Simo Poskiparta

Creating a basic tool for Disaster Recovery Planning

Helsinki Metropolia University of Applied Sciences

Master's Degree

Information Technology

Master's Thesis

20 March 2018

Metropolia

Author	Simo Poskiparta
Title	Creating a basic tool for Disaster Recovery Planning
Number of Pages	46 pages
Date	20 March 2018
Degree	Master' of Engineering
Degree Programme	Information Technology
Instructor(s)	Matti Keränen, Title: Instructor Ville Jääskeläinen, Title: Principal Lecturer

In this Master's Thesis a basic tool for Disaster Recovery Planning (DRP) was created. The goal was to create a tool which is easy to use and as self-explaining as possible so that administrators feel it convenient to use in their daily work.

First the basic concepts of contingency, continuity planning and disaster recovery are explained. Also their effect on the subject and their interactions, similarities and differences are explained in the theory section. For meeting the goal of this thesis, it is vital that the administrators' point of view was taken into account. Their suggestions on how the tool should be created and what it should contain were considered. This was done by creating an administrator questionnaire that gave an insight on how they feel about the subject.

In the second phase the tool was implemented using the selected software and features. After implementation the tool was tested with administrators. Test results and suggestions for future improvement that the test provided are included in the testing section. The testing situation proved that there is a need for this kind of guiding tool with pre fixed fields where administrator can fill in the data without thinking all the possibilities. Administrators that the tool was tested with were also contended with the features that were selected in the tool, and with the fact that they were given a chance to have an effect on the outcome of the tool in the planning phase and in the testing phase.

Although this tool for creating DRP was created for Finnish Meteorological Institute, the tool itself can be used in other organizations and companies as well as in any data center environment.

Keywords	Disaster Recovery Plan, DRP, Information Security, Contingency, Continuity Plan

Contents

List of Figures

List of Abbreviations

AD	Active Directory
BCP	Business Continuity Planning
BIA	Business Impact Analysis
CA	Criticality Assessment
DNS	Domain Name System
DRP	Disaster Recovery Planning. A plan for recovering system or service after an incident.
FMI	Finnish Meteorological Institute.
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation and Air Conditioning
ICT	Information and Communications Technology.
ISP	Internet Service Provider
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
MTD	Maximum Tolerable Downtime
RAID	Redundant Array of Independent Disk
RAM	Random Access Memory
RPO	Recovery Point Objective
RTO	Recovery Time Objective

SLA	Service Level Agreement
UPS	Uninterruptable Power Supply. Emergency power supply in case of power outages
VAHTI	Finnish Government Information Security Management Board
WAN	Wide Area Network
WRT	Work Recovery Time

1 Introduction

Information security as a whole has become one of the hottest topics in Information and Communication Technology (ICT) field today. It has grown from simple access control and identification mechanics to a huge, multi-domain sector that should be taken into account whenever new technologies and services are developed or existing technologies and solutions are used. International and national laws, directives and regulations are created for trying to ensure safety of data and services. On the other hand every piece of information ever created is going online thus making it vulnerable to different kind of unintentional breaching situations or hardware failures. Risk based approach in traditional finance business sector has grown to cover also ICT business services.

We rely on online services on a daily basis. People are so accustomed to think that their mobile phones, bank services, weather services and health services are working all the time, day and night. For example online shopping services should be running 24/7 so the companies could make maximum profit out of every minute. If services are not working, every second can be counted as a financial loss.

As the systems and services grow more complex, these kind of services need to be created in a way that there is resilience in the architecture of the ICT systems, and continuity in every part of them. This is called contingency planning. However, things do break no matter what, and when they do, there needs to be way to properly fix them as fast as possible without causing more damage while fixing them. ICT Systems rely on other systems and services, and it is crucial to know in which order they can be started to avoid further damage or downtime to services. This kind of thinking is contingency planning.This concept can be further divided in two parts in ICT field, continuity planning and Disaster Recovery Planning.

While continuity planning is responsible for trying to keep things running when something goes wrong, Disaster Recovery Plan (DRP) tries help to fix these problem at the same time. As an analogy, if electric power supply fails, critical infrastructure services such as hospitals are provided with electricity from other sources, for example with Uninterruptable Power Supply (UPS), while the electricians tries to fix the actual problem at the same time. Even though the goal seems to be the same, two different kinds of approaches are needed to ensure the safety of the electricity delivery.

Since DRP plans are often specific to certain systems, and more technical than contingency plans, creating them should be done by system administrators or persons with close liaison with them. Therefore, the research objective of this topic is to determine:

How to design an effective and a user friendly tool for Disaster Recovery Plan (DRP) that can be used by administrators every time they deploy new systems and services.

The word “tool” referred in the research objective above is to clarify that this thesis concentrates on a concrete product for Disaster Recovery Plans. The software or platform that was chosen for the implementation is discussed in the chapter 5.

1.1 Case Organization

This thesis produced a Disaster Recovery Plan tool for Finnish Meteorological Institute (FMI). The organization works under the Ministry of Transport and Communications as a research and service agency. According to FMI official website (FMI, 2018) “The main objective of the Finnish Meteorological Institute is to provide the Finnish nation with the best possible information about the atmosphere above and around Finland, for ensuring public safety relating to atmospheric and airborne hazards and for satisfying requirements for specialized meteorological products.

Finnish Meteorological Institute consist of five different centres and programmes, an administration unit and Director General’s Office, as shown in Figure 1.

Figure 1: FMI Organization chart (FMI 2018).

The main office is located in Kumpula, Helsinki, and other branch offices are located in Sodankylä, Rovaniemi and Kuopio. The overall number of staff working at the FMI was just over 700 people at the end of year 2017. As stated above, FMI works both in the research and in the operative service field. The Meteorological and Marine Research Programme, Climate Research Programme and Space and Earth Observation Centre work mainly on the research field. Weather, Sea and Climate Service Centre and Observing and Information Systems Centre work mainly on the operative and service field.

The ICT infrastructure is mainly operated by ICT and Data Production unit which resides inside Observing and Information Systems Centre. The main product of FMI is weather forecast and it is a product of a complex weather production system. At the same time

the whole production system needs to be really resilient and up and running all the time. So although the scope of this study is to create a basic tool for Disaster Recovery Planning for Finnish Meteorological Institute, it may well be used in similar complex environments and with smaller data center environments.

2 Method and Material

This section covers the research design of this thesis. At first, research approach is explained. Second, data collection both from administrative questionnaire and literature review are presented. The last subchapter introduces the research design and discusses why this approach was chosen.

2.1 Research Approach

The literature information used in this study is based on the existing knowledge on information security basic principles. However, creating a working and reliable Disaster Recovery Plan is not a simple single domain task, but needs rather an extensive knowledge on many different areas of information security. This study brings together these information security subdomains and combines them in a way that tries to make this complex administrative task easier to system administrators.

As mentioned before, this tool is designed for the administrators. Since the tool needs to be something that they find useful and easy to use, this study also uses questionnaire for administrators to ensure that their knowledge and opinions are also considered. The questionnaire is made to find out what the administrators want from the tool, and how it should be made to help them in their everyday tasks.

2.2 Data Collection and Analysis Methods

Literature Review

There is lots of system specific information available about Disaster Recovery Planning. However, the level of this information is often too intangible, or on the other end, too specific for a certain system. Since this study aims to create a working tool for the DRP,

all the information needs to be processed in a way that the goal is kept in mind. The main concepts of the disaster recovery are scrutinized and the differences and similarities between continuity planning and Disaster Recovery Planning are explained.

There are many existing best practices as well as Finnish national regulations that give guidance on what should be included in Disaster Recovery Plan. These are discussed more thoroughly in chapter 3.

Administrative Questionnaire

When we want to know what people think, and why he acts like he acts, it is wise to ask him that (Tuomi, J. – Sarajärvi, A. 2018: 84). Although every specialist knows that things do break, and systems need sometimes maintenance and even re-installing in a case of failure, this kind of a systematic approach to document the recovery instructions with critical services and systems makes fixing things faster and more reliable.

Administrators were given a short briefing about Disaster Recovery Planning, and why it is needed. Administrator questionnaire was based on a pre-fixed questionnaire list. There was also a place for free comments in the case they hold valuable information to the study and to bring up new ideas how this tool should be designed. Administrators that the questionnaire was sent are experts in their own field, and they maintain and develop the critical infrastructure of the FMI.

Planning Disaster Recovery Tool for Administrators

The tool was planned to meet the needs of the key elements of the disaster recovery that emerges from the literature review. The administrator questionnaire gave an insight on how the administrators feel about the subject and how they would like it to be addressed. The idea was to create a form with the chosen software that has fixed fields where administrators need to fill in the details about concerned appliance or service. The software that was chosen and why it was chosen will be discussed in the chapter 5. Choosing the key elements or features for the tool was done by outcome of the literature review and administrator questionnaire.

Implementation

Implementation of the tool was done based on the outcome of the literature survey and the questionnaire, and is described in detailed in chapter 6. Functionality testing is also discussed in the same chapter.

Evaluation

Since the research question is “How to make Disaster Recovery Planning easy for administrators” the tool was tested and evaluated with administrators after it was ready. The outcome and future improvement were gathered and discussed, however proposed future improvements are beyond the scope of this Master’s thesis.

2.3 Research Design

This study was conducted according to the research design seen on Figure 2 below.

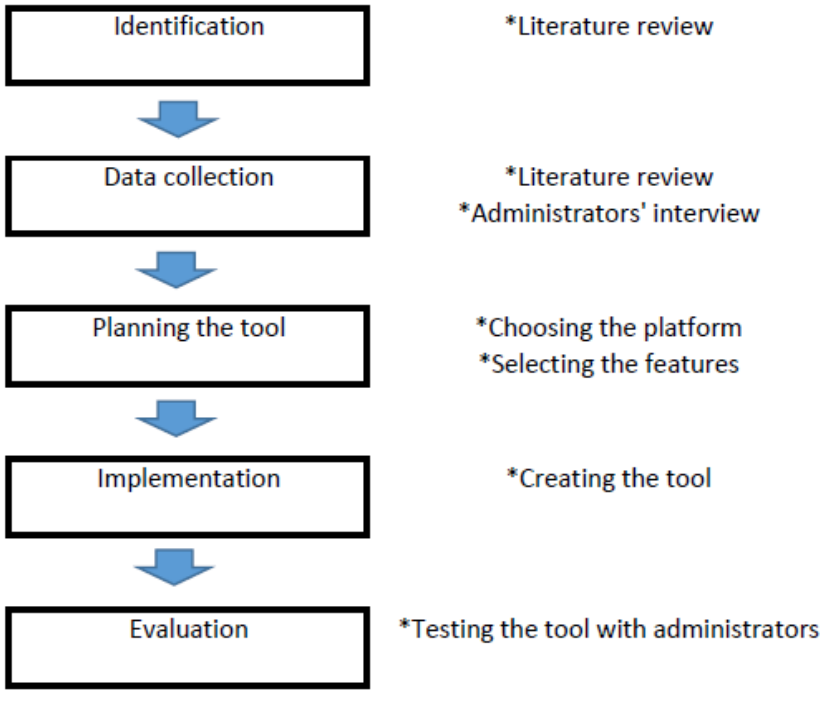

Figure 2: Research design of this study (modified from Teye 2011).

3 Business Continuity

Government Decree on information security in central government (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010 § 7) dictates that all governments agencies need to achieve the base level of security by 30.9.2013. The base level of information security includes procedures in exceptional situations (Requirements for ICT Contingency Planning (VAHTI, VM/1619/00.00.00/2012). This decree aims to ensure that the critical systems and services are continuously working even in exceptional situation.

The whole concept of business continuity, and Business Continuity Planning (BCP) is diverse and contains many sub-concepts. To make things more complicated, the concepts seem to differ from each other at least from some parts depending on the source. This chapter discusses the main concepts of business continuity, their similarities and differences. The key elements they both share are examined more closely.

