evaluating the risk model and its process. For one of the three objectives, providing insight in order to improve the success rates, it has shown that it helps solving the problem. For the two other objectives a promising start has been made and with further evaluation a more definite proof of concept can be given.

Chapter 6

Conclusions

Based on the problem stated by KPN, the demarcation made for this research and its results, a conclusion is given in this chapter. This will cover the answers to the research questions presented in the introduction. In this chapter, the theory is combined with the demonstration and evaluation, providing an answer to sub question five.

6.1 Sub question 1: What risk model is appropriate to achieve the required results?

There are two results needed from the risk model. First it needs to provide insight into what can be done to improve the current change activity in maintenance windows. The second result is that it can provide numerical substation for discussion about classification of changes. For both results, a quantitative approach is best used. These quantitative methods can be either deterministic or probabilistic. Modelling the risks of maintenance work is probabilistic, which means the amount of options has been decreased to a certain amount of methods. The bow tie method is a combination and an expansion of two of those methods, event trees and fault trees. Combining the two provides the necessary insight in order to improve the change activities and create risk ratings based on the inputted data. Therefore the choice has been made to use the bow tie methodology as risk assessment method.

6.2 Sub question 2: What information is needed to create the risk model?

This sub question and its parts are focused on determining the necessary information to be able to create the risk models. Answering these question is essential to create and use the models to answer the other questions. Collecting the necessary data and creating risk models for all the changes that are performed at KPN is not possible in the time frame of this research. Therefore, a representative selection which can be used as an example needs to be identified.

To identify what changes are good options, knowing what changes exists and how they differ is important. KPN performs all kinds of changes on their network. These can be service, infrastructure, maintenance or migration related. Each of these changes are classified based on their risks and impact. The main classification types are standard and normal changes. The difference between them is that standard changes have not caused impact on clients during at least a year, whereas normal changes have. Which means that standard changes do not need to be performed during maintenance windows and are easier to plan. For these changes to be representative, they need to represent a substantial part of the KPN workload.

After determining what kind of changes can be representative for KPN, it is important to determine if the necessary information for this research is available. The necessary information to create risk models consists of knowing what hazards, events, threats and consequences exists for the changes. This means that project managers responsible for their changes need to collect this information for a period of time. This is not common practice at KPN, as this information is not used. Risks and impact are only looked at a macro level and not at a micro level. For the selected changes, the project manager has been collecting the needed information since 2018. A total of four hazards, four events, twenty five threats and six consequences have been identified.

The next step is to identify the probabilities and impact. The probabilities can be derived from the data that has been collected throughout 2018. The amount of changes performed is compared to the amount of successful and failed activities. These percentages can then be split up into amounts per threats and how often it has led to consequences. In order to determine impact, the Be-alert classification matrix is used. This document describes the different severities of Be-alerts and what their impact is. This varies from impacted clients to damage expressed in money. All this data is put into the model and used in the calculations to calculate risk ratings.

To determine what barriers are in place a micro approach needs to have been taken. Barriers are systems or actions that have been put in place in order to prevent threats from happening or to mitigate consequences. If it is not clear what threats are responsible for failures or what the consequences are of a failure, it is not possible to consciously put barriers in place. As a micro approach to risks and impact is not used at KPN, there is no information available on barriers that have been put in place. One of the goals of the risk model is to provide the necessary insight to effectively place barriers. For each of the four changes that have been used as an example in this research, areas of focus have been identified for potential effective barrier implementation.

Determining acceptable risks for KPN is not clear cut. The goal is to determine a maximum acceptable risk rating in order to compare changes with each other and determine the classification. But this can change for each type of change. It also depends on who is interpreting the results. Therefore it is not possible to set a max acceptable risk rating or a range.

6.3 Sub question 3: How does a micro risk model help classify changes differently?

The third sub question needs to be answered because the change classification plays a big role. Changing a change type from a normal classification to a standard classification means that maintenance windows can be used more efficiently and costs of activities goes down. Using a micro risk model should make this possible more often and therefore be of worth to telecommunication providers.

The current way of determining if a change type can be classified as standard or normal is by looking at the impact it has had in the last year. If a change has had impact on clients in the last year, it is classified as a normal change. This means that planning work of that change type needs to be accompanied by a run book and needs to be approved. Then it gets accorded a place during a maintenance window. Standard changes don't have a complicated approval process. It will also be planned during the day instead of during a maintenance window. Working this way does not take all aspects into account and has as a result that certain changes are classified as a normal change while they don't need to be. This is where a micro risk model can help.

By using probabilities and impact during a risk assessment, an organisation can get a more complete view of the risks. Identifying the actual probabilities of something going wrong and actually impacting clients provides the necessary information to make logical and efficient decisions. Looking at the results of the example changes, it can be seen that changes are rated as yellow, slightly more riskful. This means that changing the classification can be done without taking a big risk. If the impact of changing the classification is impactfull, the usages of the risk model has created the opportunity to discuss this option. It can then be used to compare the changes to select which change can be best classified into a standard change while taking the least amount of risk. In this case that would either be NT or 1G migrations. This results is to be expected, as there have not been any Be-alerts in 2018 for either one of these changes.

6.4 Sub question 4: How does changing classification of changes make change planning more efficient?

The fourth sub question important to answer because it shows how using the risk model to change the classification process increases efficiency of the change planning. Increasing the efficiency in this case has been defined in two ways. First as improving the success rate of the changes that are currently being done in the maintenance windows. Secondly as increasing productivity by clearing the maintenance windows of changes that can be done during the day without too many risks.

Improving the success rate of changes is straight forward. The less activities that need to be rescheduled, the more work can be planned and performed. Looking at the four example changes, for each one of them a selection of threats on which needs to be focused has been given. Improving on those threats by implementing the right barriers can greatly improve the success rate.

The data that has been collected in 2018 for the four changes discussed in this research has also been collected for 2019. This provides the means to test if having insight into threats and consequences improves the success rate of change activity. By comparing the failures rates for each change activity and the cause of those failures in 2018 with the same data in 2019, a decrease in failure rates has been measured. This can be seen in the total failure percentages, which has decreased, but it is more interesting to look at the percentage share for each threat. For example, in 2018 for 1-10G migrations, 19.3% of the failed migrations was due to problems with the 'Cabling'. In 2019, that has been decreased to 1.6%. Proving that having insight into the relevant threats can help project managers to increase the success rate by targeting the biggest threats. This does not change the fact that new threats can arise, impacting the success and failures rates. But knowing what those threats are and how large their share is in the total failure rate can provide the tools to quickly react and improve.

Increasing productivity by clearing maintenance windows can be achieved by changing the classification process. By reevaluating all the normal classified changes performed by KPN through a micro risk model, new risk ratings based on more than just one factor can be created. Based on those results, the choice can be made to change the classification of a change if it can increase productivity without increasing the risk too much. The results of just looking at the four example changes is that changing the classification of these changes could be done without taking much more risks. It is even possible to give an order of more or less riskful change type if only one change type would need to change classification. Compared to the current process, where changing the classifications of these migrations would only be discussable once a year, this method can used as many times a year as deemed necessary.

6.5 Sub question 5: Does the risk model legitimise changing the classification of changes?

The last sub question is focused on implementation. For a method like this to work, the results need to be trusted. Compared to the current process, this is more complicated. Looking at the performance of a change type and basing its classification on one indicator, has it impacted clients in the last year, is a straight forward way of determining a classification. The proposed method, through the use of an extensive micro risk model, increases the complexity.

The way the new method of classifying legitimises classification changes is through the usage of numeric data. The first aspect of the model, increasing insight in what leads to failed activities, is easy to understand and straight forward. Identifying how often a certain threat leads to failure is an easy measuring system to identify what needs to be improved. The complexity increases when probabilities are combined with impact and the results are normalised. It does provide numerical values which can be compared, but the values don't provide a clear context. When people discuss units such as costs in money or impacted clients, users understand what is discussed. Normalised values, that tell how much a raw value differs from the mean with the standard deviation as a unit, does not convey a context or an order of magnitude. This makes it difficult to understand and use this method for users that are not specialised.

This method does however, provide a more in depth analysis of the risks and impact associated to a change. It does therefore, in the hand of an experienced user, legitimise the classification of a change better than the current way of working.

6.6 Main research question

The main research question exists out of two parts, how the use of a micro risk model legitimises classification changes and how the use of a micro risk model makes change planning more efficient. Compared to the current situation, using the provided model and its insights gives decision makers more details on which to base their decisions on. As these details are based on historic data which has been used to calculate probabilities and potential impact on different parts of the organisation, it can be said that the use of the model provides more legitimisation than the current methods. Having this detailed information also provides the tools to influence how changes are being classified. Which in turn leads to more efficient change planning. What also can be concluded for sure, is that working with a micro risk model improves insight in how the current change activity can be improved. Which does positively influences the efficiency of change planning. All in all, using risk based maintenance methodology does provide tools for the telecommunication sector to improve on their maintenance planning.

Chapter 7

Communication & Reflection

Using models and their results is never straight forward. Every type of model is a representation of a part of a real system and is therefore partly based on assumptions. The way a model is used, the information that is put into the model and the results are subject to interpretation. The research also faces several limitations. The chapter will start by giving recommendations to KPN.

7.1 Recommendations for KPN

There is much information to process from this thesis. In order for KPN to get the most out of this research there is much that still needs to be done. This section will provide a suggestion of how to best approach this.