3.1 Contingency Planning or Business Continuity Planning

As mentioned before, depending who you ask you may get a slightly different answer about the topics of business continuity. Many sources agree that BCP differs from the contingency planning in a manner that it is not ICT focused. However, nowadays almost all companies and organizations rely on their ICT to work, and things get more complicated when one tries to create a non-ICT oriented BCP. The contingency planning on the other hand is mainly ICT focused and consists of continuity planning and DRP. Kirvan, P – Lelii, S (2017) have managed to illustrate the relationship between BCP and DRP while leaving continuity planning out of the picture. The Figure 3 can be seen below:

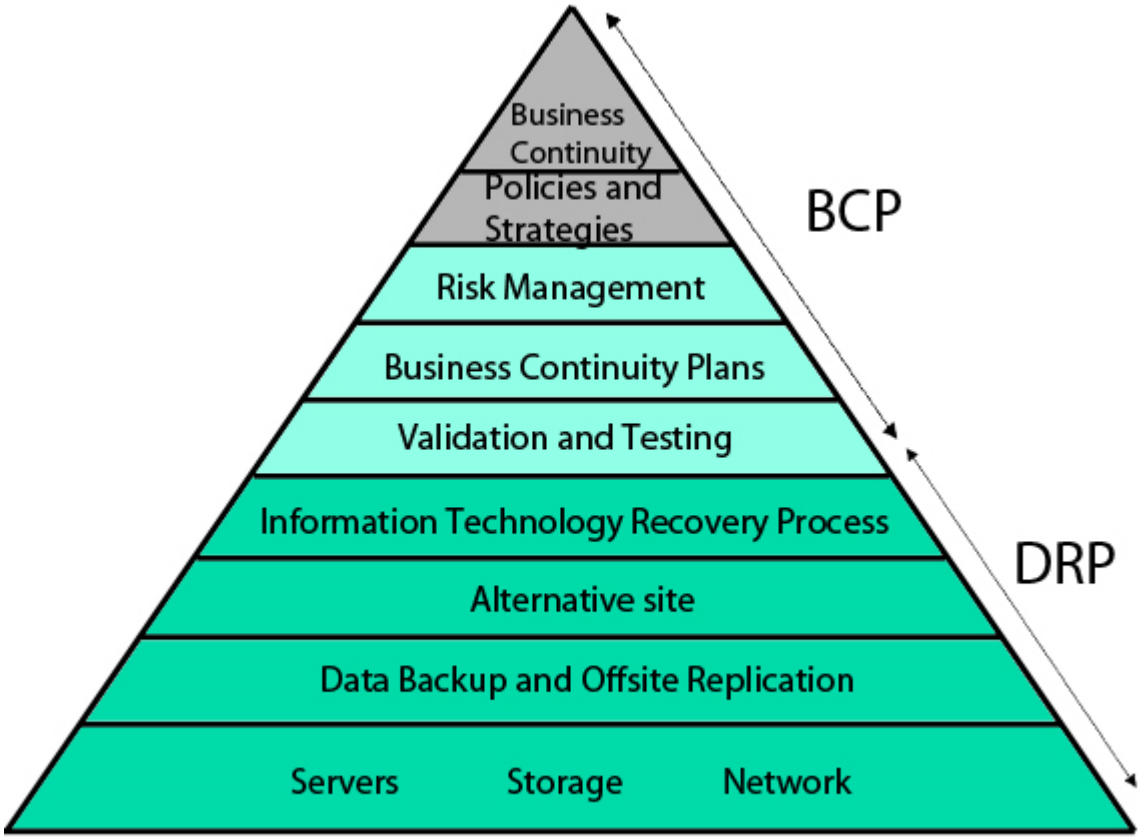

Figure 3: BCP and DRP relations (based on Kirvan, P – Lelii, S 2017)

As can be seen in the picture above, the base of the pyramid consists of the main infrastructure even though under which another level could be drawn where facilities and electricity would be pictured. The top of the pyramid consist of business continuity, policies and strategies and risk management. As can be seen, BCP and continuity planning are mixed together in this picture.

According to Harris (2013) contingency planning may seem like a normal incident handling. Contingency plans address how to deal with small incidents that do not qualify as disasters, as in power outages, server failures, a down communication link to the Internet, or corruption of software (Harris, 2013: 1277). On the other hand, Finnish Government Information Security Management Board discusses contingency planning as a top level topic that includes continuity planning and Disaster Recovery Planning.

Even though continuity planning and Disaster Recovery Planning take a different approach to achieve resiliency, both of them combined are needed in creating fully fault tolerant and disaster proof contingency plan. According to Requirements for ICT Contingency Planning (VAHTI, 2012) they can both be seen on the Figure 4 below.

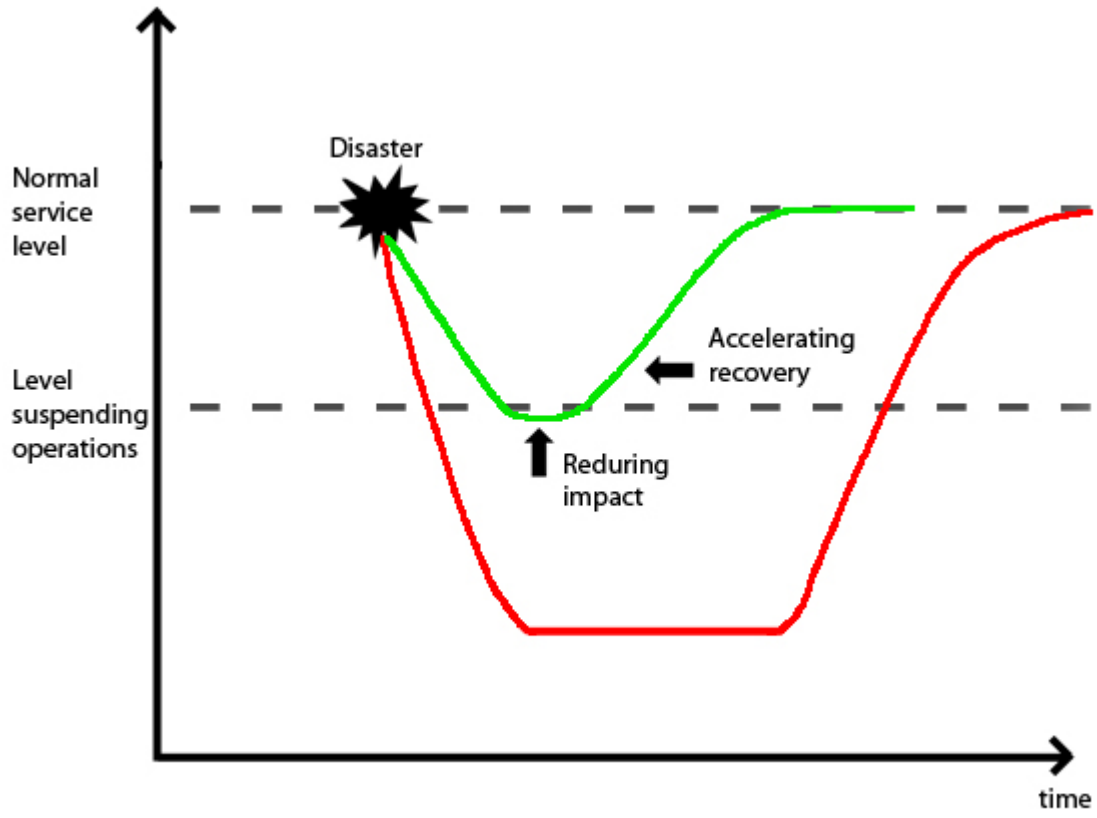

Figure 4: How continuity and Disaster Recovery Plans work together (based on VAHTI, 2012)

As can be seen in the picture, the main event is when the disaster strikes. The red line shows the process for returning to normal service level without continuity plan and Disaster Recovery Plan. The drop from the normal service level to a level where operations are suspended is steep and goes deep, and recovering back to the normal level takes long time. The green line represents an organization with both, continuity plan and Disaster Recovery Plans. As can be seen in the figure, the drop from the normal service level is more gently and less radical than on the red line. The reduced impact means working continuity planning. Also recovering from the suspended level of operations back

to the normal service level is faster. The accelerated recovery means working Disaster Recovery Planning.

To more clarify how these plans work together, Miller, L – Gregory, P. (2012: 337) give and great analogy of an anthill. Picture a working, busy anthill that is vulnerable to every kind of nature's forces imaginable. Since ants have been around for almost 100 million year, they need to have a very good contingency plan. When a little boy sees anthill, he goes and kicks it just to see how the ants react. At that point, both elements of contingency planning, continuity plans and Disaster Recovery Plans also activate.

According to continuity plan, half of the ants go and grab the eggs of the unhatched ants and larvae, and start to carry them to the predetermined, safe place. They also grab whatever food they can to make sure that their descendants have enough nutrition while the colony is evacuated. The other half of the ants are determined to follow the Disaster Recovery Plan. They start to rebuild and fix their anthill that has been partly or in worst case scenario completely destroyed. When the anthill is fixed, the evacuating colony can return back and continue on their everyday routines.

In a perfect case of continuity plan, ants would have food stored in their evacuation place and there would be some members of the colony responsible for housekeeping. However, this would add the upkeep for the whole colony. Such is the case also with ICT services. Fully running and duplicated "hot-site" would require double the money. In Disaster Recovery Plan, if the anthill (or data center) is destroyed beyond repair, all the usable and repairable equipment are scavenged and moved to another place, maybe to the evacuation spot and business (or life of the ants) continue there.

3.2 Continuity Planning

Continuity planning has traditionally meant duplication of ICT systems. Whenever something breaks, duplicated machine is ready to work. This can be true in some cases, especially with physical appliances. However, system virtualization has changed the ICT field dramatically. In a modern datacenter the physical duplication of machines would take enormous amount of space and electricity, so the services are built on virtualized platform. In a complex ICT infrastructure environment such as in data center appliances

need to be taken care of. This includes maintenance of the machines in an agreed manner. This leads to the fact that one of the most important aspects of the continuity planning is service and maintenance contracts. Service contracts specify for e.g. when the organization can expect to get help when something goes wrong. This may include calling for technician on normal business days, 7am to 5pm, or with critical services 24/7 on call duty support. When buying services, along come the Service Level Agreements which tells the level the organization should be able to use services. This can state e.g. that the service is available 99.9% of the time. But there are also other things to be considered which are discussed below. Some appliances and hardware needs to be still multiplied, and also the human perspective and services with the stakeholders needs to be taken in account.

3.3 Disaster Recovery Planning

The goal of disaster recovery is to minimize the effects of a disaster or disruption (Harris 2013: 887). Disaster Recovery Plan (DRP) is a plan for the situation when something breaks or stops working. Although administrators typically have extensive knowledge on the systems they are working with, and are quite familiar with the normal failures that can happen, it is widely recommended to have those plans documented and available when needed. Creating a uniform and simple enough document for every critical system may also help finding single point of failures. It also helps administrators since they no longer need to remember every single technical detail by heart. In a hurry, mistakes tend to happen. And in the case the main person responsible for the broken system is on a vacation and the substitute person is handling the situation, it gives him certainty that everything is done in right order.

Well documented and trained practices are also a necessity for success in complex environments with lots of dependencies. One person simply cannot know all the appliances and services by heart, and know exactly how they have an impact on the other. Whilst the disaster recovery shares a lot of elements with the business continuity planning, next subchapter introduces couple of processes and concepts that are mainly associated with the DRP plan. Also, the definition of a disaster is explained to clarify the broader view of the things that can, and eventually will happen.

3.4 Business Impact Analysis

Business Impact Analysis (BIA) is perhaps the key element in the Business Continuity Plan (BCP). The BIA highlights which resources (people, plant, ICT etc.) are important (Hotchkiss, 2010: 28). BIA focuses on company's or organization's critical business elements, and how the interruptions in those may or will disrupt the business itself. The BIA approach is very risk management based, and its goal is to achieve an acceptable risk level. In most cases in ICT, systems and services need other systems and services thus creating a complex network of dependencies. However, the BIA tries to find out the core business critical systems and services, usually by financial point of view. For example, if company's website or sales systems are down, this will directly affect to the money coming in. The outcome of the BIA results in a criticality assessment, but also gives business owners a deeper insight of the underlying technical solutions and possible risks in those. Once these risks are given a financial value, risk mitigation and cost of the risk preventive actions are more explainable to the chairmen of the company.

Finnish Government Information Security Management Board (VAHTI) has published a BIA tool that can be downloaded from their website. This tool targets the Finnish Government's organizations that possibly do not identify themselves as business organizations in a traditional way. This BIA tool evaluates the services business criticality for example through the key elements of the information security, confidentiality, availability and integrity, do the problems in the services threat the health and lives of the citizen, what is the highest classification level of the information in the systems or service and is the organization able to perform from its statutory obligations if the service is down, just to name a few.

3.5 Criticality Assessment

Criticality Assessment (CA) is a process where all the business critical systems and assets are evaluated to find out the critical points of failures. This can be done in different ways, Business Impact Analysis being one of them. The main idea is to identify all the systems that are business critical and their continuity and recovery need to be considered as number one priority in anomaly situations. If the BIA is done right, it can be a powerful tool that can increase organizations maturity and give that desired push towards more risk based approach in the company's methods. On the other hand, on smaller

companies and organizations thorough BIA can be a very time consuming task. In these cases, critically assessment can be done by listing all the critical appliances and services. If administrators are well familiar with the systems they are administering and have a good insight on the services they provide, this can be very efficient way of doing criticality assessment.

Duplication and Clustering

It is quite common that critical ICT equipment such as core appliances, firewalls, Wide Area Network (WAN) telecommunication network lines, servers, databases etc. are duplicated, tripled (or so on) or clustered. Duplicated appliances are preferably located in different physical places, and are powered on by different power supply. In the case there is a power shortage, or even a fire, only one appliance is affected by them. The other can keep running and take care of the business.

Companies also want to ensure that their telecommunication network is up and running even if near located construction yard tend to dig up the main cables of one Internet Service Provider's (ISP's) cables. That's why multiple main lines are usually bought from different ISP's.

If information is located only on one physical hard drive, fault in that may lead to irreversible data loss if there is no backup. Even if there are backups, data restoration takes time and there is usually still a gap between the lost and the restored data. That's why it is good idea to have the data stored in a way that is resilient to single or even multiple disk faults. For example, Redundant Array of Independent Disk (RAID) is very fault tolerant and can survive from multiple disk faults without data loss if configured accordingly.

Knowledge Preservation

Critical ICT equipment are typically duplicated or clustered in some way. They have backup systems and plans. So it should be with the people working with them. The knowledge and skills on how to administer and maintain complex systems need to be distributed and documented. There should be at least one substitute person for every critical task and job in case something happens to the person who is the main responsible. Up-to-date documentation and instructions are a requirement for knowledge preservation and duplication.

Uninterruptible Power Supply and Generators

Every data center and technical system needs power. Uninterruptible Power Supply is a way to ensure power to systems even the main supply line is cut out. Typical data center have multiple power feeding lines. Along that they should have generators to make sure that they can run autonomous at least for a while. While working UPS system adds reliability to business continuity in a power shortage, they may also create a critical point of failure and therefore must be considered as a part of the Disaster Recovery Planning.

Maintenance and Support Agreements

Technical appliances need regular maintenance in order to them to work as intended. Regular maintenance also decreases the spontaneous breaks of machines. But when accidents or surprising breakdowns happen, the maintenance personnel should be contacted without delay. This means that the support agreements needs to be taken seriously and especially with critical infrastructure and services the delay between breakdown and repair should be as short as possible. Maintenance and support agreements work with both, the continuity plan and Disaster Recovery Plan. In a continuity point of view, appliances should work as planned. In a disaster recovery point of view, when they eventually do break, they need to be fixed in an appointed time frame. If maintenance or breakdown affects the availability of the specific service, the repair should be implemented and services should be up and running within Maximum Tolerable Downtime (MTD). Maximum tolerable downtime will be discussed more on the chapter 3.5.

Service Level Agreements

It is quite likely that all or at least some part of the computing and storage capacity have been bought from the national or the multi-national companies. These kind of solutions based on data centers have their own continuity plans according to electricity, cooling, clustering the machines and even plans how to keep reliable amount of staff working with them. When one buys services from them, in most cases it is not even possible to have an influence on how they plan their continuity. Agreements, especially Service Level Agreements (SLA's) have become more significant since they are almost the only thing that one can rely on when buying services from the other party. SLA's usually define the availability of the service that can be expressed with percentage, traditionally with so called "nines". E.g. three nines would mean that the system should be running 99.9% of

the time, leaving the system down for 8 hours, 45minutes and 57 seconds on a yearly basis. Uptime of five nines, 99.999% can be down only 5 minutes and 15.6 seconds a year.

Virtualization

Basic virtualization enables single hardware equipment to run multiple operating system environments simultaneously, greatly enhancing processing power utilization, among other benefits (Harris 2013: 355). These other benefits include e.g. resource sharing, load balancing and bringing up virtual appliances from previously saved operating system images, so called snapshots.

Virtual environment consists of virtual machines and hypervisor that controls them. Virtual machines do not directly access the hardware such as processors, Random Access Memory (RAM) or storage resources. They communicate with a hypervisor that manages the resources. Without a hypervisor, more than one operating system from multiple virtual machines would want simultaneous control of the hardware, which would result in chaos (Portnoy, 2016: 22) Modern virtualization techniques add resilience to both, continuity planning and Disaster Recovery Planning. If a virtualized appliance such as server needs more RAM or processing power, hypervisor can automatically allocate more resources to it from the underlying shared hardware. Or if operating system of a virtual server gets infected with a ransomware, administrator can delete that virtual instance and start another one from the previously taken snapshot.

In the case where one hypervisor runs on a single hardware equipment, the hypervisor itself can become a single point of failure. To overcome that, hypervisors can be multiplied or clustered. If one hypervisor stops working, the other one can continue to manage the virtual machines.

Recovery Sites

Recovery sites are a possibility to increase the organizations chances to continue business when the organization’s headquarters is unavailable. The reason of the unavailability can be intentional, e.g. renovation of the building. However, if the reason is unpredictable such as fire or earthquake, the business can suffer a disastrous impaction, and

even drive the business come to an end. The organization can prevent this by having a backup site for their operation where they can move their staff to work in.

According to Harris (2013: 921) the recovery site can be cold, warm, hot, or mirrored site. The cold site is an empty, leased or rented space, where the organization can build the facilities and bring their equipment, data and staff when necessary. The term cold refers to the fact that there is only e.g. electrical wiring and air conditioning, the organization needs to build the necessary facilities and move everything they need in their business to the site and get the equipment running. This is the cheapest option of these sites and needs most time to get up and running.

The warm site is a leased or rented space where company can have some necessities such as Heating, Ventilation and Air Conditioning (HVAC) and basic infrastructure ready. The organization needs to bring their servers and computing equipment as well as data to the site in order to be able to continue business.

The hot site refers to rented or leased site which is ready for business when the staff and data comes in. There are office facilities ready and ICT equipment is up-to-date. The only thing usually missing is data, which needs to be retrieved from a backups. However, Wallace - Webber (2004: 217) defines a hot site “as an active duplicate of your live systems, with both systems and data ready to go at a moment’s notice” so there is clearly a difference between these two definitions.

The most expensive recovery site is a mirrored site, owned by a company. Both Wallace - Webber (2004: 217) and Harris (2013: 925) agree that the mirrored or redundant site is an exact duplicate of the main site and is the quickest way to get business up and running.

Whether the company or organization needs one of these, or any of these depends on business field and criticality of the services they are working with. If the organization is part of government, or their services are otherwise critical e.g. healthcare services, they should have at least some kind of plan how they can continue or move their business elsewhere if the main site is unavailable. In small businesses, consisting of couple of employees and laptops, the adequate plan could be renting an office from a business park.

Training

Even the organization would have a thorough plans for their business continuity or in case of disasters, these are still only plans if they are not gone through and trained with the staff. There are different kind of trainings from the simple and cheap exercises, to the comprehensive and expensive, all-staff drills in a true event simulating incidence. The simplest and the cheapest of the exercise is so-called tabletop exercise. This means that the key persons involved in the plans will go through the plans, reading them and updating them if necessary. This can be done fast, and without business interruptions. The most comprehensive and thorough trainings are so-called cut-off trainings where all the staff are included and possible simulations are used to test the plans in a real life situations. This can include hiring actors to act as injured staff members, or fire brigade generating a smoke inside the office and evacuating the building. These kind of business interrupting trainings are the most expensive ones, and most likely will affect business in some way.

The more the organization trains their plans, the more likely they will be well prepared for a disastrous situation. The training should be sized and designed to fit the organization's needs, and there is also a lots of choices between these discussed types of trainings. The main thing is to find out if there are gaps or even contradictions in the plans, and these will most likely to be found in a training situation. Also, the regular training occasion is a good time to update the plans if necessary. More testing makes recovery personnel more familiar with recovery procedures, making a smooth and successful recovery more likely (Gregory, 2007: 236).

Defining a Disaster

According to Varghese (2002, 28-47), disasters can be categorized as natural and man-made disasters. Natural disasters are a cause of extreme weather phenomenon or geologic activity. According to Varghese (2002, 28-47) natural disasters include floods, hurricanes, tornadoes, earthquakes, volcanoes, wildland fires and thunderstorms and lightning. Man-made disasters are outcome of a human error. Varghese (2002, 28-47) list these as hazardous material, house and building fires, nuclear power plant emergency and terrorism.

However, disaster does not have to be as devastating as the ones listed above. Any accident - be it a natural or man-made, that affects running the business in a normal way can be listed as a disaster in the concept of Disaster Recovery Planning. Usually these kind of technologic disasters include appliance break, stealing or encrypting the data of the company, sabotage in data center or a rapidly spreading virus. These kind of smaller disasters are far more common than for example nuclear power plant emergencies, but they still need to be addressed in a way that the business disruption is as small as possible.

Disasters and Business

Disasters can have a catastrophic impact on businesses. In 2001 terrorist crashed the planes into the World Trade Center towers. In 2004 Indian Ocean tsunami had an enormous impact on the businesses. These kind of disasters can put an end to entire companies when their business premises and staff are wiped out. Smaller disasters, such as building fires can render some part of the business premises useless, but the company may have the plans on how to continue running business elsewhere during the reparation. Most of the companies or organizations rely on their ICT services that they need themselves or provide to customers. If critical service, e.g. online shopping service is down, customers may start to shop elsewhere. This means a loss of revenue. If the service is out of order for a long time, it may cause a loss of reputation for the service provider which costs even more in the long run.

Be it either a catastrophe insurance bought from insurance company, comprehensive disaster plan, or both of them, if the company wants to survive disasters it needs to address the situations where something unexpected happens.

System Dependencies

Every ICT equipment and system is depend on at least one thing, electricity. However, commonly the list is much longer consisting of network connections, Domain Name System (DNS) services, databases, routing services, servers etc. Understanding the dependencies and the underlying technique the system resides on, is the prerequisite for understanding how to fix things when they break. In every service, at least the key dependencies should be known. For example, a server needs electricity, software to run it, configuration files, network connection and so on. A web service may need data from

different sources or other services to work properly. The more complex the system or service is, the more dependent it could be from the other appliances or services. The Disaster Recovery Plan should at least have the main appliances and services listed from which the concerned relies on.