7.1.1 Recommendation 1: Record micro data

The first recommendation is something that can be implemented without having to do other research. Start recording micro data for every change that is preformed. This means recording how many times a change is performed per month, how many times it was performed nFTR and most importantly what is the exact reason for it being performed nFTR. Doing this provides insight in what needs to be improved to get better success rates. Which in turn safes money and improves the maintenance pace. This is something that needs to be done continuously, as new problems that impact the success rate can arise at any time. The faster the project managers are informed, the better they can react. The second reason for doing this, is that this data can then be used to calculate probabilities, which can be used for more in depth risk assessments. Even if the risk assessments methods used in this research are not considered operable or efficient, there are many other possible risk assessments for which this kind of data is necessary that could be of use of for KPN. Part of this data is already being recorded by the ticketing system, but it is lacking in the most important details.

7.1.2 Recommendation 2: Perform more in depth evaluation

If KPN would like to continue with the concept provided by this research, more evaluation is needed. Creating risk models and calculating the risk ratings of other change types needs to be done in order to see how effective this method could be. Starting with the change types that have no impact on clients, but are still classified as normal changes. If this method can provide the necessary insight for one or more of those changes to be reclassified as standard, it can be tested on other changes. This step by step evaluation provides the context in which the model can be most efficiently used.

Another evaluation step that would help decide the exact value of using this model, is calculating what the exact profit is of changing change type classifications. By calculating the gains in costs and more importantly, the gains in "room" during maintenance windows, a comprehensive comparison can be made. This help determining if changing a certain classification is worth the potential increase in risk. For example, changing the classification of a change type that is performed a couple times a year while this might increase the risks ran by KPN, might not be worth it. But if the change is performed more than a 1000 times a year, the increase in risk might be worth the decrease in cost and increase in maintenance window room.

7.1.3 Recommendation 3: Make the calculations automatic

Making the models based on recorded information will stay work that needs to be done by hand. While bow tie models help structure and communicate findings, they are not necessary to collect and use the data. Therefore it is not the most critical part of the model. The calculations however, play an important role in determining the risk rating. This part of the model could be automated. Provided that an excel sheet or a piece of software is developed, which only needs data inputted to calculate the ratings. This would greatly improve the ease of use. This could in turn make incorporating this model and its calculations in a periodic process easier. For example, if every project managers collects the necessary data, every six months new risk ratings could be calculated. This could make the change planning more dynamic while preserving a risk mitigating attitude. Improvements made in performing changes could be monitored and based on the results maintenance windows could be used more efficiently.

7.1.4 Recommendation 4: Combine the results with other research plans

While using risk models to improve maintenance planning is a good start, there are many other domains where research could help improving maintenance planning. To start with client and contract management. There has never been research performed by KPN to determine what the best time for maintenance windows is. It has always been assumed that at night would be preferable, as less people are active. But in a 24/7 economy, this does not necessarily needs to be the case. This needs to be combined with contract management, as KPN has agreements with their clients which would potentially need to change. As changing contract agreements can have consequences, the details need to be figured out. Another research point of view that could contribute to solving the problems faced by KPN is process optimisation. During the research it became clear that different parts of the organisations have different expectations of each other and different ideas about what each others responsibilities are. This creates friction and does not help in solving problems. Recreating the processes around change planning could help restructure responsibilities and modernise the process, which is outdated.

7.2 Scientific contribution

This research adds to the risk based maintenance literature in the telecommunication sector. There is no literature about RBM in the telecommunication sector, while the concept has been proven efficient in other sectors. This is the first example of RBM, with some slight adjustments, being implemented in this sector.

The main difference between implementing RBM in the telecommunication sector compared to other sectors, is that RBM in other sectors focuses mainly on internal impact. For example, if a machine breaks down in a plant, production is stopped or slowed down, which results in less products made. This does not directly impact clients of the product. In the telecommunication sector, if maintenance or any adjustments to the networks fails, clients will be impacted. This is not taken in account in standard RBM. The second difference is that RBM contains a planning module, which is used in all the other sectors. Based on the risk assessment, the final result of implementing RBM is a maintenance plan. The plan tells the user when to perform maintenance on what machine, in order to decrease the risks of the production being disturbed and increase the total output. As the planning is made by only looking at internal impact, it is not useful to use it for the telecommunication sector.

In order to incorporate impact on the clients, the damage categories have been altered. In general, there are four damage categories that are mostly used. These are People, Environment, Assets and Reputation. Changing them to represent different services delivered to the clients, made the risk assessment more workable for the telecommunication sector. For the final result, the planning module is not used, but it ends with a risk rating for the change types. These can be used to change conditions (such as change classification) that impact the final change planning.

Using RBM to influence the change planning in the telecommunication sector is interesting, but there are some reasons why making it applicable in the telecommunication sector is challenging. The fact that the impact in not focused internally, as with other sectors, means that there are several restrictions a RBM implementer need to deal with. There are agreements and contracts with the clients for example, that complicate the matter. Another complication is that when calculating the risk of a machine failing, the impact on the production process is measurable and objective. This is not always the case in the telecommunication sector, where the impact is not always clear, nor the severity of the impact. These challenges are not a deal breaker for RBM in the telecommunication sector. But they are the reason that more intensive evaluation is necessary for RBM to be embraced in the telecommunication sector.

Even if the results are not definite, some promising results have been shown. A lot more research has to be done in order to make a convincing case for RBM in the telecommunication sector, but this start could be a trigger for more tests. The model itself, as well as the calculations, are not groundbreaking. It is the process in which the model and calculations are used that is interesting. The idea to focus the process on a micro level, instead of a macro level, is not common in the telecommunication sector. But the potential benefit of working on a micro level, warrant the time spend on researching and implementing micro methodologies in the telecommunication sector. This way of thinking and looking at the maintenance issue in the telecommunication sector is new.

7.3 Limitation of the generalizability

The limitation of this research in context of generalizability, is that it is focused on one provider. Because of the lack of information and data in regards of this topic, most concepts originate from KPN, as well as processes that have to do with maintenance. This makes it difficult to use the results for the whole sector. In discussing this matter with professionals working at KPN, the conclusion was quickly made that even though most of the information originates from KPN, most other providers work in a comparable fashion. There might be slight differences, but in general the logic behind maintenance planning is very much comparable. While this is a comforting thought, it is not the same as having confirmation by other providers that this is really the case. Therefore it is difficult to generalise the results of this research. For that to be legitimate, more research in this sector is necessary.

The main assumption that is made during this research in terms of generalizability, is that working on a micro level is not common practice for all telecommunications providers. If that is not the case, the results or the model are not less applicable, but it would decrease the innovative value of the research. The potential gains in the FTR percentages due to recording and acting on micro data will still be relevant. The same goes for giving risk ratings based on a more detailed risk assessment. Another assumption is that all the telecommunication providers work with maintenance windows or a similar concept. If that is not the case, providing a process which can help change risk classifications in order to unburden maintenance windows, losses a part of its application value. A more detailed risk assessment can still retain some value, but the goal for which it has been devised is lost in this case. The last major assumption is that all telecommunication providers use risk and impact to classify their changes. If they do not do that, but have another system, then the results are invalidated and the models losses all its application. The model could still be used to start measuring risks and impact, but for it to work properly, basic information about risks and impact need to be available.

7.4 Limitation of the scientific contribution

This research is a first step for RBM in the telecommunication sector. The results of the research show promise, but there is one important limitation to the results. A comprehensive evaluation is missing. Because of this, most of the results are unsure. This means that while it looks promising, the results could in the end be underwhelming. This is a shame, as the potential of RBM has been proven in other sectors. If a better evaluation would have been possible, it might have meant a stronger start for RBM in the telecommunication sector.

7.5 Limitation of the validation

In the department of validation a lot more could be done to compare the proposed method to the current process used at KPN. One of the first things that could be done is to calculate the cost reduction of changing the classification of one type of change. For example, in 2018, the 1G migration was performed 3058 times. This has always been done during maintenance windows. Is would be interesting to see how much it would reduce the cost if the 3058 migration were performed outside of maintenance windows. It would also be of interest to know what could have been done in the 3058 of spots freed up because of the classification change. Putting in context what the total impact of a classification change can be. This would also make the trade off between an increase of productivity against taking a bit more risk more tangible. The reason that this would be of added value is because it provides a measure of effectiveness. This can then be used to determine in what cases a change in classification would be worth it. The reason this has not been added to this research is a lack of information availability and a lack of time to create this data.

7.6 Limitation of the results

Next to the limitations of the models themselves, a very important note to make is the limitation of the results. Often, numerical values are taken for they are, as an absolute truth. Nothing is less true in the case of these results. There are many ways in which these values can be calculated. The way that was used during the research is just one way, but even here a short mention is made of how the Z-score could have been calculated differently as shown in Appendix **??**. This can be combined with the difficulty mentioned about the risk models, where a thorough understanding of the system is necessary. Knowing the system will give the modeller a better idea of how to get results that best represent the organisation.

Another complication is this regard is that one could choose to look at the total risk rating, but one could also look at the risk ratings of the consequences. Where an overal risk rating could communicate that a risk is not eligible for a classification change, looking at the consequences risk rating could say something different. In the examples used in this research, the orange and red Be-alerts have had a big impact on the total risk rating. But considering that there have never been any orange or red Be-alerts triggered by these changes and that the risk of that happening is very close to 0, one could decide to change the overal risk rating to almost no risk (green) instead of slightly more riskful (yellow). The reason that the red and orange Be-alerts have such an influence is because the impact used to calculate the rating increases a lot in those categories of Be-alerts. While this is something that KPN likes to have represented in their risk assessments, it does not necessarily result in the best advice.