Data Backups and Off-Site Storage

Business critical data should always have backups. Backing up the data means that there is a another source of the data saved in some form, in case the original data gets corrupted or destroyed because of an incidence. The incidence can be as simple as fault in the data storage system or the administrator accidentally wiping the data. However, cyberattacks have become more frequent and organizations have to be prepared for them also. In a last few year the type of malware known as ransomware have spread widely becoming the most expensive type of information security incident. According to (Morgan, 2017), costs of the ransomware are predicted to exceed $5 billion globally in 2017. The ransomware is type of malware that breaches in to organizations ICT equipment, usually through email messages. When user opens the seemingly innocent message, such as invoice or monthly report, the ransomware program starts to encrypt the data on the user's computer or the network drives and USB drives the computer or the user has access to. After the encryption is done, the ransomware programs tells the user that the data has been encrypted, and the only way to get the data back is to pay the attackers a sum of money after which the ransomware attackers send the encryption key back to the user. The official advice is to not to pay the money, but to restore the data from the backups. On a global scale, paying the money to the attackers encourages them to keep on doing their criminal business.

Restoring the data from the backups is possible if organization has data backup plans and the backups are done in a frequent basis. Depending on the business criticality of the data, the backups can be done e.g. on a daily or weekly basis. The most critical data that should never get altered can be replicated and saved in a separate data storages and locations. A good practice is to have full data backups stored in a completely different geographical location, in a so called Off-Site Storage. According to Gregory (2007: 45) "What good are backups if the backup media are damaged by the same fire, flood, or earthquake that damaged the systems?"

If organization gets struck by a catastrophic disaster, such as destructive fire or natural disaster such as hurricane or flood, at least the data backups are safe and there is something the organization can start to build on.

Maximum Tolerable Downtime

The outage time that can be endured by a company is referred to as the Maximum Tolerable Downtime (MTD) (Harris, 2013: 909). MTD means the most amount of time that company can survive without the concerned service before it starts to affect business permanently. The concept of the MTD is illustrated in the Figure 5 below.

:

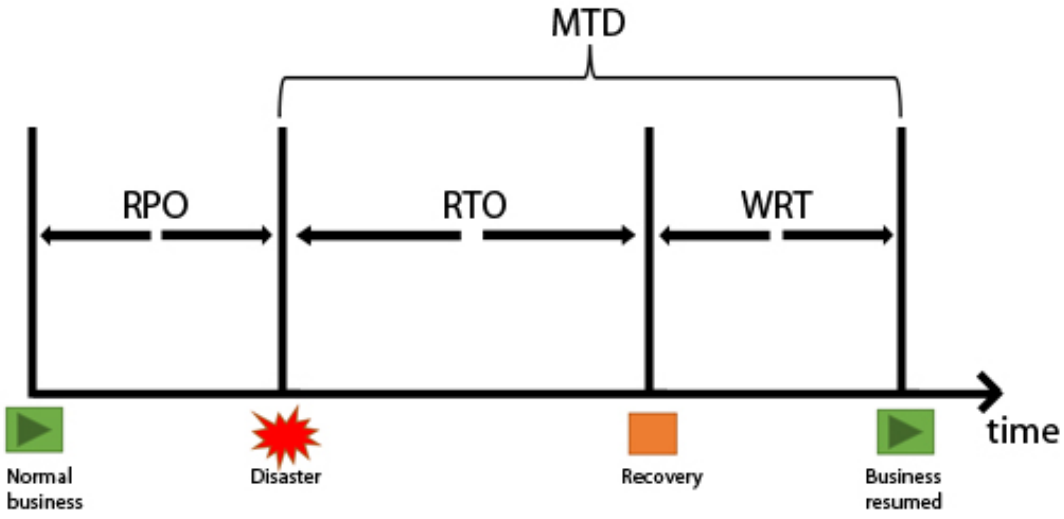

Figure 5: MTD explained (based on Zdrojewski, M 2013)

The figure shows four phases in the timeline on the x-axis. The phases are normal business, disaster, recovery and business resumed. The time between the normal business and disaster is called and Recovery Point Objective (RPO). The RPO denotes the accepted data loss measured in time. RPO value depends on the nature of the system. If changes to the data are done rarely, and the data is not critical, the value can be days rather than minutes. In critical systems RPO can be only minutes.

The time between the two phases, disaster and recovery is called Recovery Time Objective (RTO). Value of the RTO is the amount of time needed for getting the service

back online. Depending on the disaster, this can include everything from restarting the service to installing a new equipment and software with necessary configurations.

The time between two phases, recovery and business resumed is called Work Recovery Time (WRT). WRT usually consists of recovering the data from the backups and verifying that the system works as intended. The MTD value consists of RTO and WRT. If MTD value of the service is short, the continuity of the service and Disaster Recovery Plan should be of top priority. This can mean having a duplicated or clustered environment for the service or having a spare components or appliances ready in case of malfunction or break of the appliance. Overall, a good planning can greatly reduce the MTD value, whereas strict MTD value without plans and practice can difficult to achieve.

4 Administrator Questionnaire

This chapter focuses on the questionnaire that was sent to administrators. It discusses the questions that were chosen, and how the answers were processed. In this master's thesis questionnaire made with forms was efficient way to implement gathering the information. In a form questionnaire it is a typical to use open or half open questions. This questionnaire uses half open questions, and they are used to find out meaningful answers to the research question.

4.1 Target Group for Questionnaire

The target group consisted of ten administrators and experts who are working closely with the critical infrastructure on a daily basis. The area of expertise of these administrators covered weather product services, including firewalls, networks, computing, data storages and quality management just to name a few. In a qualitative research it is essentially important that the target group know about the topic of the research, hopefully as much as possible or they have experience about the topic (Tuomi, J. – Sarajärvi, A. 2018: 98)

This questionnaire uses so called elite sampling where the target group is chosen by the hypothesis that the chosen group will provide the best information for the research. According to Tuomi – Sarajärvi (2018: 99) sampling of six to eight persons is enough for the thesis.

4.2 Creating the Questionnaire

The questionnaire was done in Finnish, since it is the native language of the target group. This gave administrators a better chance to write the answers without the possible language problems becoming the barricade, hence improving the quality and usability of the answers. The questionnaire was implemented with Google Forms. Google Forms provides an easy platform to create a pre-fixed questionnaire and to send them to the target group. It also organizes the answers in a way that they are easy to compare. There was four compulsory questions and one voluntary question where administrators were given an opportunity to write freely on the topic.

4.3 Questions

At first, the topic of each question were thought. The topics were chosen in a way that they will give a good insight on how the administrators feel the disaster recovery tool should be implemented and what would be the main services and appliances they think should be the first ones to cover. Secondly, the questions were formatted in a way that they were suitable for open answers. Although the Disaster Recovery Plan principles are quite common, the final product or the way it will be accomplished varies widely depending on the company or organization's culture, needs and the field they are working with. Because of that qualitative questions, rather than quantitative ones, were chosen.

The topic on the questionnaire is "How to create a Disaster Recovery Plan in such a way that it fulfills its objectives and is also easy to use from an administrator's point of view".

Question one, "How necessary and important do you think is creating a Disaster Recovery Plan with an aid of some tool?"

The answers to this question gives insight about how the administrators think the importance of creating a tool for Disaster Recovery Planning.

Question two, "What services or appliances should be the primary concern when creating a Disaster Recovery Plan?"

The answers to this question will make the list of services or appliances that the Disaster Recovery Plan will be made and tested for with the developed tool. It also gives an insight on administrators thinking, which services and appliances are in fact the critical ones on their point of view.

Question three, "How the process of creating Disaster Recovery Plans could be made most effective?"

The answers to this question will help to understand how the process of making a Disaster Recovery Plan should be implemented in a way that it would be effective for administrators on their daily work. Although Disaster Recovery Planning is something that the administrators do on daily basis at some level, creating a particular process out of it should be made a simple and efficient task, rather than a burden.

Question four, "What kind of tool should be implemented for creating the Disaster Recovery Plan so it would be easy to use? Some particular platform, informal text, or something else?"

The answers to this question focuses on the ease of use of the developed tool. Although the question itself gives some alternatives to the answerer, these alternatives are included in the question to give administrators a suggestion that the tool can be made in a many ways, and the focus of this Master's thesis was to make this tool to be suitable for their needs.

Question five, "Do you have something else on your mind about creating a Disaster Recovery Plan?"

The answers to this questions will give administrators an opportunity to write freely on their thoughts about the topic. It can give good advices how the tool should be implemented, as well as out-of-the-box suggestions.

4.4 Question Answers

After a given time, seven out of ten administrator had given their answers. A reminder to answer the questionnaire were sent to the missing three, but at a time of writing, the answer percentage was 70%. As mentioned in a chapter 4.1 this is a sufficient sampling for this master's thesis.

Answers to question one

All of the administrators thought that making the Disaster Recovery Plan is either important or very important and necessary. Almost all of the answers stated the importance of a tool for doing the plans.

Answers to question two

Over half of the answers that was given brought up that the critical services and appliances should be the main concern when doing Disaster Recovery Plans. This included critical systems such as the core appliances, as well as services listed critical in criticality assessment that was done before. Operative weather production services were also mentioned in a two answers. Two answers mentioned that primary concern should be the customer services and services for public authorities.

Answers to question three

Answers to question three varied more than they did in the previous answers. One answer suggested that it should be included in a normal daily work. One answer though that it would be implemented through an existing management system, possibly with ISO 9001:2015 Quality Management System that the FMI's weather production services are already certified for. However, evolving processes take time and their goals and plans should be communicated clearly was also stated I the same answer. In a three answers a clear plan with a guiding and self-explaining fillable form would be the most efficient way.

Answers to question four

Almost all of the answers to the question four stated that the tool should be a fillable form with fixed features or topics that would require answers. All of these answers also suggested additional free-text area where administrators can write freely. One answer suggested that some kind of document management system should be used. One answer also suggested using software already in use at FMI, Atlassian Jira and Confluence. One answer pointed out that when the plan for a single appliance or service has been written down, someone should inspect it and approve it. Also one answer brought up the fact that if the tool itself is out-or-order or the systems it depends on are down, how the plans can be reached?

Answers to question five

The final question got three answers. One answer proposed that the DRP tool should include a field where it is required to write down who knows the appliance or service best, or who has initially installed it. One answer recommended that it should include a field for backup plans if some parts of the weather production systems are offline and something need to be done manually. Last answer welcomed the clear and easy process for creating DRP's.

4.5 Conclusions on the Questionnaire

It seemed that all of the administrators think that creating a Disaster Recovery Plan is important and it should be made in a harmonized way, maybe with some tool. A fillable form including fixed fields and free-text areas seemed to fit the needs. Critical services, be them either single appliances or more complex services should be the main concern when creating DRP's. The customers and services for public authorities need also to be taken into account although they are mainly already included in the critical services. The tool needs to be also self-explanatory at least in some level, and should guide the administrator to use it. Also combining the DRP process to the existing management systems would be efficient.

5 Planning Disaster Recovery Tool for Administrators

This chapter covers the planning of the tool. The chosen platform is introduced as well why it was chosen. Elements and features that the tool includes are discussed more closely and explanation why they add value to this tool are demonstrated.

5.1 Choosing the Platform

The chosen platform for this disaster recovery tool was Jira Software from Atlassian Company. Although the company itself states it a project and issue tracking software, many plugins and integrations it provides makes it a powerful tool for many purposes. At FMI the Jira Software is used as a project tool and issue tracking as well as service desk operations. The integration to the Atlassian Company's other product, Confluence Wiki is often seamless, and used together they may add value to possible future plans for this disaster recovery tool. Confluence Wiki itself is a document collaboration software, and is also widely used at FMI. This makes purchasing or learning a new software also unnecessary and answers to one of the results from the administrator questionnaire. The Figure 6 shows the basic installation and topology of Jira.