In this research no use has been made of weights to amplify certain aspects of changes. For example, KPN wants to limit the down time their clients experience. In the performed risk assessment, the down time of the different changes have not been taken in account. Two of the migrations have a max down time of five minutes, while the other two have a max of one hour. This is a major difference, which could impact the possibility of changing classifications. What this section is trying to say is that the way the results are created, interpreted and used is depended on the users. This means that organisations that will want to use a method like this, will need in house knowledge of how to best interpret and use the results. Increasing the difficulty of using this method in comparison to the overly risk preventive method used currently.

7.7 Limitation of the scope

The underlying problem that lies at the basis of this research, stated in the problem statement of KPN, making better use of maintenance windows, is a multi-disciplinary problem. This research has looked at the organisation of the maintenance process, specifically at the risk and impact assessment part. While this is a logical scope for a thesis, it is not big enough of a scope to solve this problem. Other parts where research is necessary to solve this problem is client management, contract management and process optimisation. This will be discussed in more detail in the 'Further research' section.

7.8 Further research

To increase the usage of RBM in the telecommunication sector in general, more research is necessary. The most important step would be to have similar studies done across the telecommunication sector. If more studies are done at different providers around the world, a standard of working can be devised. That way the general applicability of RBM in the telecommunication sector can be improved. For the adaptation of RBM in the telecommunication sector, it is important that research is done specifically evaluating different approaches of RBM. There are many risk assessment methods that are potentially as efficient if not more efficient at creating risk ratings, as the method used during this research. Evaluating how efficient each method is in different situations can help increase the implementation of RBM in the telecommunication sector. The focus of these studies should be on evaluation, because it is not clear in how far RBM is an effective way of organising maintenance in this specific sector. If the gains of using RBM are minimal and the effort to use it effectively are high, then an alternative will need to be found or developed.

References

Abdi, H. (2007). Z-scores. *Encyclopedia of measurement and statistics*, *3*, 1055–1058.

Aceto, G., Botta, A., Marchetta, P., Persico, V., & Pescapé, A. (2018). A comprehensive survey on internet outages. *Journal of Network and Computer Applications*, *113*, 36–63.

Alcatel-Lucent. (2012). *Transforming the brand through improved customer experience: service provider strategies: Highlights from a heavy reading study for alcatel-lucent.* Retrieved from https://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2013/7149-alcatel-lucent-transforming-brand-through-improved-customer-experience.pdf

Anvarifar, F., Voorendt, M. Z., Zevenbergen, C., & Thissen, W. (2017). An application of the functional resonance analysis method (fram) to risk analysis of multifunctional flood defences in the netherlands. *Reliability Engineering & System Safety*, *158*, 130–141.

Arunraj, N., & Maiti, J. (2007). Risk-based maintenance—techniques and applications. *Journal of Hazardous Materials*, *142*(3), 653 - 661. Retrieved from http://www.sciencedirect.com/science/article/pii/S0304389406007345 (Papers Presented at the 2005 Symposium of the Mary Kay O'Connor Process Safety Center) doi: https://doi.org/10.1016/j.jhazmat.2006.06.069

Baybutt, P. (2014). The alarp principle in process safety. *Process Safety Progress*, *33*(1), 36-40. Retrieved from https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.11599 doi: 10.1002/prs.11599

Bhandari, J., Arzaghi, E., Abbassi, R., Garaniya, V., & Khan, F. (2016). Dynamic risk-based maintenance for offshore processing facility. *Process Safety Progress*, *35*(4), 399-406. Retrieved from https://aiche.onlinelibrary.wiley.com/doi/abs/10.1002/prs.11829

Castells, M. (2014). The impact of the internet on society: a global perspective. *F. González, ed*, 132–133.

CGE Risk Management Solutions. (2015). Bowtiexp - bowtie methodology manual [Computer software manual]. Retrieved from https://www.icao.int/safety/SafetyManagement/SMI/Documents/BowTieXP%20Methodology%20Manual%20v15.pdf

Dahiya, K., & Bhatia, S. (2015). Customer churn analysis in telecom industry. In *2015 4th international conference on reliability, infocom technologies and optimization (icrito)(trends and future directions)* (pp. 1–6).

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The iso 31000 standard in supply chain risk management. *Journal of Cleaner Production*, *151*, 616–633.

Dhillon, B. S. (2002). *Engineering maintenance: a modern approach.* cRc press.

EFMNS. (2019). *Efmns - who are we?*

Gandini, G., Bosetti, L., & Almici, A. (2014). Risk management and sustainable development of telecommunications companies.

Gericke, K., Klimentew, L., & Blessing, L. (2009, 01). Measure and failure cost analysis: selecting risk treatment strategies. In (p. 61-72). Retrieved from https://www.researchgate.net/publication/237049565_Measure_and_failure_cost_analysis_selecting_risk_treatment_strategies

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, 337–355.

Hanna, A., & Rance, S. (2011). Itil® glossary and abbreviations. *ITIL officialsite.* Retrieved from www.itil-officialsite.com/Publications/PublicationAcknowledgements.asp

Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22). Springer Science & Business Media.

ISO 31000: 2018. (2018). *Risk management–guidelines.* International Organization for Standardization Geneva.

ISO/IEC. (2006). International standard-iso/iec 14764 ieee std 14764-2006 software engineering; software life cycle processes &; maintenance.

Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E., & Mannan, M. S. (2018). Process resilience analysis framework (praf): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*, *53*, 61–73.

Kamoun, F. (2005). Toward best maintenance practices in communications network management. *International Journal of Network Management*, *15*(5), 321–334.

KarimiAzari, A., Mousavi, N., Mousavi, S. F., & Hosseini, S. (2011). Risk assessment model selection in construction industry. *Expert Systems with Applications*, *38*(8), 9105 - 9111. Retrieved from http://www.sciencedirect.com/science/article/pii/S0957417410014739 doi: https://doi.org/10.1016/j.eswa.2010.12.110

Khan, F. I., & Haddara, M. (2004, 12). Risk[U+2010]based maintenance (rbm): A new approach for process plant inspection and maintenance. *Process Safety Progress*, *23*(4), 252–265. Retrieved from https://doi.org/10.1002/prs.10010 doi: 10.1002/prs.10010

Khan, F. I., & Haddara, M. M. (2003). Risk-based maintenance (rbm): a quantitative approach for maintenance/inspection scheduling and planning. *Journal of Loss Prevention in the Process Industries*, *16*(6), 561 - 573. Retrieved from http://www.sciencedirect.com/science/article/pii/S0950423003000949 doi: https://doi.org/10.1016/j.jlp.2003.08.011

KPN. (2016, June 17). Change management process (2016). Retrieved from http://teamkpn.kpnnet,org/group/documents/groep-cics/6848e311-bab6-4b03-8318-366c4f026e6b

KPN. (2017). *Van isdn naar kpn een.* Retrieved from https://www.kpn.com/zakelijk/blog/van-isdn-naar-kpn-een.htm

KPN. (2018, August 1). Be alert classificationmatrix. Retrieved from https://teamkpn.kpnnet.org/embeds-ajax/download-document/lRjjM8DOyzmwnLfW26KI6iH0AHVfnmFzXh5k6czXPEWSeZeQdqpFAVeSkgW0-ZUC/lBPMxSDc8kOwnLfW26KI6iH0AHVfnmFzXh5k6czXPEWSeZeQdqpFATXLaDpK0Sv_

Krishnasamy, L., Khan, F., & Haddara, M. (2005). Development of a risk-based maintenance (rbm) strategy for a power-generating plant. *Journal of Loss Prevention in the Process Industries*, *18*(2), 69 - 81. Retrieved from http://www.sciencedirect.com/science/article/pii/S095042300500015X doi: https://doi.org/10.1016/j.jlp.2005.01.002

Kushnir, V. (1985). Risk: A probabilistic concept. *Reliability Engineering*, *10*(3), 183 - 188. Retrieved from `http://www.sciencedirect.com/science/article/pii/0143817485900204` doi: https://doi.org/10.1016/0143-8174(85)90020-4

Lees, F. (2012). *Lees' loss prevention in the process industries: Hazard identification, assessment and control.* Butterworth-Heinemann.

Lubritto, C., Petraglia, A., Vetromile, C., Curcuruto, S., Logorelli, M., Marsico, G., & D'Onofrio, A. (2011). Energy and environmental aspects of mobile communication systems. *Energy*, *36*(2), 1109–1114.

Mayer, N., Aubert, J., Cholez, H., & Grandry, E. (2013). Sector-based improvement of the information security risk management process in the context of telecommunications regulation. In *European conference on software process improvement* (pp. 13–24).

Musolesi, M. (2014). Big mobile data mining: Good or evil? *IEEE Internet Computing*, *18*(1), 78–81.

Nielsen, J. J., & Sorensen, J. D. (2011). On risk-based operation and maintenance of offshore wind turbine components. *Reliability Engineering & System Safety*, *96*(1), 218 - 229. Retrieved from `http://www.sciencedirect.com/science/article/pii/S0951832010001705`

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45–77.

Rausand, M. (2013). *Risk assessment: theory, methods, and applications* (Vol. 115). John Wiley & Sons.