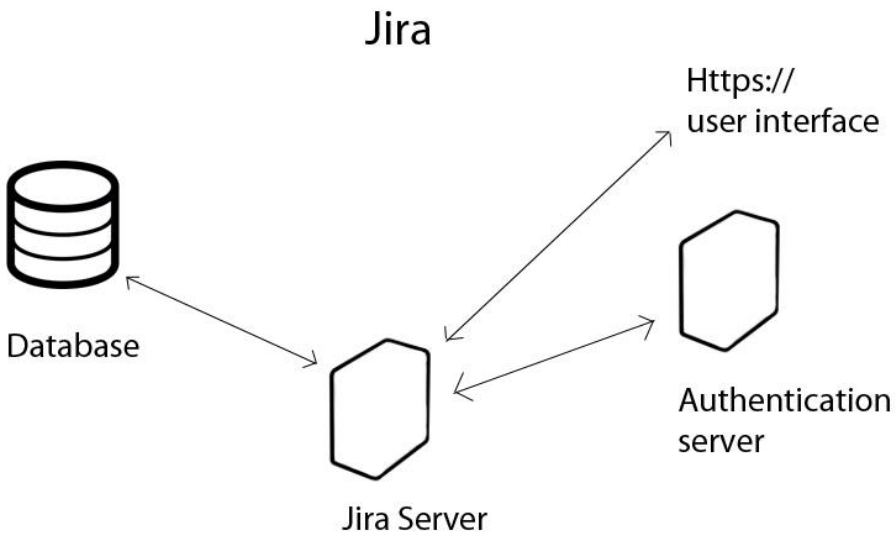

Figure 6: Jira installation.

Basic installation of Jira runs on a dedicated Jira server. User interacts the software with a web browser through a secure communication channel Hypertext Transfer Protocol Secure (HTTPS). The Jira server authenticates the user with Windows Active Directory (AD) authentication server using a Lightweight Directory Access Protocol (LDAP). The database Jira uses is PostgreSQL database, to which it communicates with a Java Database Connectivity (JDBC) driver.

5.2 Selecting the Features

The features or topics that were included in the tool are discussed in this subchapter. Argument why it was an important element of the DRP is also explained. Since the DRP was made to be suitable for both appliances and services, filling every field of the single DRP page is not a requirement. While filling some of the fields is compulsory, such as the name of the appliance or service, or the criticality grading, others were left to administrators themselves to decide if they could be left blank.

Name of the System or Service

The name of the system or service is a good first field for the DRP plan. It is also compulsory field since it is the obvious starting point e.g. when searching a specific system or a service.

Criticality Grading

Criticality grading is based on the criticality assessment that was already made when the creation of this tool was started. The criticality grading is four stepped, from number 1 to number 4. Appliances or services belonging to group 1 are the most critical, while number 4 represents appliances or services that are either not critical or are in the test phase and not yet operational. The grading system is explained more detailed below:

Criticality grade 1 - Top Priority: The system or service is critical for the weather production system and is needed for the services for the public authorities. The system or service needs to be working even in exceptional situations. MTD should be as small as possible, preferably seconds than minutes.

Criticality grade 2 – High Priority: The system or service is critical or of high priority for the weather production system and is needed for the services for the customers. MTD should be as small as possible, preferably minutes than hours.

Criticality grade 3 – Normal Priority: The system or service is needed for the customer products, but discontinuation in the services does not cause harm for the customers. MTD should be hours to one day.

Criticality grade 4 – Low Priority: The system or service is a support service for other services or is a system or service in a testing phase. No need for continuous service. MTD should be one to two days.

Backups of the System or Service

This field contains the backup plan of the system or the service. It can be e.g. a centralized backup system, a program that collects the backups, a local backup storage or something else depending on the system and its settings.

Configuration Files for the System or Service

This field is most important for network devices, such as switches, routers etc. Basic switches usually share at least some part of their configuration, and having them around when new devices needs to be installed or old ones are re-installed can really make a difference compared to the situation where these configurations would need to be copied from other devices or be written from the beginning.

Password Policy for the System or Service

This field is for checking if the appliance or the service needs to comply with the predefined password policy.

Most Important Dependencies of the System or Service

The field for the dependencies is possibly the most difficult one. Every system or service should include only the main dependencies it relies on, but since the dependency chain can go very deep, administrator should decide how many systems or services is enough.

Main Responsible Person

It is vital that every system or service has at least one name listed as the main responsible person that can be contacted in a case of system failure. All the critical services should have at least two to three persons listed in case the main responsible cannot be reached or is on a vacation.

Customer or Maintenance Support Contact

Almost all the appliances or systems have some kind of maintenance or support service. This field should list the email address and/or phone number of the service, and also the type of the service. The type of the service can vary, but the essential information is if the support is open from 9pm to 5pm, or is it open 24/7.

Documentation for the System or Service

This field contains the address or location for further documentation for the device if available. The documentation can be e.g. FMI Wiki-pages, or manufacturer's webpages.

Backup Systems or Spare Parts for the System or Service

If there is a backup system that can be used, it should be listed here. E.g. in a modern office malfunctioning of a copier machine is not a showstopper, other ones can be used as a substitute. In a modern ICT environments, some systems and services are also duplicated or clustered in case one appliance breaks.

Vital Data Source Dependencies

This field is for noting is the system or service reliant from some data or data source. This sounds like a previous field "dependencies" but the idea is to differentiate the idea of a more physical or static dependency from the data stream dependency. E.g. in a case of a database, the database and its contents can be restored from the backups. But if the function of the database is to gather data from other sources and that is the vital function of that database, those data streams or inputs should be listed here.

Other Comments

There should be always a place for free comments somewhere in any form. It is most likely that systems and services exist that in the time of writing were not known. These may hold information that should be documented somewhere. Or if there is a legacy system that is listed in the DRP plans that do not have to be fixed after it breaks, it can be written here. Or just in case something else comes in administrator's mind.

Attach File

Sometimes a picture is worth a thousand words. Specifically with network equipment, it could be sometimes a good practice to attach a picture file illustrating the network topology and where the system or appliance is located in it.

Plan Approved by

It is a good idea that someone else than the administrator itself goes through the plan. The more critical the system is, more important it is that the DRP plan consists of the ideas of main responsible administrators, not just one administrator. The approval for the plan could be written e.g. by their supervisor or a team leader.

Plan Revised or Updated (date):

ICT systems are usually under frequent changes. Since there are changes to the systems, there should also be changes to the plans. It is a good advice to go through the plans at least once a year and see if there are major changes. If there are no changes to the systems, or the plan is up to date, it is recommended to update the revised date. This also shows that the plans are revised periodically.

6 Implementing the Tool

This chapter describes the creation of the Jira form that administrators will be using when creating the DRP plans. The chapter goes through basic settings that are needed when creating fillable form with Jira. Settings and adjustments that are irrelevant for making this DRP form will not be discussed. Security and visibility of Jira form will be also discussed in the last subchapter.

6.1 Creating the Tool

At first, a new project is created using Jira with administrator rights. A new project is chosen so it is possible to adjust the project visibility and user rights. Jira create project options are shown in Figure 7 below.

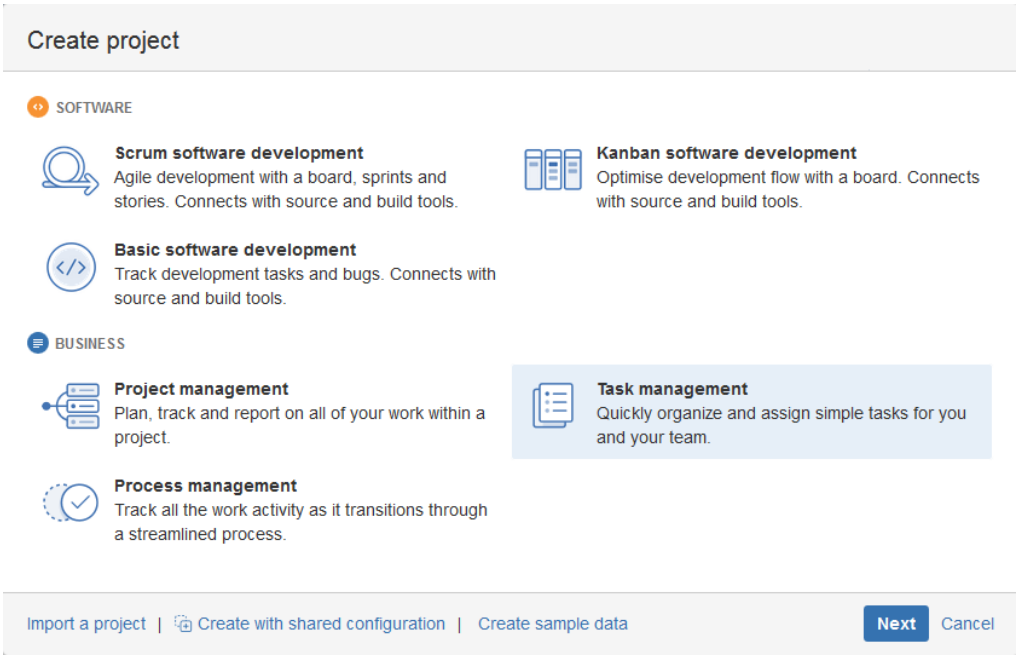

Figure 7: Creating a new project with Jira.

As mentioned in the previous chapter, Jira can be used in many ways, e.g. in project management and software development. When creating a fillable form, Task Management was chosen. The new project was given a name Disaster Recovery Plan. The key value is a tag that also uses running numbering, so DRP was chosen as an abbreviation.

This means that the first DRP plan that is made will have the identifier of DRP-1, the second DRP-2 and so on. At last the project lead name was chosen. The lead of the project is a role that can be used in the project settings, e.g. forwarding automatic emails to the project lead. A project administrator can make future changes to the project, and change the user rights and visibility of the project without having an administrator rights to Jira itself. These settings in the Task management screen can be seen in Figure 8 below.

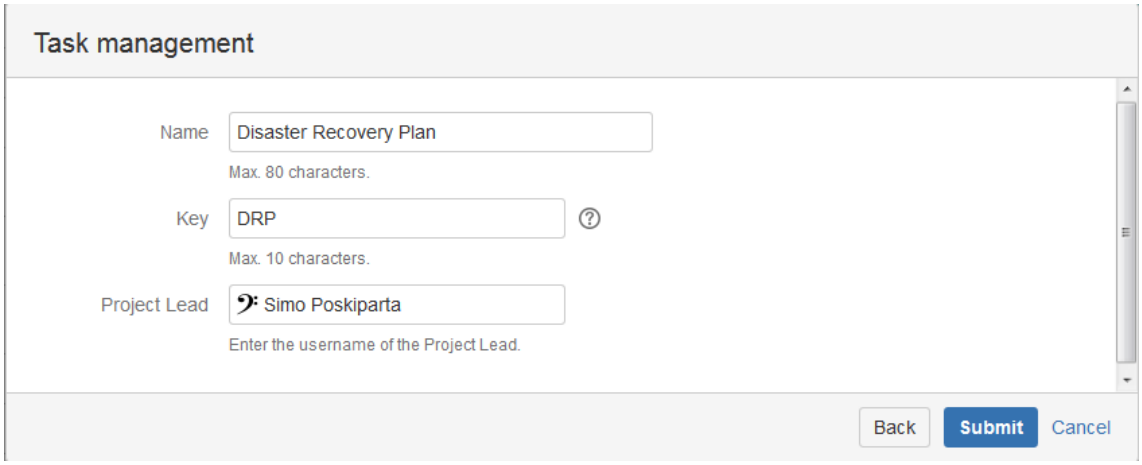

Figure 8: Jira Task management screen.

After submitting the information in Task management screen, a new project was created showing Project settings as shown in Figure 9 below.