Ray-Bennett, N. S. (2018). Systems failure revisited. In *Avoidable deaths* (pp. 79–107). Springer.

Ruijters, E., & Stoelinga, M. (2015). Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer science review*, *15*, 29–62.

Sarwar, M., & Soomro, T. R. (2013). Impact of smartphone's on society. *European journal of scientific research*, *98*(2), 216–226.

Sorensen, J. D. (2009). Framework for risk-based planning of operation and maintenance for offshore wind turbines. *Wind Energy*, *12*(5), 493-506. Retrieved from `https://onlinelibrary.wiley.com/doi/abs/10.1002/we.344`

Spiess, J., T'Joens, Y., Dragnea, R., Spencer, P., & Philippart, L. (2014). Using big data to improve customer experience and business performance. *Bell labs technical journal*, *18*(4), 3–17.

Van den Poel, D., & Lariviere, B. (2004). Customer attrition analysis for financial services using proportional hazard models. *European journal of operational research*, *157*(1), 196–217.

Verbeke, W., Dejaeger, K., Martens, D., Hur, J., & Baesens, B. (2012). New insights into churn prediction in the telecommunication sector: A profit driven data mining approach. *European Journal of Operational Research*, *218*(1), 211–229.

Vereecken, W., Van Heddeghem, W., Deruyck, M., Puype, B., Lannoo, B., Joseph, W., ... Demeester, P. (2011). Power consumption in telecommunication networks: overview and reduction strategies. *IEEE Communications Magazine*, *49*(6), 62–69.

White, D. (1995). Application of systems thinking to risk management: a review of the literature. *Management Decision*, *33*(10), 35–45.

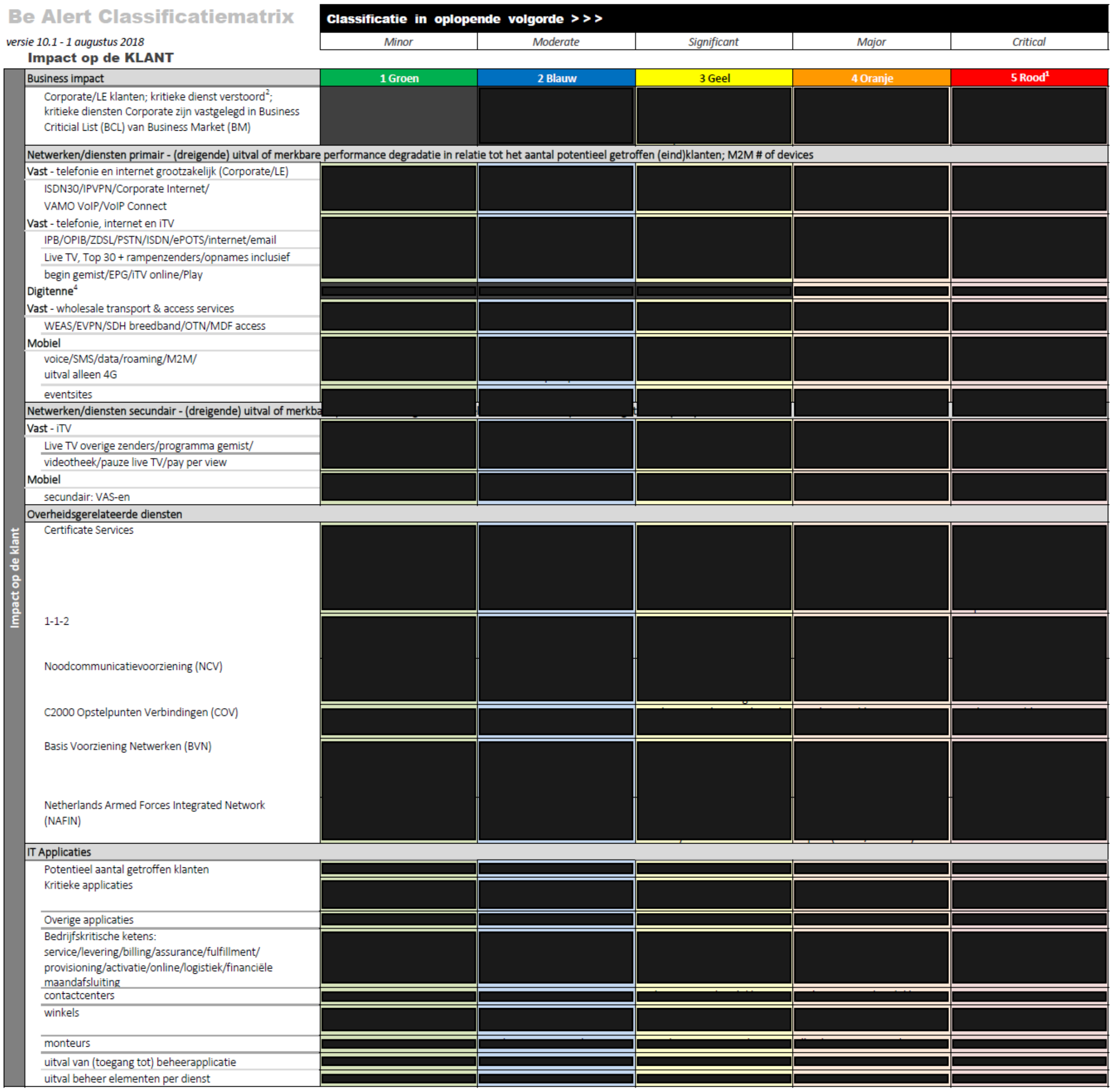
Appendix A

Be Alert classification matrix

The Be Alert classification matrix is an official document used by KPN (KPN, 2018). It defines what classification of Be Alert is given to any kind of loss of service distribution. As this document is an official document in use by KPN that details information that is not supposed to be shared with the public, the data has been taken out. That is the reason that two of the three figures in this Appendix contain black boxes. While this prevents getting a complete idea of how Be-Alerts are classified, it does give an idea what of what services impact is being measured on.

The table has been cut in to three parts. The first part, Figure A.1, is focused on client impact. Based on the amount of impacted clients and the importance of the service that is malfunctioning, a problem in service delivery is classified as one of the five Be Alert categories. The classifications are based on the colours green, blue, yellow, orange and red, representing the severity levels minor, moderate, significant, major and critical respectively. The second part, Figure A.2, is focused on the impact on KPN. The classification is based on security impact, damages in € and service disruption. The last part, Figure A.3, explains how to upscale a Be Alert and when a Be Alert manager needs to consider this.

The different types of impact on the client can be seen in Figure A.1 in the left column. These are business impact, primary services, secondary services, government-related services and IT applications. Depending on the importance of the service the amount of impacted clients differs. This can go up till more than a million clients impacted. These values are used in determining the risk ratings of different change types. For government-related services other measurements are used. But as government-related services like for example 1-1-2 are critical services, changes related to them will never be classified as standard changes. No risks are to be taken with these services. Therefore they are less relevant for this research. IT application is measured in impacted clients, aswell as accessibility of locations, accessibility of applications and down time.