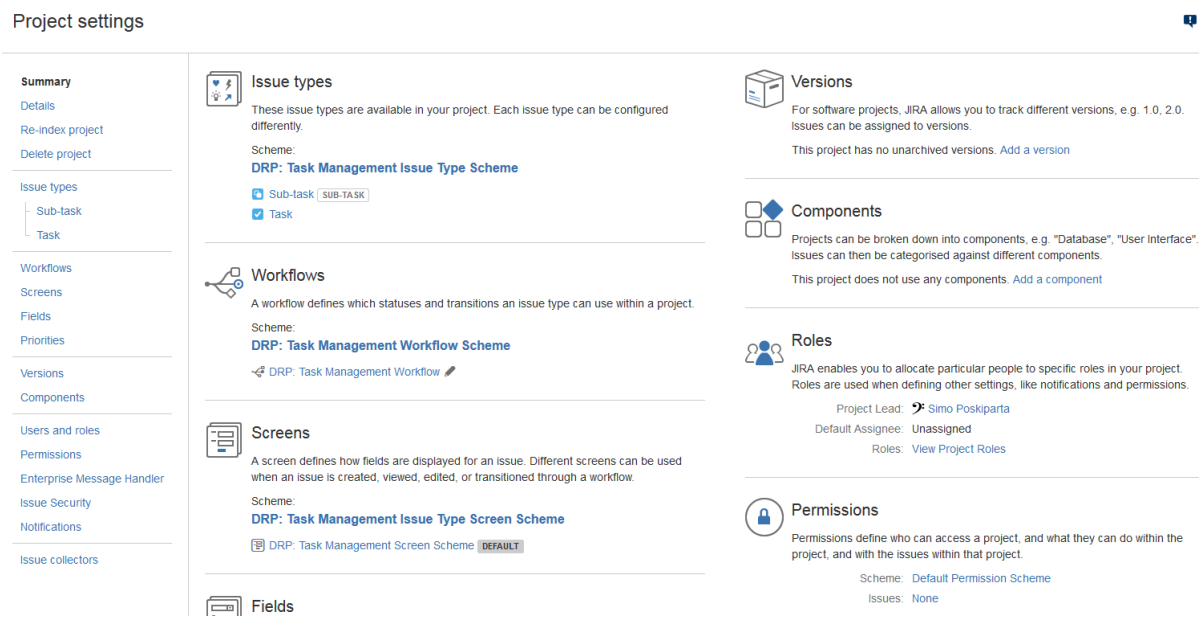

Figure 9: Jira Project Settings.

After the DRP project was created, custom fields were made to act as a text boxes where user can fill in the actual data. These fields were chosen from the features that were discussed in the chapter 5.2. There are many options for the custom fields, but in this case almost all of them were chosen to be multi-line text field, which enables the user to fill in more than 254 characters to one text field, which is a limitation when using single-line text field. In a criticality grading field, a select list from numbers one to four was chosen, since they are the only options that are used in that specific feature. Plan revised or updated field was chosen to be date picker field, which makes it more convenient for the user to fill in, since the date can be picked from a list, other than writing it.

Next, an issue collector for the project was created. The issue collector defines the basic functions of the form. Creating the issue collector is shown on Figure 10 below, and the settings that were chosen are explained after the figure.

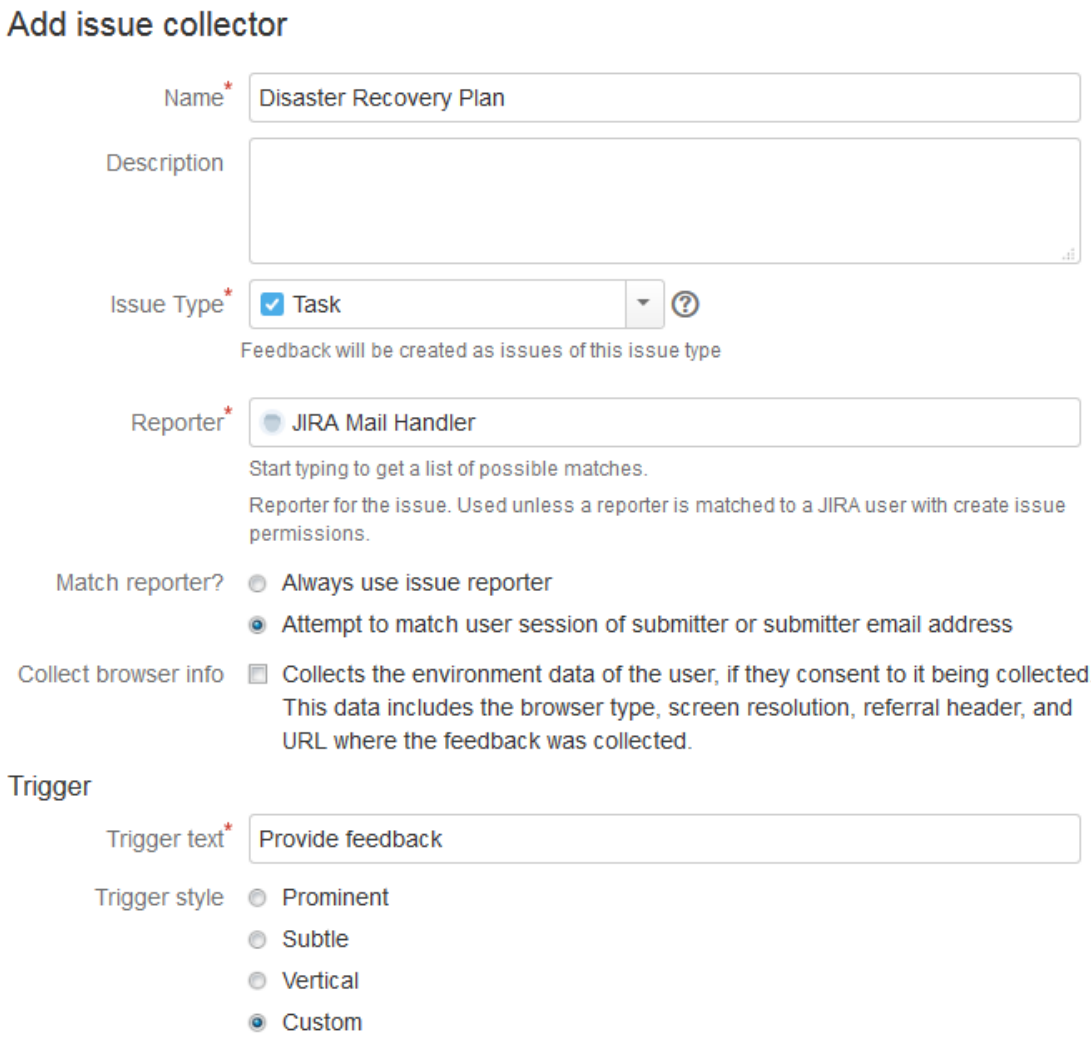

Figure 10: Creating the issue collector.

The name for the issue collector was chosen Disaster Recovery Plan. Issue type is “task” since a form was made using a basic task management. The reporter field was chosen JIRA mail handler. With a Jira mail handler and chosen setting “Attempt to match user session of submitter or submitter email address” the reporter is always the person who fills in the form if he/she has signed in to Jira. Without signing in, the person is asked to fill in his/her email address and the Jira Mail Handler tries to match the email address with its user database. If there is a match, a username corresponding the email address will be chosen as a reporter. Without a proper match, Jira Mail Handler will be chosen as a reporter.

Collect browser info was not chosen, since it is not needed to gather any browser data for statistical purposes. Last, the trigger option defines how and where the form will be embedded. The option was chosen custom since it enables embedding the form in any

web page using JavaScript. The custom fields that were discussed earlier can be seen in Figure 11 below.

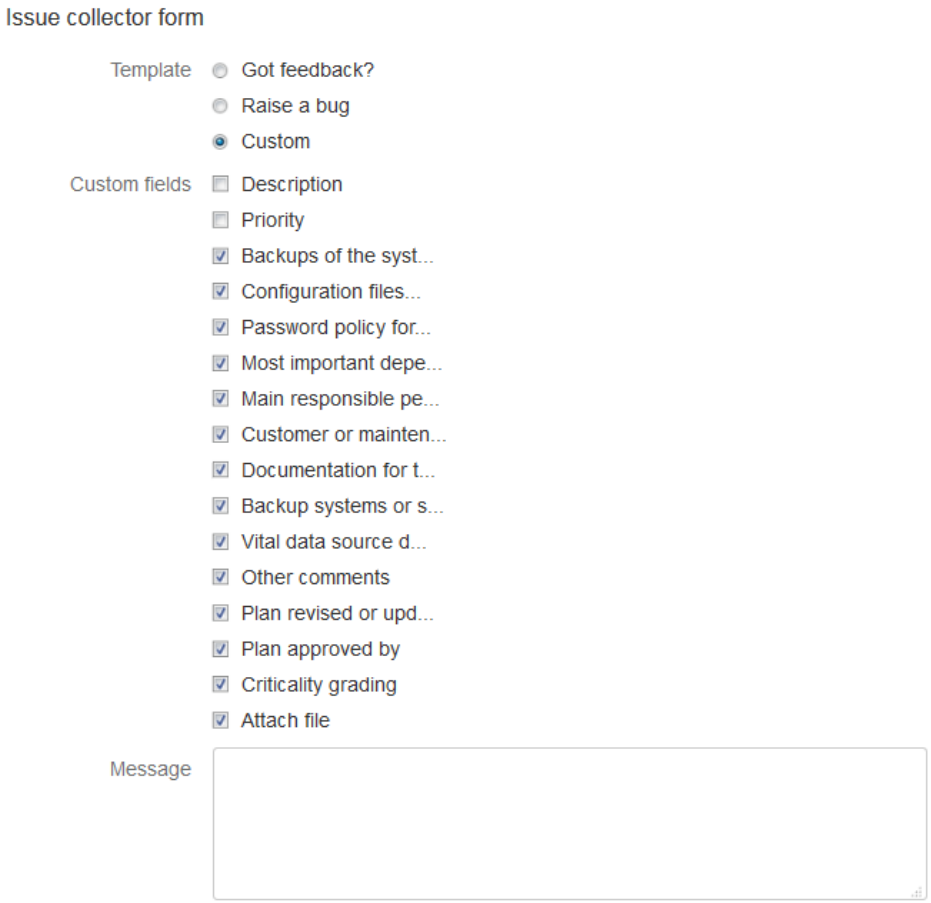

Figure 11: Issue collector form custom fields.

Issue collector form seen in Figure 11 above defines the fields that are used to collect the data for the DRP form. Template was chosen to be “custom” so it is possible to use the fields that were chosen before. As can be seen, there is no field for “Name of the system or service”. Since Jira automatically wants a field called “Summary”, the name of this automatic summary field was changed to “Name of the system or service” thus making the premade custom field unnecessary. Also some fields were left blank such as the description and priority fields that are default fields, but can be left unchecked since they are not used in this form. The Message field allows to create instructions to the administrators in the beginning of the form if necessary.

6.2 Finished Disaster Recovery Planning Form

The final DRP form that the administrators are able to fill can be seen on the Figures (12,13,14) below.