Be Alert Classificatiematrix

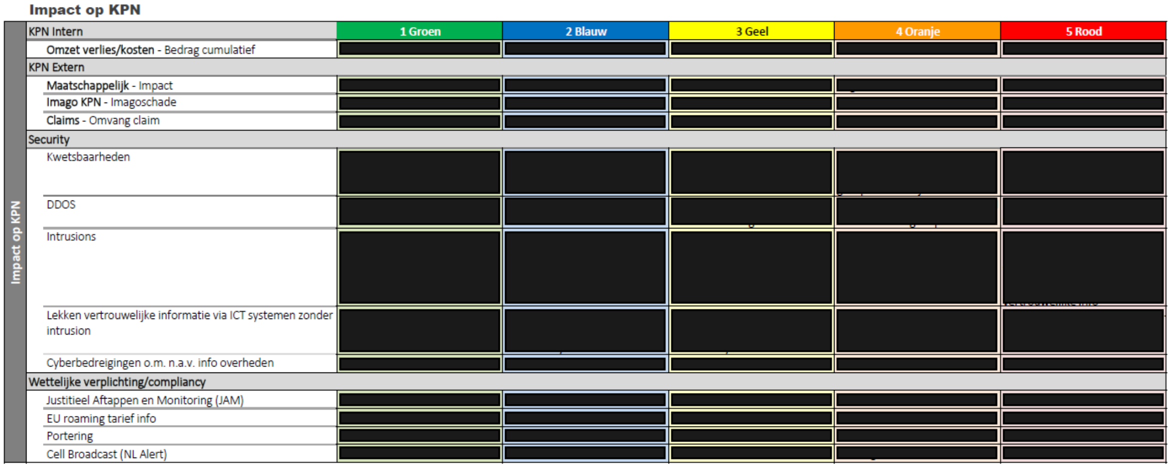
versie 10.1 - 1 augustus 2018

Impact op de KLANT

Impact op de klant

	Classificatie in oplopende volgorde > > >				
	Minor	*Moderate*	*Significant*	*Major*	*Critical*
Business impact	1 Groen	2 Blauw	3 Geel	4 Oranje	5 Rood[1]
Corporate/LE klanten; kritieke dienst verstoord[2]; kritieke diensten Corporate zijn vastgelegd in Business Criticial List (BCL) van Business Market (BM)		[redacted]	[redacted]	[redacted]	[redacted]
Netwerken/diensten primair - (dreigende) uitval of merkbare performance degradatie in relatie tot het aantal potentieel getroffen (eind)klanten; M2M # of devices					
Vast - telefonie en internet grootzakelijk (Corporate/LE)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
ISDN30/IPVPN/Corporate Internet/					
VAMO VoIP/VoIP Connect					
Vast - telefonie, internet en iTV	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
IPB/OPIB/ZDSL/PSTN/ISDN/ePOTS/internet/email					
Live TV, Top 30 + rampenzenders/opnames inclusief					
begin gemist/EPG/iTV online/Play					
Digitenne[4]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Vast - wholesale transport & access services	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
WEAS/EVPN/SDH breedband/OTN/MDF access					
Mobiel	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
voice/SMS/data/roaming/M2M/ uitval alleen 4G					
eventsites	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Netwerken/diensten secundair - (dreigende) uitval of merkba					
Vast - iTV	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Live TV overige zenders/programma gemist/					
videotheek/pauze live TV/pay per view					
Mobiel	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
secundair: VAS-en					
Overheidsgerelateerde diensten					
Certificate Services	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
1-1-2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Noodcommunicatievoorziening (NCV)					
C2000 Opstelpunten Verbindingen (COV)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Basis Voorziening Netwerken (BVN)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Netherlands Armed Forces Integrated Network (NAFIN)					
IT Applicaties					
Potentieel aantal getroffen klanten	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Kritieke applicaties	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Overige applicaties	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Bedrijfskritische ketens: service/levering/billing/assurance/fulfillment/ provisioning/activatie/online/logistiek/financiële maandafsluiting	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
contactcenters	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
winkels	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
monteurs	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
uitval van (toegang tot) beheerapplicatie	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
uitval beheer elementen per dienst	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Figure A.1: Be Alert classification matrix - Impact on the client

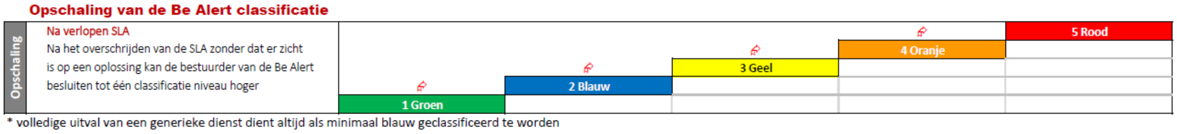


Impact op KPN

Impact op KPN	KPN Intern	1 Groen	2 Blauw	3 Geel	4 Oranje	5 Rood
	Omzet verlies/kosten - Bedrag cumulatief	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	KPN Extern					
	Maatschappelijk - Impact	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Imago KPN - Imagoschade	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Claims - Omvang claim	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Security					
	Kwetsbaarheden	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	DDOS	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Intrusions	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Lekken vertrouwelijke informatie via ICT systemen zonder intrusion	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Cyberbedreigingen o.m. n.a.v. info overheden	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Wettelijke verplichting/compliancy					
	Justitieel Aftappen en Monitoring (JAM)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	EU roaming tarief info	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Portering	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	Cell Broadcast (NL Alert)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Figure A.2: Be Alert classification matrix - Impact on KPN

Figure A.2 shows the different conditions regarding Be Alert classifications for impact at KPN. The types of impact at KPN are internal impact, external impact, security and legal obligations. Loss in revenue and damages in claims is measured in €. Societal impact and damage to the image of KPN due to failures of services are measured in amount of clients and area of effect. Security is split up different types of attacks. Governmental obligations are measured in quality of service and outages. For this research, governmental obligations are not of importance, as changes that have an impact on the services will never be classified as standard.



Opschaling van de Be Alert classificatie

Opschaling						
	Na verlopen SLA					5 Rood
	Na het overschrijden van de SLA zonder dat er zicht				4 Oranje	
	is op een oplossing kan de bestuurder van de Be Alert			3 Geel		
	besluiten tot één classificatie niveau hoger		2 Blauw			
		1 Groen				

* volledige uitval van een generieke dienst dient altijd als minimaal blauw geclassificeerd te worden

Figure A.3: Be Alert classification matrix - Upscaling

The last part of the table can be seen in figure A.3. This is used to show when a Be Alert manager needs to consider upscaling the classification.

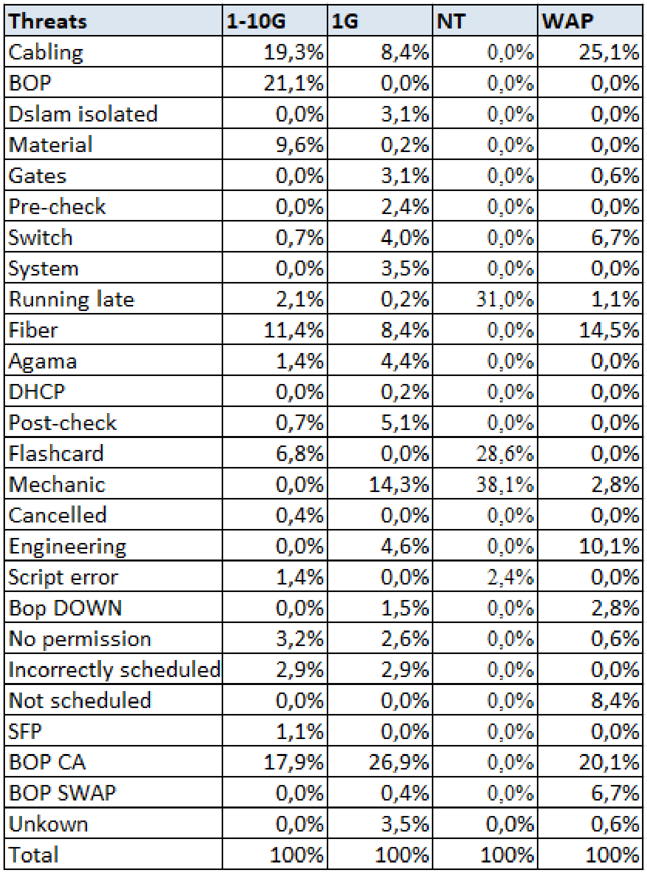
Appendix B

Threat percentages

B.1 Percentages 2018

In Table B.1 an overview is given off all the threats for each migration type and how often these threats have lead to an nFTR situation in 2018.

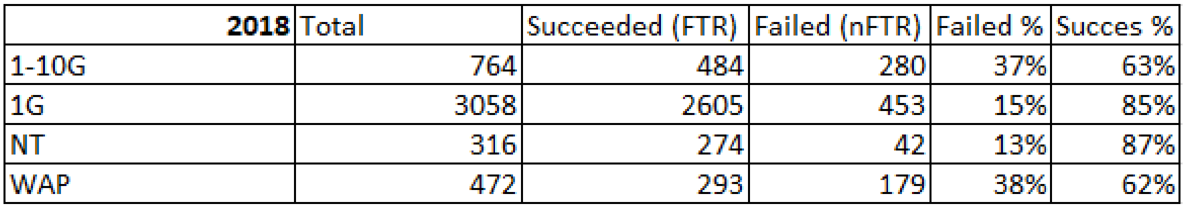
Table B.1: Threat percentages per change 2018



Threats	1-10G	1G	NT	WAP
Cabling	19,3%	8,4%	0,0%	25,1%
BOP	21,1%	0,0%	0,0%	0,0%
Dslam isolated	0,0%	3,1%	0,0%	0,0%
Material	9,6%	0,2%	0,0%	0,0%
Gates	0,0%	3,1%	0,0%	0,6%
Pre-check	0,0%	2,4%	0,0%	0,0%
Switch	0,7%	4,0%	0,0%	6,7%
System	0,0%	3,5%	0,0%	0,0%
Running late	2,1%	0,2%	31,0%	1,1%
Fiber	11,4%	8,4%	0,0%	14,5%
Agama	1,4%	4,4%	0,0%	0,0%
DHCP	0,0%	0,2%	0,0%	0,0%
Post-check	0,7%	5,1%	0,0%	0,0%
Flashcard	6,8%	0,0%	28,6%	0,0%
Mechanic	0,0%	14,3%	38,1%	2,8%
Cancelled	0,4%	0,0%	0,0%	0,0%
Engineering	0,0%	4,6%	0,0%	10,1%
Script error	1,4%	0,0%	2,4%	0,0%
Bop DOWN	0,0%	1,5%	0,0%	2,8%
No permission	3,2%	2,6%	0,0%	0,6%
Incorrectly scheduled	2,9%	2,9%	0,0%	0,0%
Not scheduled	0,0%	0,0%	0,0%	8,4%
SFP	1,1%	0,0%	0,0%	0,0%
BOP CA	17,9%	26,9%	0,0%	20,1%
BOP SWAP	0,0%	0,4%	0,0%	6,7%
Unkown	0,0%	3,5%	0,0%	0,6%
Total	100%	100%	100%	100%

Table B.2 shows the total amounts of performed migrations. This has been split up in failed and successful migrations. This gives an idea of how many migrations of this type are being performed during maintenance windows, as well as showing how much improvement can be made in the success rate.