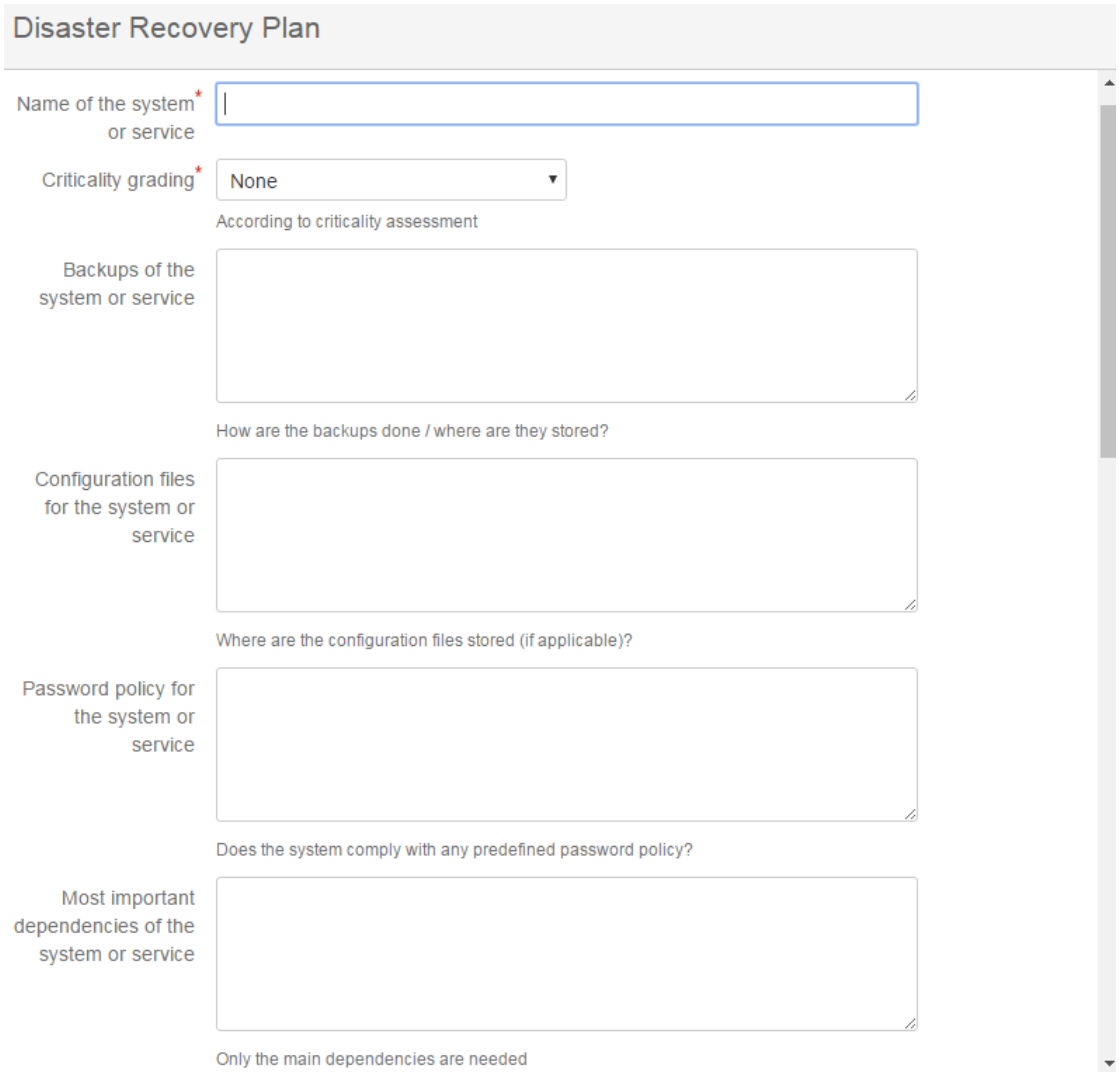

Figure 12: DRP plan form (1 of 3)

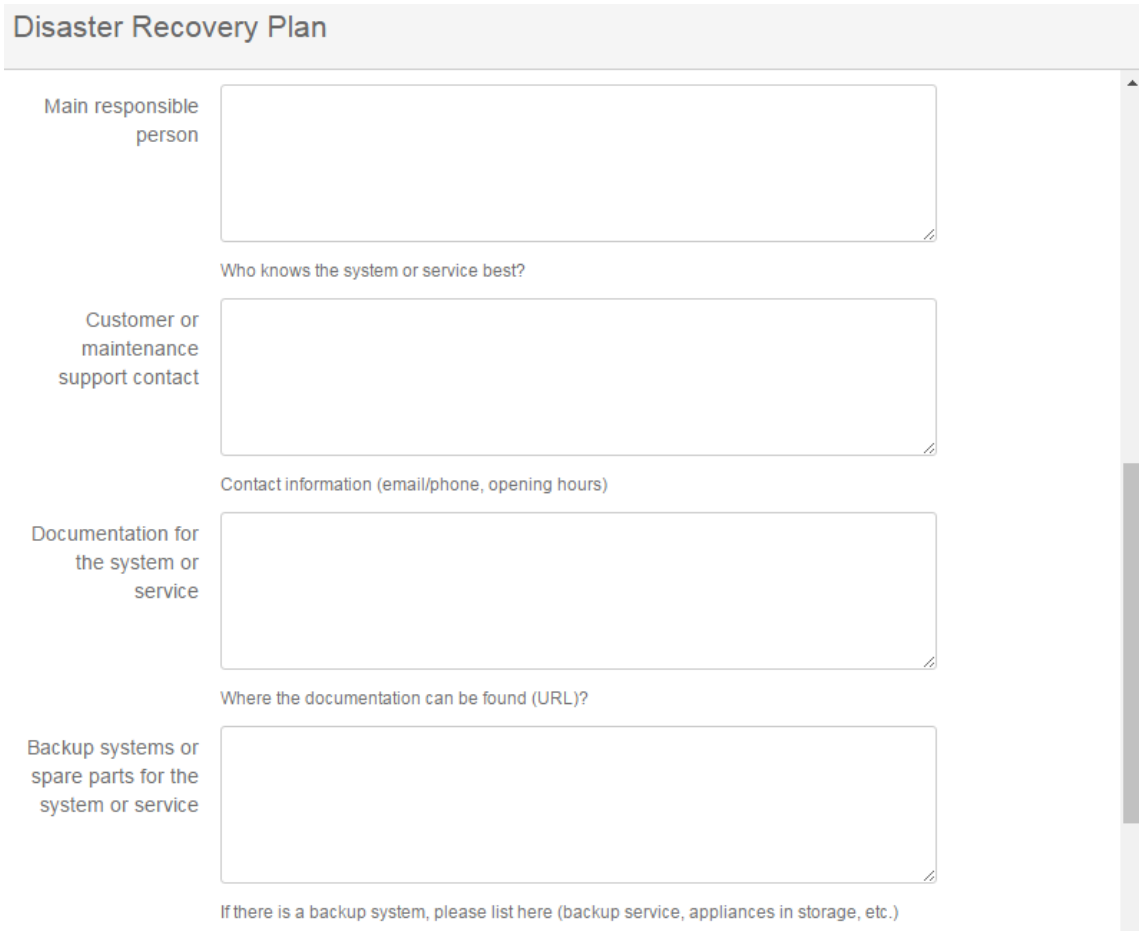

Figure 13: DRP plan form (2 of 3)

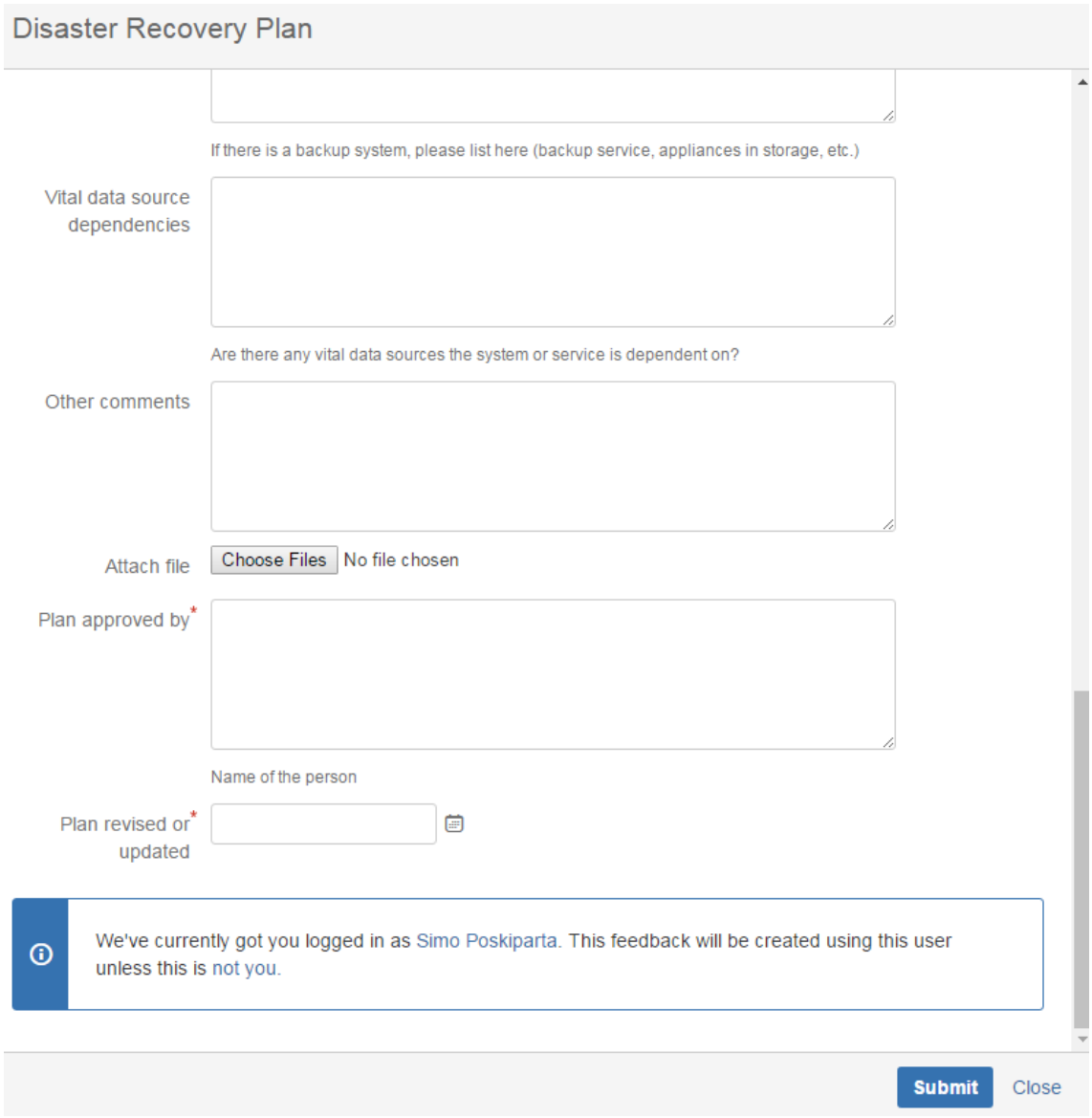

Figure 14: DRP plan form (3 of 3)

6.3 Security and Visibility of Disaster Recovery Planning Form

Since Disaster Recovery Plans are a vital piece of information for the organizations and often classified as confidential or secret because they contain detailed information on systems or services, it is important to protect them accordingly for any hostile actions or from persons that are not allowed to view them. Information security often uses multi-layered protection mechanisms that gives multiple security controls for the protected asset.

At FMI, Atlassian Jira software used to create this DRP planning tool is not visible to the Internet. The user willing to fill in the form needs to have user rights to the FMI network and know the address where the form is located. These protections give the first level of protection for DRP plans. At this DRP project the visibility of these plans were restricted to the persons that work in the unit that administers the ICT infrastructure of the FMI, ICT and Data Production unit. This further narrows down the number of the people who are able to see the actual DRP plans. If needed, the restrictions can be made even stricter, to the personal level so only the designated administrators can see certain plans. These restrictions and visibility settings can be changed by the project administrator or Jira administrator if needed. Jira itself does a log files that records all the changes to the permissions, so these changes leave a mark, and can be audited later if necessary.

As is with Jira software as well all the other software, there is a possibility for errors, data corruption, update bugs and service malfunctions. The database that contains all the data is backed up, and can be restored if necessary. With Jira export options, these DRP plans can be exported to a text format that is printable and can be stored in a safe just for a precaution in a case where Jira service itself is down and the plans stored in the database cannot be reached.

7 Testing the Tool with Administrators

This chapter discusses testing the DRP tool with administrators. The testing was implemented as a tabletop exercise with five administrators. The testing was made by filling in the form with two test subjects, a standard network switch and also with a web service. Administrator observations on filling in the forms are discussed in a system specific subchapter. The overall observations and future improvements are included in the subchapter 7.3.

7.1 Testing the Tool with an Example Appliance

At first the tool was tested with a standard appliance, a network switch. The test group was able to fill in almost all the fields without difficulties, except the “Vital data source dependencies” field. This was due the fact that although a network switch needs data from the core switch, it was chosen to be left blank. In this case “Backups of the system or service” and “Configuration files for the system or service” were the same because of the nature of the appliance and the software that is used to control and maintain it. The result of the DRP plan for this specific appliance can be seen in the Figure 15 below.

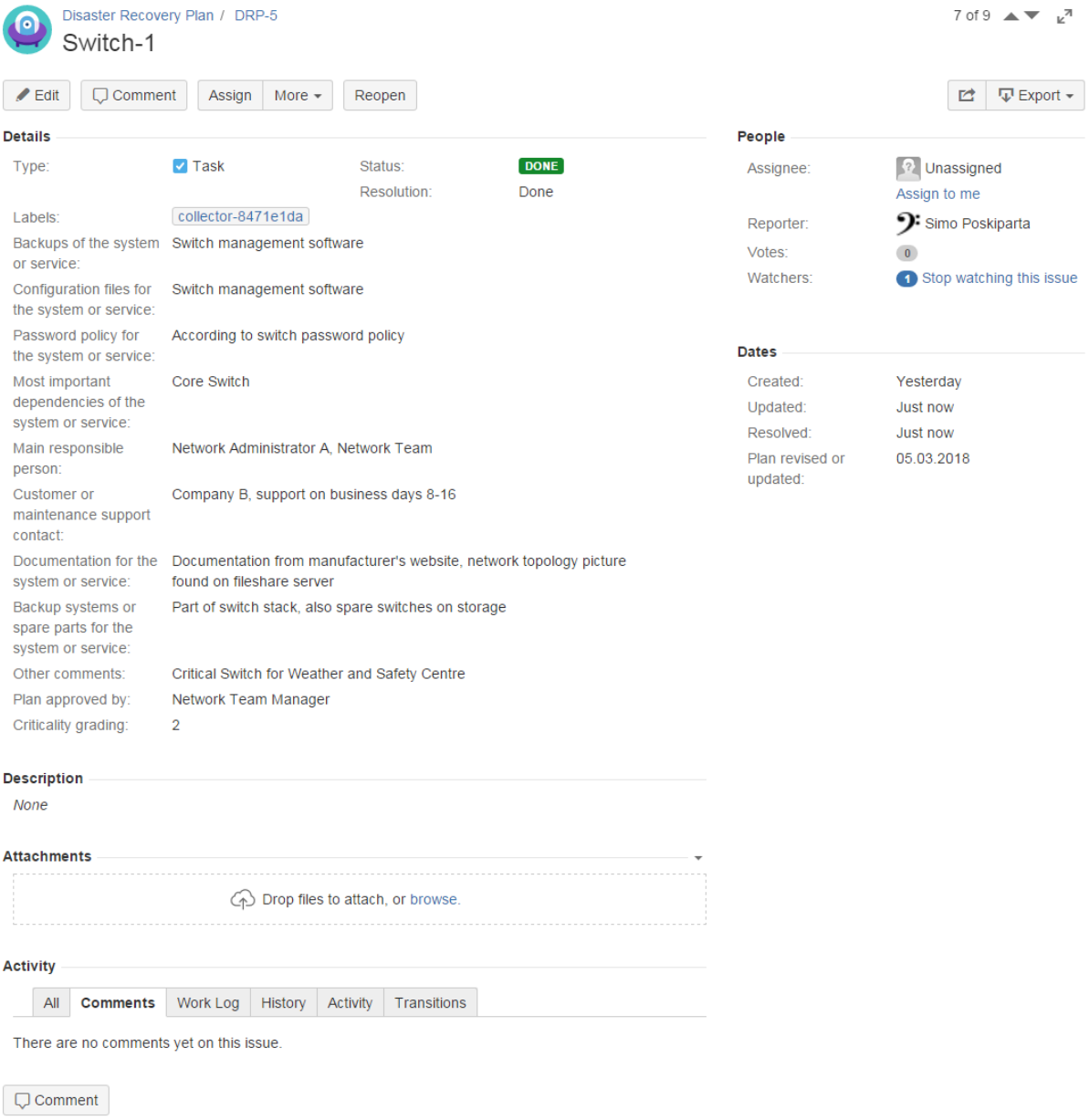

Figure 15: DRP for Switch-1.

7.2 Testing the Tool with an Example Service

At second, the DRP tool was tested with a web service in a similar situation as before. The test group was able to fill in almost all the fields without any difficulties. As with the testing with a network switch, the field “Vital data source dependencies” were left blank. The results for this DRP plan are shown in the Figure 16 below.

Figure 16: DRP for Web Service B.

7.3 Observations on Testing the Tool and Future Improvements for Tool

Overall the administrators were really pleased with the DRP tool. It was easy to fill in, and had pre-fixed fields that they wanted according to questionnaire that was made before. All the features, or fields were thought necessary although in some cases all the fields are not necessary to fill in. In network appliances, backups and configuration files can be the same, or be stored in same system. As with a web services the field “Backup systems or spare parts for the system or service” could be named in a way that it focuses more on how the resilience or high availability is obtained, rather than indicating that there would be a spare system for the service in a case of malfunction. As

discussed in the previous chapters, in a modern data center the ways of making systems and services resilient and highly available are more than just having a different physical machine or having a bag of nuts and bolts ready just in the case.

The possibility to add three new features or fields were also discussed. These were “How is the reserve power obtained”, “What systems are included in the stack, cluster or similar”, and “Location of the system or service”. In some cases, all the systems and services do not reside in a data center that has reserved power, or even have the UPS systems for a short power outages. The second field was discussed due the fact that in most cases systems run in a stacks or clusters, and services run on a virtualized environment. This field would make it easier to understand how the resiliency of the system is obtained and what are the systems and services that are included in the entirety. The location field would be helpful in a cases that the organization or company have many locations or premises that the systems and services are located in. In the case of a single data center this could also point to the location of the machine within the data center.

Improvements to the existing fields were also discussed. It would be nice to have an automatic date picker instead of having to fill in the field “Plan revised or updated”. An idea for an automatic counter for the update process was expressed. If there is an agreement that all the DRP’s are revised e.g. biyearly, it would be helpful to have an automatic counter running for the time of a next revision. An improvement for the free text boxes was also stated. There are many fields that – at least in an ideal situation, would lead to a similar choices. For example, there should not be numerous different backup systems or documentation places. In the suggested new fields such as location and reserve power, there could be only a couple of choices. These could be obtained by making the field a drop-down menu with the possibilities already listed, and an administrator would only need to pick the right one. This would make the task even faster, and leave out the possible spelling errors in the free text boxes. One suggestion was also that this would enable a totally new way of presenting the dependencies of the systems, in a two dimensional or even using a 3D modelling since it would be possible to combine the pre-fixed choices in many ways.

The whole chain of approval was also discussed. It was left unclear that what does the approval of the DRP actually mean. Is it the approval that someone has filled in the

form, or is it the approval that the content of the DRP is coherent and meets the existing criteria in case there is such? Or is there even a need for a formal approval agreement, or can the person that has approved the plan be held responsible in a case there is e.g. a lawsuit in case of a disaster? These are questions where there are no clear or unambiguous answers, but they need to be discussed in a context of an organization culture, and possible legal agreements.

As a summary for the testing, administrators thought this tool is a simple enough to use, and has all the necessary fields. The improvements that were discussed are possible included in the next version of this tool. It was widely agreed that filling this kind of a form for a system or a service really makes one to think all the facts that are listed in it. Although the data that this tool produces is by no means something totally new and possibly nothing that the administrators hadn't though before, filling in all the fields for a single system or a service adds a value for the system resiliency thus increasing the whole contingency planning process as a whole.

8 Conclusions

The concepts of contingency, Business Continuity Planning (BCP), Business Impact Analysis BIA, Disaster Recovery Planning (DRP), Continuity Planning etc. may seem a little confusing for the first time they are heard of. This may well be the case, as can be seen in the literature review of this Master's thesis since even the specialists' opinions and terminology and how they discuss the concepts and their relatedness seem to vary. The goal of this Master's thesis was to overcome this terminology, and to create something simple administrator can use, and is willing to use in his daily job. It must not be a necessity to know all the industry jargon and specific fancy terms so that one could fill a form that will help in case of a disaster.

The literature review revealed that there are a lot of features that need to be taken into account if an all-inclusive DRP form would be made. Depending on the size of the organization or company, some features such as types of reserved power may be unnecessary. On the other hand, large data centers may have several ways to achieve a solid way to ensure their power feeding.

The important part of this master's thesis was also to ask administrators how they feel about the subject, and what they think is important. The questionnaire that was implemented gave informative answers on the subject. The need for self-explaining and easy to approach fillable form was one thing they wanted. The use of pre-existing software was also on the list, so that creating DRP's would not need another new software. Also, creating the process to be clear and simple was also on their wanted list, but it was out of the scope of this master's thesis. The process itself depends so heavily on the organization or company that it should always be implemented to fit the culture of the organization or company and ways of acting.

The testing phase showed that this tool may as well be used with a single appliance as with a larger web service. That was also important, since the goal was also to harmonize the way that DRP's are done rather than creating few different approaches depending on the appliance, system or service. Testing the tool with administrators also brought up few improvement ideas that could be implemented in the next phase of this tool. The fact that these ideas arose only after the questionnaire had been done, and the tool had been implemented shows the importance and necessity to test the final product with the people who are going to be mostly using it. Things need to be thought on the customer's point

of view if one wants to really satisfy the customer. And in many cases customer may not know what they want before they see it. Based on the opinions administrators gave on the testing phase, one can say the outcome of this master's thesis was successful. The implementation of the tool itself is possible in countless ways. It can be created as a web page, as a separate coding project etc. The Atlassian Jira software was chosen in this case because it was already in use, thus decreasing the threshold to start to fill in the DRP's. The theory and discussion about the necessary features will give a good starting point for creating DRP's in any environment. One should always think his/her organization or company, and the protected assets. In the information security, everything needs to be adapted for the object. There are no commercial off-the-shelf products for this type of a need.

References

FMI – FMI (2018). Organization webpages. Available at: www.fmi.fi [Accessed 20 February 2018].

Gregory, P. (2007). IT Disaster Recovery Planning For Dummies. 45, 236

Harris, S. (2013). All In One CISSP , sixth edition 355, 887, 921, 925, 909, 1277

Hotchkiss, S. (2010). Business Continuity Management. *Business Impact Analysis.* 28

Kirvan, P – Lelii, S (2017). Techtarget Network webpages. Available at: http://searchdisasterrecovery.techtarget.com/Data-center-disaster-recovery-plan-template-and-guide [accessed 22 February 2018]

Miller, L – Gregory, P (2012). CISSP for Dummies. Business Continuity and Disaster Recovery Planning. 212

Morgan, S. (2017). Cybersecurity Ventures Company webpages. Available at: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ [accessed 18 February 2018].

Portnoy, M. (2016). Virtualization Essentials. *Understanding Hypervisors.* 22

Requirements for ICT Contingency Planning 2012. Instruction Helsinki: Ministry of Finance

Tuomi, J. Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi. (new edition) 84, 98, 99

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. Annettu Helsingissä 1.10.2010

Varghese, M. (2002). Disaster Recovery. *What Constitutes a Disaster*. 28-47

Wallace, M. Webber, L (2004). The Disaster Recovery Handbook. *The Assets*. 217

Zdrojewski, M. (2013). Default Reasoning webpages. Available at: http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/ [accessed 20 March 2018]