Table B.2: Success and failures percentages 2018

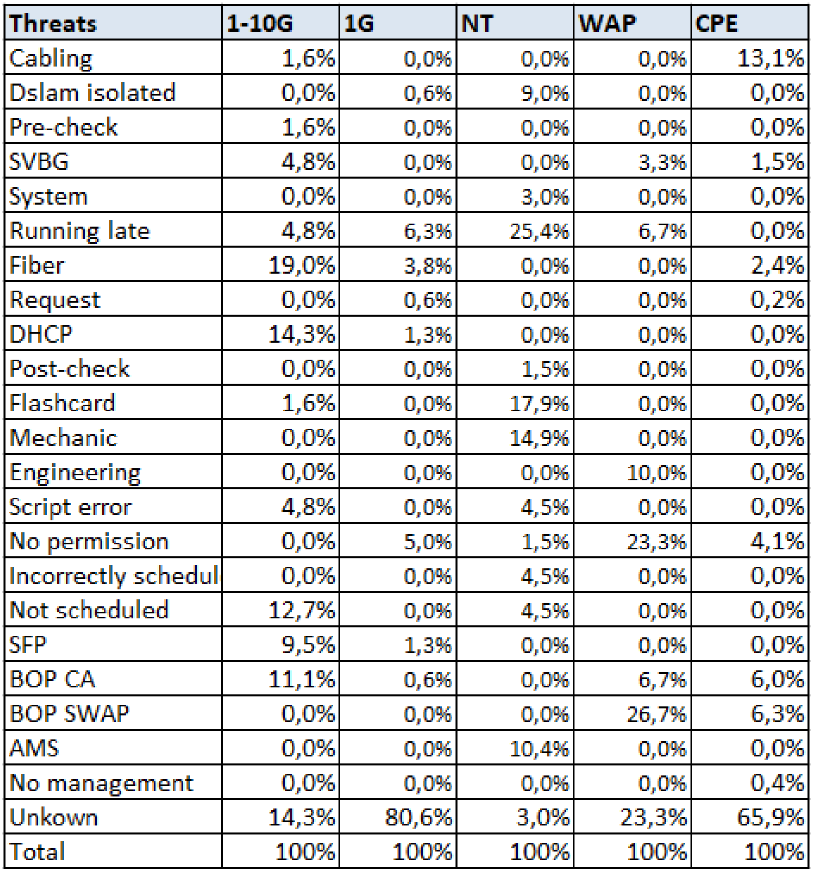


2018	Total	Succeeded (FTR)	Failed (nFTR)	Failed %	Succes %
1-10G	764	484	280	37%	63%
1G	3058	2605	453	15%	85%
NT	316	274	42	13%	87%
WAP	472	293	179	38%	62%

B.2 Percentages 2019

Table B.3 shows an overview of all the threats for each migration in 2019. The percentages for each threat represent their share in the total amount of failed changes.

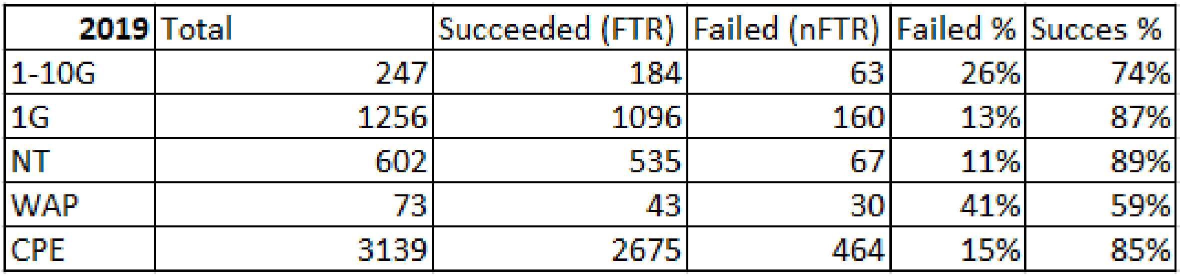
Table B.3: Threat percentages per change 2019



Threats	1-10G	1G	NT	WAP	CPE
Cabling	1,6%	0,0%	0,0%	0,0%	13,1%
Dslam isolated	0,0%	0,6%	9,0%	0,0%	0,0%
Pre-check	1,6%	0,0%	0,0%	0,0%	0,0%
SVBG	4,8%	0,0%	0,0%	3,3%	1,5%
System	0,0%	0,0%	3,0%	0,0%	0,0%
Running late	4,8%	6,3%	25,4%	6,7%	0,0%
Fiber	19,0%	3,8%	0,0%	0,0%	2,4%
Request	0,0%	0,6%	0,0%	0,0%	0,2%
DHCP	14,3%	1,3%	0,0%	0,0%	0,0%
Post-check	0,0%	0,0%	1,5%	0,0%	0,0%
Flashcard	1,6%	0,0%	17,9%	0,0%	0,0%
Mechanic	0,0%	0,0%	14,9%	0,0%	0,0%
Engineering	0,0%	0,0%	0,0%	10,0%	0,0%
Script error	4,8%	0,0%	4,5%	0,0%	0,0%
No permission	0,0%	5,0%	1,5%	23,3%	4,1%
Incorrectly schedul	0,0%	0,0%	4,5%	0,0%	0,0%
Not scheduled	12,7%	0,0%	4,5%	0,0%	0,0%
SFP	9,5%	1,3%	0,0%	0,0%	0,0%
BOP CA	11,1%	0,6%	0,0%	6,7%	6,0%
BOP SWAP	0,0%	0,0%	0,0%	26,7%	6,3%
AMS	0,0%	0,0%	10,4%	0,0%	0,0%
No management	0,0%	0,0%	0,0%	0,0%	0,4%
Unkown	14,3%	80,6%	3,0%	23,3%	65,9%
Total	100%	100%	100%	100%	100%

Table B.4 shows the total results for five types of migration changes. Four of those changes also have had their results measured in 2018. The results are shown in real amounts aswell as in percentages.

Table B.4: Success and failures percentages 2019



2019	Total	Succeeded (FTR)	Failed (nFTR)	Failed %	Succes %
1-10G	247	184	63	26%	74%
1G	1256	1096	160	13%	87%
NT	602	535	67	11%	89%
WAP	73	43	30	41%	59%
CPE	3139	2675	464	15%	85%

Appendix C

Threat and consequences overview

In this appendix, for each type of migration, an overview is given of the importance of each threat and consequence on different scales. First a percentage is given that shows how often a threat has led to a failed migration. Then this is put in perspective by showing it next to the amount of successful migrations. The last chart shows how often a failed migration has led to a certain consequence and how many migrations were successful.

C.1 1-10G

C.1.1 Threats percentages failed migrations

The first thing that can be seen is that there are five main threats that make up almost 80% of the causes for a failed 1-10G migration. These are cabling, BOP CA, BOP, material and fiber. The other threats play a lesser role, as they only happen sporadically.

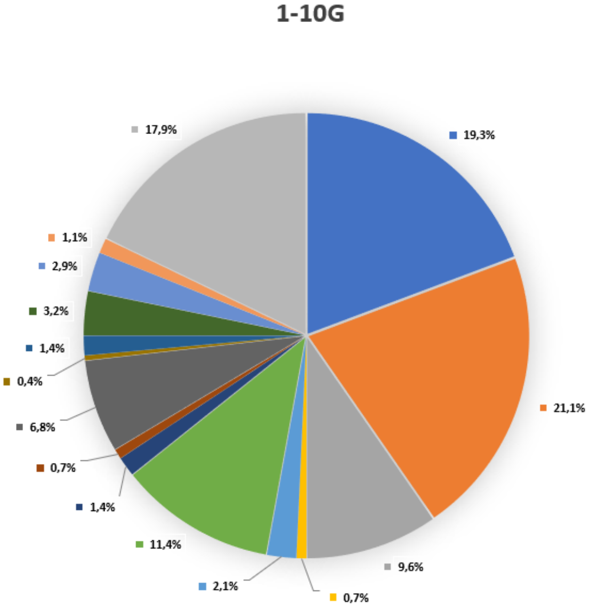


Figure C.1: Importance per threat 1-10G migrations

C.1.2 Threat percentages all migrations

The success rate of the 1-10G migrations in 2018 was 63.4%, making the percentages of failures 36.6%. In this chart the 36.6 percent is split up in all its causes and is shown next to the success rate.

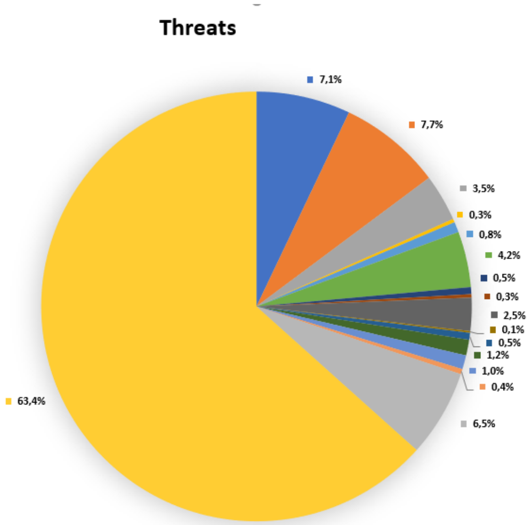


Figure C.2: Failed vs successful 1-10G migrations

C.1.3 Consequences percentages

The following chart shows how often failure has led certain consequences. Of the 36.6% of the failures, 35.5% ends up being rescheduled. Only 0.1% becomes a blue Be-Alert.

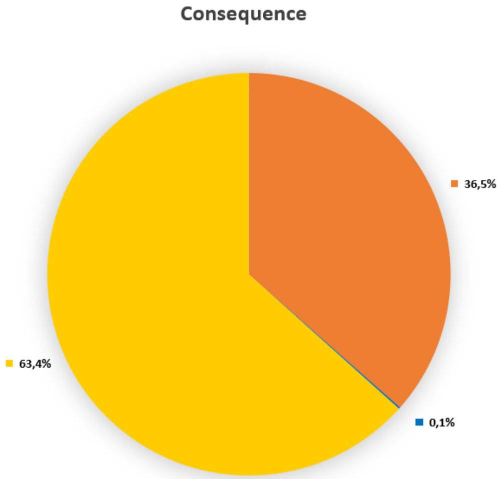


Figure C.3: Consequences of 1-10G migrations

C.2 1G

C.2.1 Threats percentages failed migrations

In the case of 1G migrations, there are two threats that play a big role. For a total of 41.2%, problems with Bop CA and mechanics are the leading cause for a 1G migration to fail in 2018. The other 68.8% is made up of 18 different threats in varying amounts, with cabling and fiber problems sticking out, just like with the 1-10G migrations.

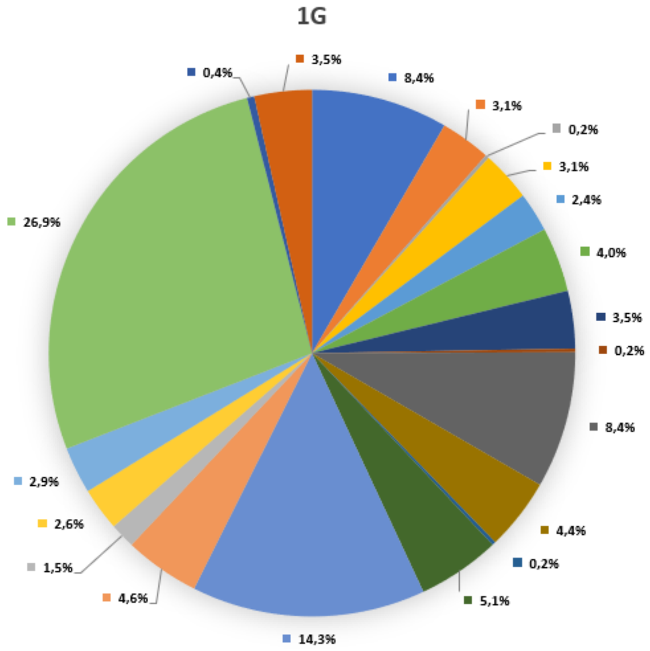


Figure C.4: Percentages per change

C.2.2 Threat percentages all migrations

The second chart shows that all in all, 1G migrations have only failed 14.81% of the time. Which means that improving on the two main threats will bring the success rate up past 90%.

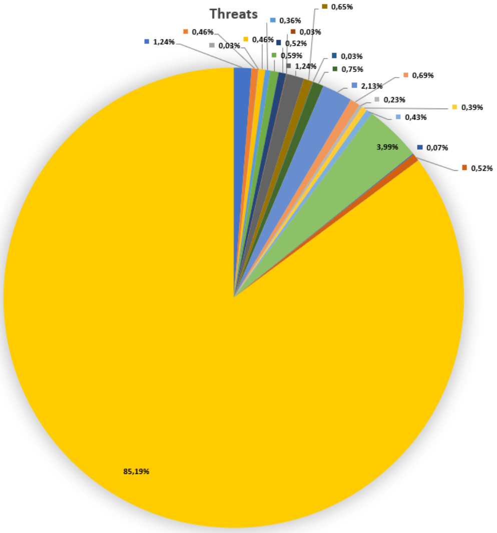


Figure C.5: Percentages per change

C.2.3 Consequences percentages

In the final chart the two consequences are shown. During 2018, 1G migration either ended up as a success (85.2%), or being rescheduled (14.8%). Combined with the knowledge that these migrations don't often become failures, it could be stated that 1G migrations are low risk and low impact.

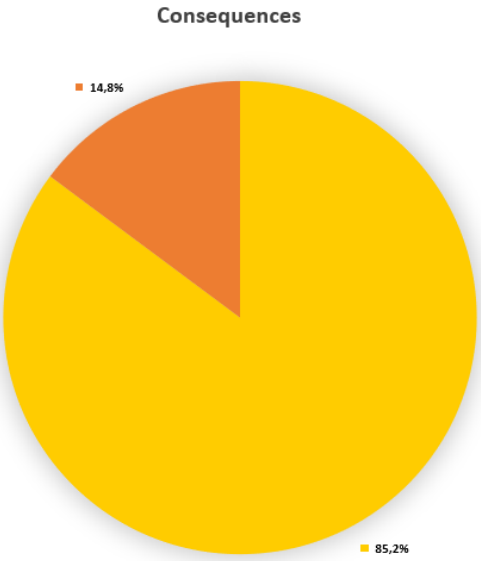


Figure C.6: Percentages per change

C.3 NT

C.3.1 Threats percentages failed migrations

NT migrations in 2018 that failed, failed because of four reasons. These can be seen in Figure C.7. This makes it easier to improve performance, as solving or improving on one of the three major causes of nFTR has a major impact on performance. The fourth cause, script error, is only 2.4% of the time the reason of nFTR and can be regarded as non recurring problem.

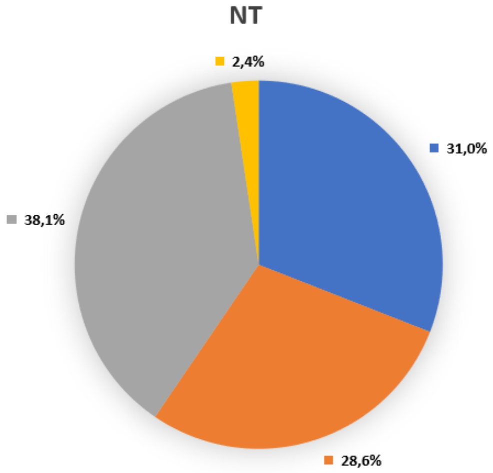


Figure C.7: Percentages per change

C.3.2 Threat percentages all migrations

The overall success rate is 86.71% for NT migrations in 2018. This means that while solving one of the three main threats (Problems with mechanics, migrations running late and flashcards) that account for around 30% of the failures each, will only improve the overall success rate with a maximum of 5%.

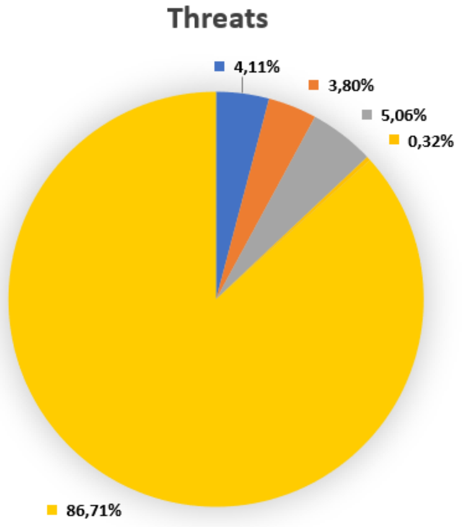


Figure C.8: Percentages per change

C.3.3 Consequences percentages

As there have been only two consequences in 2018 for NT migrations, reschedule and success, it can be said that this migration is not very riskful or impactfull. Especially combined with the knowledge that no Be-alerts have been created and that the overall success rate is 86.71%.

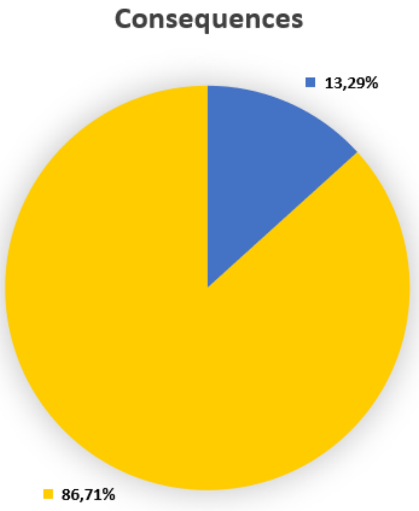


Figure C.9: Percentages per change

C.4 WAP

C.4.1 Threats percentages failed migrations

Looking at Figure C.10, there are three main causes for failure, four minor causes and a couple of sporadic causes. The three main causes account for approximately 60% of the failed migrations. The minor causes take almost 32% for their account. This means a broad focus is necessary to bring the nFTR percentage down.

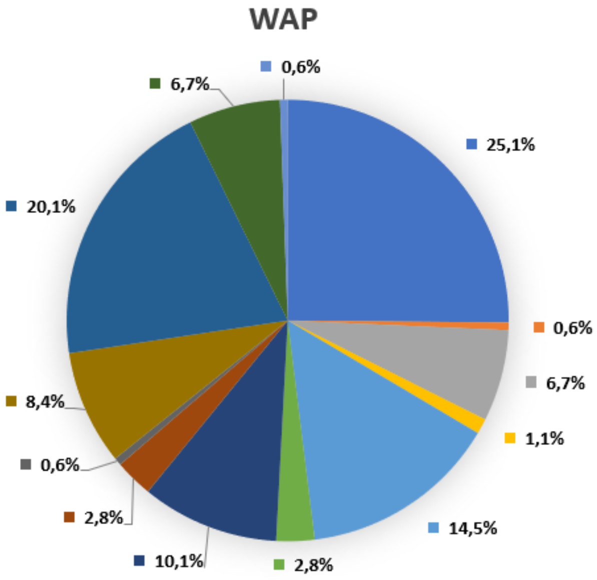


Figure C.10: Percentages per change

C.4.2 Threat percentages all migrations

Figure C.11 shows that WAP migrations were 62.1% successful against 37.97% unsuccessful in 2018. Improving on the three main causes for nFTR would push the success rate up to around 80%.

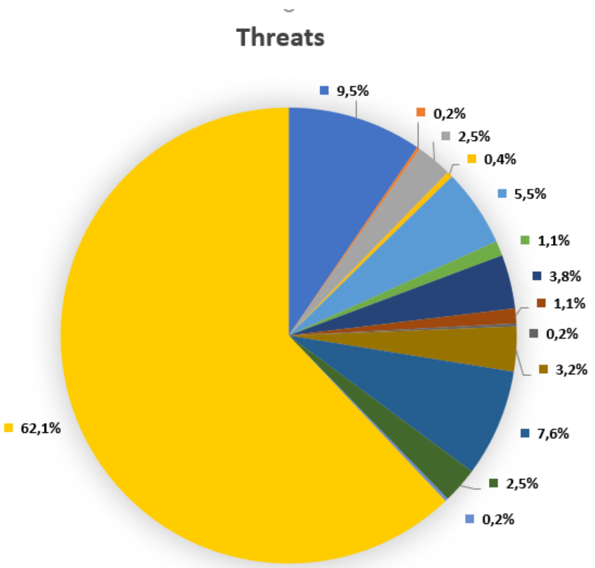


Figure C.11: Percentages per change

C.4.3 Consequences percentages

Looking at the consequences, one can see that the WAP migrations were the cause of one blue Be-Alert (0.2%). The rest of the failed migrations (37.5%) ended up being rescheduled without further consequences. There is still much improvement necessary, making this a more riskful and influential migration type.

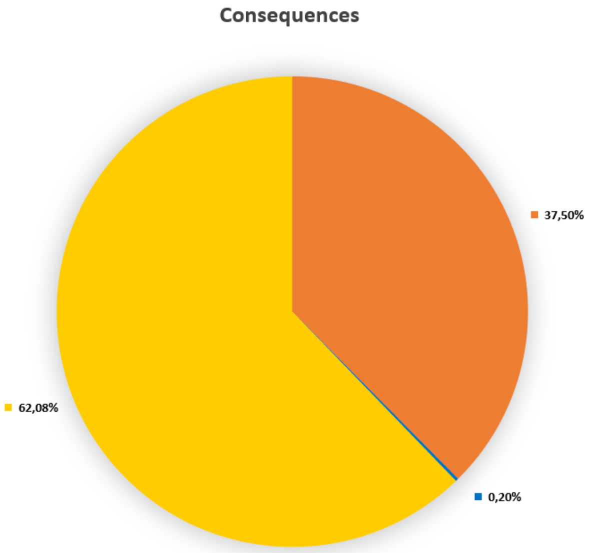


Figure C.12: Percentages per change

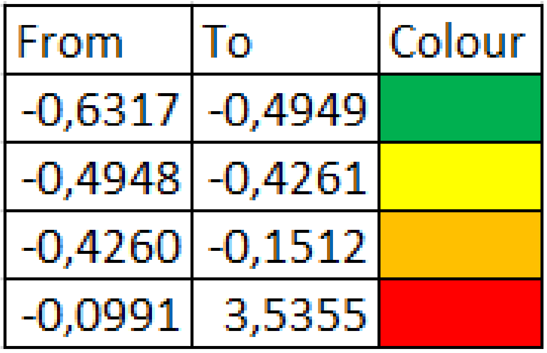
Appendix D

Risk rating colours

D.1 Colour calculation

In order to determine what ratings get what colour, a colour scheme is created. This is done by taking all the results of the standardisation and filtering out the unique values. From a total of 200 values, a list of 107 unique values remain. Having the risk rating measured on a four colour scale, means each colour represent a 25th percentile of the unique values. Dividing 107 by four results in 26,75, This means that each colour has 26 values. The last three values are added to the red colour for it to contain a bit more than a 25th percentile. The results can be seen in Table D.1.

Table D.1: Colour scheme



From	To	Colour
-0,6317	-0,4949	🟩
-0,4948	-0,4261	🟨
-0,4260	-0,1512	🟧
-0,0991	3,5355	🟥

Different approaches were possible to determine the most logical colour scheme. Starting with the amount of colours used to communicate different results. The choice to use four colours instead of three is because the goal of using this model is to increase insight in risk ratings. By only using three colours to represent low, medium and high risk, some of the subtlety of risk and impact ratings is lost. The differences between low risk and medium risk changes are sometimes not as outspoken and using an extra colour to define that difference can be useful when discussing change type classifications. Not having the tools and information to have such a discussion is one of the reasons for developing a more micro risk model.

Another approach was to use all the results do define the colour scheme, instead of using unique values only. The results using all the values instead of only the unique values, did not however, match with KPNs views on risk ratings. This is because recurring values, like the ones for costs, reputation and security just make those recurring values weigh heavier. This is not a good representation of the real situation and resulted in less logical results. Therefore the decision was made to use unique values, as described in the beginning of this Appendix.

D.2 Colours explained

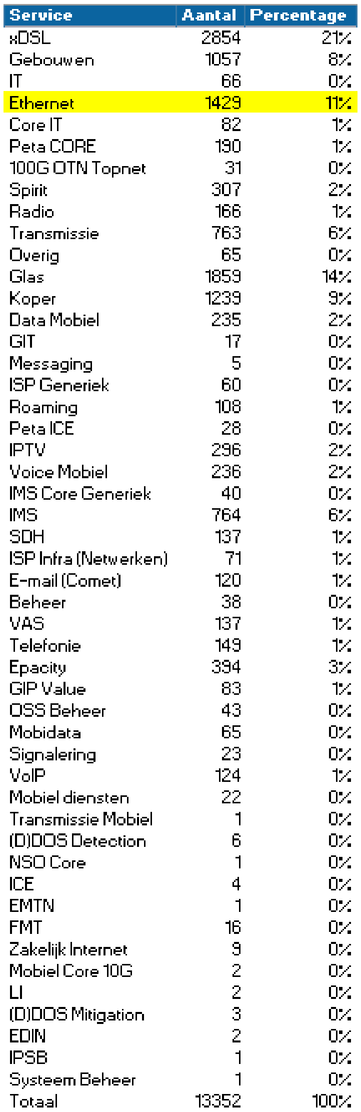
This section contains an explanation about what each colour means and how to best treat such a result.

- **Green - No to low risk:** Risk ratings that are coloured green are almost risk free. Change types rated as such should be the first options considered to be discussed when wanting to change change type classification in order to create more room during maintenance windows.
- **Yellow - Low to medium risk:** Ratings coloured yellow are considered more riskful. These change types need improvement in order for them to change their classification type to standard. In the case that there is not enough time to first improve them, a calculation needs to be made to see if it is worth taking them out of the maintenance windows. Based on the reduction of costs, room created during maintenance windows for other work and the increase in risk, a decision can be made.
- **Orange - Medium to high risk:** When a change type has a rating that is coloured orange, many improvements need to be made. These change types are riskful and need to be performed during maintenance windows. In no case is it acceptable to try and change the classification of these kind of change types. There might be a chance that in the long run improvements are made which positively influences the risk rating, but that will take time.
- **Red - High to unacceptable risk:** Change types rated red are very riskful and have a big impact. There is no chance that these change types will improve enough in a short time for them to become less riskful. Even in the long run it is probably better to not take the risk and keep performing them during maintenance windows.

Appendix E

Representativity

The table shown in Figure E.1 has been created from an export of the ticketing system used at KPN (ASTRID). This export contains all the tickets created in 2018 and the planned tickets in 2019 up to November. Filtering out all the tickets of 2019, as the data used in this research all originates from 2018, the table shown in Figure E.1 was created. The four migrations types used in this research fall in the domain 'Ethernet'. That is the highlighted value in the table. Comparing this value to the other values, leads to the conclusion that these kinds of changes are the third most common changes.



Service	Aantal	Percentage
xDSL	2854	21%
Gebouwen	1057	8%
IT	66	0%
Ethernet	1429	11%
Core IT	82	1%
Peta CORE	190	1%
100G OTN Topnet	31	0%
Spirit	307	2%
Radio	166	1%
Transmissie	763	6%
Overig	65	0%
Glas	1859	14%
Koper	1239	9%
Data Mobiel	235	2%
GIT	17	0%
Messaging	5	0%
ISP Generiek	60	0%
Roaming	108	1%
Peta ICE	28	0%
IPTV	296	2%
Voice Mobiel	236	2%
IMS Core Generiek	40	0%
IMS	764	6%
SDH	137	1%
ISP Infra (Netwerken)	71	1%
E-mail (Comet)	120	1%
Beheer	38	0%
VAS	137	1%
Telefonie	149	1%
Epacity	394	3%
GIP Value	83	1%
OSS Beheer	43	0%
Mobidata	65	0%
Signalering	23	0%
VoIP	124	1%
Mobiel diensten	22	0%
Transmissie Mobiel	1	0%
(D)DOS Detection	6	0%
NSO Core	1	0%
ICE	4	0%
EMTN	1	0%
FMT	16	0%
Zakelijk Internet	9	0%
Mobiel Core 10G	2	0%
LI	2	0%
(D)DOS Mitigation	3	0%
EDIN	2	0%
IPSB	1	0%
Systeem Beheer	1	0%
Totaal	13352	100%

Figure E.1: Representativity